GANNETT

GANNETT POLICY HANDBOOK

Last updated on 6/11/2025

Internal Use Only

The information in this handbook may or may not apply to you if you are covered by a collective bargaining agreement, represented by a union, or employed or contracted by a publication that Gannett manages pursuant to a Joint Operating Agreement.

Section 7 of the National Labor Relations Act ("the act") guarantees employees the right to self-organization, to form, join, or assist labor organizations, to bargain collectively through representatives of their own choosing, and to engage in other concerted activities for the purpose of collective bargaining or other mutual aid or protection, as well as the right to refrain from any or all such activities. Section 8(a)(1) of the act makes it an unfair labor practice for an employer to interfere with, restrain or coerce employees in the exercise of the rights guaranteed in Section 7 of the act.

Nothing in this handbook will be interpreted, applied or enforced to interfere with, restrain or coerce employees in the exercise of their rights under Section 7 of the National Labor Relations Act. To the extent that you are an employee covered by the act, nothing in this handbook prevents you from:

(a) Organizing a union to negotiate with the company concerning your wages, hours, and other terms and conditions of employment.
(b) Forming, joining or assisting a union, such as by sharing employee contact information; talking about or soliciting for a union during nonwork time, such as before or after work or during break times; or distributing union literature during nonwork time, in nonwork areas.
(c) Discussing wages and other working conditions with co-workers or a union.
(d) Taking action with one or more co-workers to improve working conditions by, among other means, raising work-related complaints directly with the employer or with a government agency, or seeking help from a union; striking and picketing, depending on its purpose and means; and taking photographs or other recordings in the workplace, together with co-workers, to document or improve working conditions, except where an overriding employer interest is present.
(e) Wearing union hats, buttons, t-shirts, and pins in the workplace.
(f) Choosing not to engage in any of these activities.

Table of Contents

Acceptable Encryption Policy

Policy Owner: IT Security and Data Privacy
Version: 20250101
Employee Scope: All US employees who work with the encryption methods for data required to be encrypted by the Data Protection Policy, including those encryption methods developed internally, purchased or that are open source

Purpose

This policy will define appropriate types of encryptions to protect Gannett Sensitive Data as defined in the Data Protection Policy. While there are several ways to encrypt data, not all methods provide appropriate protection or are appropriate for use in all circumstances.

Definitions and Acronyms

When navigating this policy, it's important to grasp the terminology. Our Glossary of Cybersecurity Terms provides concise definitions for key concepts.

Policy

General Information

- Acceptable encryption must be used for protecting Level 1 and Level 2 Sensitive Data requiring encryption as defined in the Data Protection Policy.
- Encryption keys and passphrases must be securely maintained to prevent data loss.
- Gannett's key length requirements will be reviewed annually and upgraded as technology allows. See in Acceptable Encryption section below.
- The export of encryption technologies is restricted by the U.S. Government. Residents of countries other than the United States should make themselves aware of the encryption technology laws of the country in which they reside.
- Gannett also has certain contractual obligations regarding export that it must comply with. If there is any question whether an encryption technology can be used in a certain geography, please consult with the Gannett Legal department.

Acceptable Encryption

- Only proven, standard algorithms or higher encryption algorithms should be used as the basis for encryption technologies. Examples of proven standards are AES, RSA and Chacha20. These algorithms represent the actual cipher used for an approved application.
- Elliptic-curve Diffie-Hellman (ECDH) key agreement scheme or other Elliptical Curve algorithm should use 'curve25519
- A secure one-way hashing algorithm such as SHA2-256/384/512 (see FIPS-180-2) or SHA3-256/384/512 (see FIPS-PUB-202) may be used to encrypt information that does not need to be decrypted again (to securely store passwords or to ensure data integrity, for example).
- Symmetric cryptosystem key lengths must be at least 256 bits.
- Asymmetric cryptosystem keys must be 2048 bits or a length that yields the equivalent strength of a 256-bit symmetric cryptosystem key.

Unacceptable Encryption

- As legacy applications are discovered, the encryption protocol used in those applications should be evaluated for upgrade to current standards to the extent feasible given the application, technology and resource limitations. If the acceptable encryption algorithms per this policy Information Security Policies and Standards Exceptions Policy cannot be met, an exception must be submitted per Gannett's Information Security Exception Policy. Proprietary (non-standard) encryption algorithms must not be used for encrypting Level 1 and Level 2
- Developers should never develop and implement their own encryption or hashing mechanisms.
- Any symmetric algorithm with maximum block sizes under 128 bits.
- Any symmetric algorithm with maximum key sizes under 256 bits.
- Any asymmetric algorithm with maximum key sizes under 2048 bits.
- Any stream algorithm with maximum key sizes under 128 bits.
- Any elliptical curve algorithm utilizing suspected compromised curves:
- Any version of nistp192/nistp224/nistp256/nistp384/nistp512
- Any version of ecdh-sha2 (sha2-1.2 and 1.3, or NIST)
- Any curve generated using the Dual_EC_DRBG PRNG algorithm.
- Certain widely-used, but undesirable algorithm(s):
- RC4/ArcFour/RC5/RC6 (obsolete or unproven design)
- SAFER/IDEA/IDEA NXT (obsolete or has licensing issues)
- TEA/XTEA/XXTEA/BTEA (unproven design)

Vendor Encryption Standards

- Vendor encryption policies and practices applicable to vendor owned and/or controlled systems that process Gannett data must be reviewed as part of Gannett's vendor review process for compliance with this Acceptable Encryption Policy, as applicable (which may be provided by review of available audit or attestation documentation). An exception or a risk treatment plan will be implemented for any gaps based on severity.

Enforcement and Exception

- Compliance with this policy is required under Gannett's Information Security Policies and Standards Enforcement Policy and Gannett may take actions in response to non-compliance as provided under the Enforcement Policy.
- Any exceptions to this policy must follow Gannett's Information Security Policies and Standards Exceptions Policy.

This policy may be updated occasionally by the Company. The current version of this policy, as well as other referenced policies, may be viewed on MyLife@Gannett.

Acceptable Use and IT (Information Technology) Monitoring Policy

Policy Owner: IT Security and Data Privacy
Version: 20250101
Employee Scope: All US-based Gannett employees, as well as independent contractors and agents, whether working in a Gannett office or remotely (collectively, "Users" "User")

Purpose

The Acceptable Use and IT Monitoring Policy (the Policy) outlines the acceptable use of Gannett information, electronic and computing devices, and network resources. The policy applies to resources owned or leased or otherwise under contract by Gannett including computers, email, chat, and other electronic systems. Monitoring activity helps Gannett ensure network security, prevent unauthorized access, investigate security incidents, and/or ensure compliance with legal obligations.[1]

Scope

Information governed within this policy's scope includes all company-owned and controlled information, all information shared with Gannett by customers, suppliers and other stakeholders and all information created, transmitted, received and/or stored on Gannett Systems (as defined below). This Policy applies to all US-based Gannett employees, as well as independent contractors and agents, whether working in a Gannett office or remotely (collectively, "Users" "User").

Definitions and Acronyms

When navigating this policy, it's important to grasp the terminology. Our Glossary of Cybersecurity Terms provides concise definitions for key concepts.

Policy

Gannett Systems

Gannett Systems are intended for business purposes only (except for limited personal use as described below) during working hours and at all other times. To protect Gannett and its various stakeholders, Gannett restricts the use of all Gannett Systems. Users must use Gannett Systems in a productive, ethical, and lawful manner.

Ownership and Business Purpose Use

Gannett owns Gannett Systems and information transmitted by, received from, accessed through, or stored in them.

Users are to only use approved software and approved SaaS services and must not transmit, process, or store company information (data) anywhere other than on a Gannett System. Only designated persons (per Signature Authorization Policy) are authorized to

[1] CPRA requirement

sign-up or enter into an agreement with an online or SaaS service. See list of approved software and services:
https://gannett.service-now.com/sp?id=kb_article_view&sysparm_article=KB29364

Use of Gannett Systems is intended for business-related use. Occasional use for legitimate personal purposes (such as using a Company phone to make an appointment) is allowed where such use does not affect the individual's business performance and is not detrimental to Gannett in any way. The content of any communication via Gannett Systems must always follow the policies around prohibited activities described below, regardless of purpose.

No Expectation of Privacy
All contents of Gannett Systems are the property of Gannett. Users understand that they can have no expectation of privacy in connection with the use of any part of the Gannett Systems or with creation, transmission, receipt, or storage of any documents, files, data, messages, information or other materials ("Materials") in the Gannett Systems and by continuing in employment or engagement with Gannett by contract, expressly waive any right to such privacy. Even though Users may have unique user log-in identification codes and passwords to access an electronic device or Gannett Systems, Users have no expectation of privacy in the use of any Gannett System or Materials created on, within or transmitted over or stored in Gannett Systems, including System traffic and servers.

Personal privacy is different from confidentiality. If there is a separate basis for keeping confidentiality (vis-a-vis third parties) of User communications, such as the attorney-client privilege between in-house counsel and internal business clients or the confidentiality of journalistic sources, those will be kept confidential by Gannett where appropriate as decided by Gannett.

Use of Personal Devices for Company Business
Gannett recognizes that some Users use personal devices for Company business purposes. This is allowed, given the User follows this Acceptable Use and IT Monitoring Policy when using Gannett Systems.

Companies are required by certain data privacy laws to implement policies for the protection of Gannett Systems and customer data, including when accessed through external devices used for Company business. Those policies must be consistent with applicable law requirements, including those under the National Labor Relations Act (NLRA).

Currently, the only monitoring tool Gannett uses for personal devices used for Company business is Microsoft InTune (for mobile devices), which is needed to enable Gannett to wipe Company data stored on a personal mobile device if it is lost or stolen. This tool was separately announced by Gannett IT. For more information about Microsoft InTune, see these knowledge articles.
https://gannett.service-now.com/sp?id=kb_article_view&sysparm_article=KB28117
https://gannett.service-now.com/sp?id=kb_article_view&sysparm_article=KB24096

Consistent with applicable laws, other security tools and measures may be implemented by Gannett for personal devices used for Company business. Additional notice and/or FAQs (Frequently Asked Questions) will be provided to Users in connection with any such implementation. For example, Gannett will implement a broader "Bring Your Own Device" (BYOD) policy, at which time it may support use of the Global Protect VPN and other security tools on User personal devices used for Company business. A separate announcement will be supplied when Gannett implements its broader BYOD policy, which will outline the specific privacy and security requirements for the use of personal devices for Company business. Any monitoring of personal devices will be described in the BYOD policy.

Monitoring and Inspection
Gannett reserves the right, without further notice and at its sole discretion, to monitor, access, review, search, inspect, audit, and intercept any component of the Gannett Systems and all Materials contained or created therein, or transmitted over the Gannett Systems, including but not limited to by means of firewalls, SSL (Secure Sockets Layer)/TLS (Transport Layer Security) and HTTPS interception, and other measures deployed by Gannett. Gannett will exercise these rights at any time for any reason, including but not limited to, suspected or actual: external cybersecurity threats, violations of Company policies or code of conduct, illegal or improper activity, or misuse of Company resources. Gannett also reserves the right to show such Materials when consistent with Gannett's business purposes, when required by legal process and/or in response to requests from law enforcement. Such activity will be conducted as allowed by and in accordance with any applicable laws, including the National Labor Relations Act.

Do not use Gannett Systems for any matter that you want to be kept private or confidential by Gannett.

Materials will be kept in line with Gannett's Record Retention & Destruction Policy

Use of the Gannett Remote Access VPN
Remote access via the Gannett Remote Access VPN, password multifactor authentication and anti-virus software is required on Gannett-issued laptops. For further information about the use of the Gannett VPN, please see the FAQs.

Camera Surveillance
Gannett makes limited use of video surveillance at its facilities for legitimate business purposes, such as physical security and fraud and theft prevention. Cameras will be visible in the place where the monitoring is taking place within and around Company property in view of Users and visitors. No sound will be recorded with visual surveillance and cameras will not be in private workplace areas such as the restrooms. The video footage will be kept as part of Gannett's Record Retention & Destruction Policy.

Examples of Prohibited Activities
Gannett prohibits any misuse of Gannett Systems. The following list has examples of prohibited uses of Gannett Systems. This list is intended to supply examples and is not

exhaustive (and excludes any such uses undertaken by Gannett and its legal advisors and security service providers as part of its monitoring and inspection activities outlined in this policy). Subject to applicable law, Gannett reserves the right to take proper disciplinary action for any conduct which it considers a misuse of Gannett Systems or that violates Gannett's policies.

- Creating, downloading, posting, giving, or viewing harassing, defamatory, threatening, or discriminatory messages or materials;
- Sending, receiving, or viewing material that is obscene or of a sexual or pornographic nature;
- Sending anonymous e-mail;
- Allowing others to use a user's e-mail address except where expressly allowed by the User as needed for business purposes (such as having an administrative assistant access and use their e-mail while they are out of office);
- Sending e-mail messages under another person's name except where expressly allowed by the User as needed for business purposes (such as having an administrative assistant access and use their e-mail while they are out of office);
- Viewing another User's e-mail without permission;
- Tampering with another Users e-mail or computer;
- Sending chain e-mail or unsolicited commercial e-mail ("spam");
- Using Gannett Systems for personal gain;
- Not following policies or guidelines established by Gannett for use of Gannett Systems or not following any other policies or guidelines established by Company administrators or their designees;
- Violating any license to any part of Gannett Systems or any international, federal, state, or local law, or promoting, supporting, or engaging in any illegal purpose(s);
- Monitoring or intercepting the files or electronic communications of other Users or third parties;
- Hacking or obtaining access to systems or accounts they are not authorized to use;
- Using other people's logins or passwords except where expressly allowed by the User as needed for business purposes and approved by Gannett Information Security and Legal (such as having an administrative assistant access and use their e-mail while they are out of office) or circumventing log-in procedures;
- Using administrative accounts to access the Internet, such as web browsers or email;
- Breaching, testing, or monitoring computer or network security measures; and
- Because of the danger of malware, malfunctions, data breaches and other problems, Users are prohibited from:
    - Using unapproved online or SaaS services to transmit, process, or store company information (data), which includes but not limited to note taking, task tracking, planning, workflow, or calendar services.
    - Signing up for online services (free or paid) for business purposes. This includes using services provided by an approved vendor but is outside of Gannett's licensed use. For example, users are prohibited from using a gmail.com account for business purposes, even though some Google services are approved for use. Only designated persons are authorized to enter into agreements on behalf of Gannett.

- Downloading any software or programs (including without limitation, surveys, forms and AI (Artificial Intelligence) functionality) from the internet or otherwise introducing into or placing any software or programs on Gannett Systems without express permission from Information Security, or where legal terms are needed for such use, review by Legal;
- Using personal e-mail and instant messaging accounts for sending Company business communications (except for limited situations as business needs may require, such as when Gannett Systems are down and Users need a temporary alternative communication channel, or when it is urgent to reach a particular User for a business matter)

Enforcement

Users who violate this policy will be subject to disciplinary action, which may include, without limitation, termination of employment (for employees) or termination of contract (for contractors and agents), reporting to law enforcement and /or legal action.

Additionally, Users are obligated to report any alleged violations of this policy of which they are aware. Reports of violations will be investigated. Users must cooperate with the investigation. False information provided during an investigation may lead to disciplinary action.

Enforcement and Exception

- Compliance with this policy is required under Gannett's Information Security Policies and Standards Enforcement Policy and Gannett may take actions in response to non-compliance as provided under the Enforcement Policy.
- Any exceptions to this policy must follow Gannett's Information Security Policies and Standards Exceptions Policy.

This policy may be updated occasionally by Gannett. The current version of this policy, as well as other referenced policies, may be viewed on MyLife@Gannett.

Account and Access Management Policy

Policy Owner: IT Security and Data Privacy
Version: 20250101
Employee Scope: All US employee accounts used to access Gannett electronic data, systems, resources, and services

Purpose

This policy defines how employee accounts should be used and administered within Gannett.

Accounts that are not properly created, monitored, maintained, used, or terminated may be used to gain unauthorized access to Gannett systems. Unauthorized access has the potential of compromising Gannett systems, data, business partners and/or customers with resultant harm to Gannett finances and/or reputation.

This policy will define general account policies; how and when an account is created; who is authorized to request a new account or change an account; when an account should be disabled or deleted; and policies related to specific account types.

Scope

This policy applies to all employee accounts used to access Gannett electronic data, systems, resources, and services.

Definitions and Acronyms

When navigating this policy, it's important to grasp the terminology. Our Glossary of Cybersecurity Terms provides concise definitions for key concepts.

Policy

Employee Account Types

- Individual Employee User Account
  - Individual named account used to obtain access to standard employee resources for employees managed by the workforce management system.
- Elevated Privilege Account
  - Individual named account providing the permanent or temporary ability to view and/or change system or application configurations or data beyond the ability of a "standard" user of that system or application.
  - Misuse of elevated access privileges must be reported immediately according to the Cybersecurity Incident Reporting Policy.
  - Misuse of elevated access privileges is a violation of Gannett policy and could lead to disciplinary action including without limitation termination.
- External Account
  - Any account provided by a third-party to a Gannett employee to manage Gannett data, services, or resources.
- Shared Account

  - Non-individual account where more than one person can log into the account using the same login credential. Typically used to support access to shared equipment, applications, or processes (examples include kiosks, production equipment, software application dashboards or console job processing).
  - Use of Gannett shared accounts (where Gannett controls the account setup and access vs. a vendor) is discouraged except where documented as a Policy Exception and specifically authorized by the appropriate business owner.
- Mailbox Account
  - A non-individual account associated with a shared mailbox that can direct received messages to multiple users (for example, privacy@Gannett.com).

System Level Accounts

Both employees and non-employees may access System Level Accounts, subject to the requirements in this Policy.

- Service Account
  - Non-individual account that is usually not accessed by a personal login to perform its regular functions because it provides automated access between computers or applications.
    Designated IT (Information Technology) personnel will have logins to Service Accounts for system maintenance using Elevated Privilege – but not for routine access. Service accounts operate services, schedule tasks, and perform similar automatic processes without human interaction, in cases where those automated functions are associated with a particular named account.
- Built-in Account
  - Non-individual accounts included by the licensor with the system cannot be removed. These may be elevated privilege accounts.
- Top Level Account
  - Highly privileged account typically required for initial system configuration and/or disaster recovery purposes and is not used daily.

General Account Policies

- Each employee and non-employee user must be assigned and use an individual account to access Gannett owned or licensed systems, resources, and data. The use of Shared Accounts is discouraged and is subject to the Information Security Exception Policy.
- All accounts must have a password or equivalent authentication mechanism that complies with the Password Security Policy.
- System permissions should be assigned to system roles where appropriate, and the role(s) should be assigned to an account based on the individual's job function.
  - Outside of established birthright permissions (the standard set of permissions that are associated with a particular account type), system permissions should NOT be assigned to a user account by default; if no permissions are explicitly granted, the user should have no ability to perform any activity.
  - Users whose job duties require Elevated Privilege Account access to a system or application must be assigned and exclusively use an account separate from their

primary Gannett identity account for the specified Elevated Privilege Account activities.
    - Users with multiple account types should use the type of account with the least privilege that will allow them to accomplish the task. For example, use non-privileged accounts when accessing non-security functions.
- Documented review of accounts associated with financially significant systems must be completed at the frequency (e.g., annual, semi-annual) defined by the SOX Application Risk Ranking (pursuant to the User Access Review process implemented pursuant to SOX (Sarbanes Oxley) requirements) to verify that users have appropriate, authorized, role-based systems access, ensuring compliance with appropriate internal and external requirements.
    - Based on the review, appropriate action must be taken to correct inappropriate access.

Segregation of Duties

- Account authority for all account types must be assigned on the principle of least privilege, allowing only system access by authorized users as necessary to accomplish assigned tasks in accordance with that user's job function.
- Duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of assets. When provisioning access, care should be taken that no single person can access, modify or use assets without authorization or detection. The initiation of an event should be separated from its authorization.

Access to Networks and Network Systems

The following security standards shall govern access to Gannett networks and network services:

- Technical access to Gannett networks is the responsibility of and performed by the appropriate team(s) and/or appropriate automation.
- Only authorized employees, with a business need, shall be granted access to the production networks and resources.
- Remote connections to production systems and networks must be encrypted.

System and Application Access – Information Access Restriction

Applications must restrict access to program functions and information to only authorized users in accordance with the defined access control policy. The level and type of restrictions applied by each application should be based on the individual application requirements, as identified by the data owner.

Before implementation, evaluation criteria are applied to application software to determine the necessary access controls and data policies. Assessment criteria include, but are not limited to:

- Sensitivity and classification of data
- Risk to the organization of unauthorized access or disclosure of data

- Granular control(s) on user access rights to the application and data stored within the application
- Restrictions on data outputs, including filtering sensitive information, controlling output, and restricting information access to authorized personnel
- Controls over access rights between the evaluated application and other applications and systems
- Programmatic restrictions on user access to application functions and privileged instructions
- Logging and auditing functionality for system functions and information access
- Data retention, aging and destruction

All unnecessary default accounts must be removed or disabled before making a system available on the network. Specifically, vendor default passwords and credentials must be changed on all Gannett systems, devices, and infrastructure prior to deployment. This applies to ALL default passwords, including those used by operating systems, software that provides security services, application and system accounts, and Simple Network Management Protocol (SNMP) community strings where feasible.

Secure Log-on Procedures and Access
Secure log-on controls shall be designed and selected in accordance with the sensitivity of data and the risk of unauthorized access based on the totality of the security and access control architecture.

Access to Program Source Code
Access to program source code and associated items, including designs, specifications, verification plans, and validation plans shall be strictly controlled to prevent the introduction of unauthorized functionality into software, avoid unintentional changes, and protect Gannett intellectual property.
All access to source code shall be based on business needs and must be logged for review and audit.

Access Provisioning
All newly hired employees complete New Employee Orientation (NEO), and the human resources team assigns the required compliance training based on the role of the new hire. Training is mandated for specific employee groups dependent on role, position and/or location. Eligible employees will receive more information about required training within their first several weeks of employment. For Example:

- Anti-Harassment
- Active Intruder
- Cybersecurity Awareness
  - Employees with a company computer/email address
- Gannett Code of Conduct
- Gannett Technology Orientation
- Inclusion and Diversity

- Protecting the Safety and Health of Workers at Gannett

Account Creation/Change Policies

- Account administration including the creation, modification, and deletion of all account types is the responsibility of and performed by the appropriate account provisioning team(s) and/or appropriate automation.
- New account creation must be initiated through a documented request to an appropriate manager or initiated via the workforce system automation and approved by the appropriate manager or their specified designee(s).
- Changes to existing account privileges must be initiated through a documented request to an appropriate manager or initiated via the workforce system automation and approved by the appropriate manager or their specified designee(s). This is not intended to regulate resource sharing by resource owners in self-managed collaboration tools (such as SharePoint).
- Creation of and changes to elevated privilege accounts must be approved by the appropriate manager of the application in question, or designated members of the SRC (Security Review Council) for IT elevated privilege accounts.
- Documentation associated with the request and authorization (approval) of new accounts or account modifications must be retained for future reference, where required for finance controls compliance, fraud prevention and/or in accordance with the relevant system documentation and retention policy.
- Accounts used by vendor entities to remotely access, support, or maintain system components should be enabled only when needed, supervised while in use, and disabled when not in use and should be associated to an appropriate account expiration, recertification and/or periodic account review process upon creation.
- Prior to account creation, the appropriate account provisioning team should verify that the account does not violate any of Gannett security or system access control policies to ensure segregation of duties, fraud prevention measures, and access rights restrictions are met.
- Account provisioning team(s) and/or managers perform annual access rights reviews of user, administrator, and service accounts to verify user access is limited to systems required for their job function. Access reviews may include group membership and evaluations of specific or exception-based permission.
- Access rights shall also be reviewed as part of any job role change, including promotion, demotion, or transfer within the company.

Access Termination and Account Removal

- Manager or their specified designee must update the workforce management system upon termination of an employee with the employee's termination and/or last day of work dates (whichever date is earlier) and account access for all accounts must be revoked on a timely basis.
- Employees responsible for the oversight of non-employee accounts must submit notification (via standard procedures in the appropriate system) of a non-employee separation, and account access for all such accounts must be revoked on a timely basis.

- Accounts should be removed once it has been confirmed that related data access is no longer needed.
- Dormant individual named accounts must be disabled or rendered unusable after 90 days. Any exceptions to this policy must be documented and handled in accordance with the Information Security Exception Policy.
- Elevated Privileges Accounts must be removed if access is no longer needed due to a change in job duties.
- Non-individual (unnamed) accounts with elevated privileges (including, but not limited to Built-in and Top-Level accounts) must be maintained in a secrets vault or must be changed whenever an individual who knew the password is terminated, has a change in job role or is otherwise no longer authorized to gain access to these accounts.
- If a password is stored, it must be stored in a secret vault.

Enforcement and Exception

- Compliance with this policy is required under Gannett's Information Security Policies and Standards Enforcement Policy and Gannett may take actions in response to non-compliance as provided under the Enforcement Policy.
- Any exceptions to this policy must follow Gannett's Information Security Policies and Standards Exceptions Policy.

This policy may be updated occasionally by Gannett. The current version of this policy, as well as other referenced policies, may be viewed on MyLife@Gannett.

Anti-Discrimination, Harassment & Retaliation Policy

Policy Owner: Legal
Version: 20241202
Employee Scope: All new employees upon hire and annually for existing US employees in California, Connecticut, Delaware, Maine, Illinois, New York

Overview

Anti-Discrimination

At Gannett, everyone should be able to work in an environment that is free from any form of discrimination, harassment, retaliation, bullying, abusive conduct or other unlawful conduct. The Company is committed to maintaining a work environment that is free from unlawful discrimination, harassment, retaliation, bullying or abusive conduct, and any other unlawful or unprofessional conduct.

Specifically, this policy prohibits conduct that is discriminatory, harassing, retaliatory or bullying based on sex (including pregnancy, childbirth, breastfeeding or related medical conditions), race, religion (including religious dress and grooming practices), color, gender (including gender identity and gender expression), ethnicity, national origin or ancestry, physical, mental or sensory disability, medical condition, genetic information or characteristics, genetic predisposition or carrier status, height, weight, marital status, familial status or responsibilities, registered domestic partner status, age, union membership status, enrollment in any public assistance program, sexual orientation, military or veteran status, immigration status or citizenship, reproductive health decision making, status as a victim of domestic violence, sexual assault, stalking or other crimes, use of protected leave of absence, intersectionality (meaning having a combination of two or more such characteristics), housing status, or any other basis protected by federal, state, local anti-discrimination law, ordinance or regulation (the “Protected Characteristics”).

Our Anti-Discrimination, Harassment and Retaliation Policy also prohibits discrimination, harassment, retaliation, bullying, abusive conduct, and/or unprofessional conduct based on the perception that anyone has one or more Protected Characteristics or is associated with a person who has or is perceived as having one or more Protected Characteristics. Finally, our Policy also prohibits discrimination, harassment, retaliation, bullying and/or unprofessional conduct based on hairstyle, hair texture or employee dress and grooming practices associated with a Protected Characteristic.

Gannett will not tolerate any such conduct directed to any and all applicants, employees, independent contractors, temporary workers, interns or other persons (the “Covered Persons”) who work or perform services for Gannett.

Our Anti-Discrimination, Harassment and Retaliation Policy applies to all phases of the employment/business relationship, including decisions concerning recruitment/hiring, promotional opportunities, disciplinary actions, transfers, layoffs and other forms of involuntary terminations, benefits, and selection for training. Discrimination in compensation between Covered Persons of the opposite sex or between Covered Persons

on the basis of other Protected Characteristics performing substantially similar work, as defined by federal and state law, is also prohibited.

Anti-Harassment

The conduct prohibited by this policy includes any verbal, visual or physical conduct that may reasonably be perceived as denigrating or showing hostility toward a Covered Person because of any Protected Characteristics. Among the types of conduct prohibited by this policy are epithets, slurs, negative stereotyping, or intimidating acts based on a Covered Person's Protected Characteristic and/or the circulation (including by e-mail) or posting of written or graphic materials that show hostility toward a Covered Person because of their Protected Characteristic.

In addition, it is a violation of the Company's policy for any person to engage in any form of sexual harassment by, among other things, engaging in any act of sexual battery, by making unwelcome sexual advances, requests for sexual favors, or by engaging in other verbal, visual or physical conduct of a sexual nature towards a Covered Person where:

- submission to such conduct is made either explicitly or implicitly a term or condition of an individual's employment or business relationship with the Company; or
- an employment decision affecting a Covered Person is based on that person's acceptance or rejection of such conduct; or
- such conduct interferes with a Covered Person's work performance or creates an intimidating, hostile, or offensive working environment.

Other examples of unwelcome sexual conduct may include, but are not limited to, jokes or comments of a sexual nature, the displaying of sexual materials at work, leering or stalking an employee (including cyberstalking), making sexual propositions, making repeated flirtations or sexual advances, and engaging in inappropriate touching or other conduct of sexual nature towards a Covered Person.

Sexual harassment can occur between any individuals, regardless of their sex or gender. A perpetrator of sexual harassment can be a superior, a subordinate, a co-worker or anyone in the workplace including an independent contractor, contract worker, vendor, client, customer or visitor.

Sexual harassment is not limited to the physical workplace itself. It can occur while a Covered Person is traveling for business or at Company-sponsored events or parties. Calls, texts, emails, and social media usage by persons can also constitute unlawful harassment towards a Covered Person, even if they occur away from the workplace premises or not during work hours.

Bullying

The Company also prohibits abusive conduct or bullying in the workplace such as repeated verbal abuse, derogatory remarks, insults and epithets; verbal or physical conduct that is threatening, intimidating or humiliating; or gratuitous sabotage or undermining of a Covered Person's work performance. A single act generally may not constitute abusive conduct or bullying unless it is especially severe and egregious.

Bullying involves a malicious and persistent pattern of mistreatment of a Covered Person from another or others. Examples of bullying include, but are not limited to, unwarranted criticism; engaging in threatening, intimidating or cruel behaviors; screaming, swearing, or name calling; blaming someone without factual justification, unfairly singling someone out; humiliating, ridiculing or taunting; and spreading false rumors.

Reasonable Accommodations

Finally, in connection with our commitment to Anti-Discrimination and to ensuring equal access to employment and employment opportunities for all Covered Persons, the Company will also engage in the interactive process with all Covered Persons to provide reasonable accommodations that may be needed to apply for employment with Gannett, perform the essential functions of a Covered Person's position, or access a benefit, privilege or term or condition of employment as a result of a Covered Person's disability, pregnancy, religion or status as a victim of domestic violence, sexual assault, stalking or crime, or as a result of the need to express breast milk while at work following the birth of the child. Reasonable accommodations will be provided in a manner consistent with the Company's legal obligations unless the requested accommodation creates an undue hardship on the Company's operations.

Anyone who needs reasonable accommodations to ensure equal employment opportunity should contact their supervisor or Human Resources to address their needs.

Retaliation

Gannett also forbids individuals from treating any Covered Person adversely for engaging in any of the following conduct in good faith: **(i)** making a complaint or report of discrimination, harassment, bullying or other abusive, unlawful or unprofessional conduct or otherwise opposing such conduct, **(ii)** assisting or encouraging another person to make a complaint or report of discrimination, harassment or other abusive, unlawful or unprofessional conduct, **(iii)** cooperating in an investigation into such a complaint or report, **(iv)** filing an administrative complaint with the US. Equal Employment Opportunity Commission (EEOC) or a state or local governmental agency that investigates such complaints or reports, or **(v)** filing a civil action or testifying in a civil action or proceeding involving discrimination, harassment or other abusive, unlawful or unprofessional conduct. In addition, no one may be subjected to retaliation for making a good faith request for reasonable accommodation as a result of their disability, religion or status as a victim of domestic violence, sexual assault or stalking, or their need to express breast milk at work following the birth of a child.

Retaliation can be any action that would keep a person from coming forward to make or support a harassment or discrimination claim or request a reasonable accommodation. Adverse action need not be job-related or occur in the workplace to constitute retaliation. Any such retaliatory action is a violation of Company policy.

Your Role

All persons who perform services on behalf of Gannett must refrain from engaging in any form of discrimination, harassment, retaliation, bullying or other abusive conduct in the workplace.

Gannett affirms its commitment to complying fully with both the letter and spirit of federal, state and local laws relating to discrimination, harassment, retaliation, bullying or other abusive conduct in the workplace, and we have a protocol for handling complaints of any such inappropriate behavior. If you are experiencing or observing conduct that you believe violates this policy, you must promptly report the conduct to your supervisor, Human Resource Business Partner, hr4u or any other member of management with whom you feel comfortable. If reporting to your Human Resource Business Partner or hr4u is not an option, you may contact the Ethics Violation Reporting Hotline at 866.553.4734.

You may also file complaints of alleged discrimination, harassment, denial of accommodation or retaliation to the U.S. Equal Employment Opportunity Commission (EEOC) or various state anti-discrimination/civil rights agencies in the state where you work. The Company's labor law posters located in the Company's worksites provide additional information, including the contact information, procedures to file a complaint and remedies available through the EEOC and such state agencies. Employees may also locate the EEOC's contact information at www.eeoc.gov.

Our Role

The Company will conduct a prompt, thorough and objective investigation of any complaint of a violation of our Anti-Discrimination, Harassment and Retaliation Policy. All persons are required to cooperate with any internal investigation of any complaint made of conduct that is inconsistent with this policy. During the investigation, the Company may put certain interim measures in place, such as a leave of absence or a transfer. Once the report has been thoroughly investigated, the Company will take further appropriate action based on its findings. That action may be a conclusion that a violation occurred, as explained immediately below. The Company may also conclude, depending on the circumstances, either that no violation of policy occurred or that the Company cannot conclude whether or not a violation occurred.

If an investigation reveals that a violation of this policy or other inappropriate conduct has occurred, then the Company will take corrective action, as is appropriate under the circumstances, regardless of the job positions of the parties involved. The Company may discipline an employee for any inappropriate conduct discovered in investigating reports or complaints made under this policy, regardless of whether the conduct amounts to a violation of law or even a violation of this policy. If the person who engaged in any conduct deemed inappropriate under this policy is not employed by the Company, then the Company will take whatever corrective action is reasonable under the circumstances, which may include termination of employment.

Every effort will be made to keep all matters relating to the investigation and claim report confidential to the extent feasible.

Training

As a further means to prevent discrimination, harassment, retaliation, abusive conduct and bullying in the workplace, Gannett provides employees and supervisors with harassment and abusive conduct prevention training. Please see your Human Resources Business Partner or hr4u regarding the state requirements.

Questions

Questions regarding this policy should be addressed directly to Human Resources.

Resource Links

- See the Ethics Policy on MyLife@Work > Guidelines and Policies > Code of Business Conduct and Ethics Policy.
- Gannett Core Values
- Additional Information for Employees Residing in New York State

Approved Technology Policy

Policy Owner: IT Security and Data Privacy
Version: 20240701
Employee Scope: All employees authorized to use or access Gannett data, systems, resources, and/or services, including those accessed on Gannett computers or on personal or public devices

Purpose

The Approved Technology policy outlines what software and online services are approved for use, how to request access, install software or online services, and the process to purchase if required. Software and online services for employees include collaboration services, project management tools, document storage services, and cloud computing services, Software as a Service (SaaS) or any other online "as a Service" service.

This policy is in place to protect Gannett data and for the purpose of maintaining system availability, security, privacy, and legal compliance. Accordingly, use of software and online services needs to have proper security and privacy controls in place and legal and finance approval before use. This will help us ensure the security and integrity of our systems and data and avoid unnecessary spending by utilizing existing approved technology.

Gannett utilizes a large, diverse set of software and online services to run its business and deliver products to our customers and may already have approved technology for your use. Purchasing new software or online services may not be required if the same or similar technology has already been purchased.

Examples of software or online services not approved for using with or storing Gannett data:
Free for use downloads or extensions
Surveys or Forms (Use Microsoft Forms)
Dropbox or Box (excluding instances where clients or sources place documents or data in these services that must be retrieved by Gannett)
Google Docs (use Microsoft Sharepoint or OneDrive instead)
Airtable (use Microsoft Lists instead)
ChatGPT (don't use the free web version – Gannett has an enterprise agreement)

To view the list of approved technology or to request software or service be added please go to the following link:
https://gannett.service-now.com/kb_view.do?sysparm_article=KB93930

Scope

This policy applies to all employees authorized to use or access Gannett data, systems, resources, and/or services, including those accessed on Gannett computers or on personal or public devices.

Policy

Approved Technology

Technology is only approved once the Enterprise Technology Governance Council (ETGC) has approved it, the provider has completed the vendor review process, the contract has been completed and the software has been added to the Approved Technology list.

Information about Approved Technology is located in ServiceNow:
https://gannett.service-now.com/kb_view.do?sysparm_article=KB93930

Installation of Technology

Most approved technology applications can be found and requested by submitting an Access Request. Some approved software is already available and can be installed from Software Center (Windows Users) or Self Service (Mac Users).

If you are unable to find an application or tool or would like to make a request, please submit a Service Request.

Use of Technology

Use of technology for Gannett business or accessed through Gannett environments must comply with the Acceptable Use and IT Monitoring Policy.

Procurement of Technology

The acquisition or procurement of technology (software), including new vendor contracts, addendums to existing contracts and renewals, must go through the vendor risk assessment process. To initiate the process for a new or existing vendor, email vendor@gannett.com with the vendor name, Gannett business owner and the email address of the primary vendors.

The vendor risk assessment process consists of the following steps that must be completed to designate software as approved technology:

1. The requestor must initiate the process with an email to vendor@gannett.com as described under Procurement of Technology, above.
2. The ETGC reviews and provides preliminary approval to proceed with vendor and contract review. If rejected, the ETGC will provide a reason, but regardless the technology may not be used within Gannett or for Gannett business.
3. Funding approvals by the finance planning and analysis team.
4. The software vendor must complete the third-party security and privacy risk assessment review.
5. The ETGC must evaluate and sign off on any risks that are outside of risk tolerance (e.g., there is no encryption of data, or no SOC report, SLAs do not meet Gannett IT goals, etc.)
6. Legal review must be completed for all agreements, such-as Terms of Service, SLAs, Data Processing Agreements, order forms, and software licenses
7. The agreement(s) may only be signed by an authorized signatory per the Signature Authorization Policy.

Enforcement and Exception

- Compliance with this policy is required under Gannett's Information Security Policies and Standards Enforcement Policy and Gannett may take actions in response to non-compliance as provided under the Enforcement Policy.
- Any exceptions to this policy must follow Gannett's Information Security Policies and Standards Exceptions Policy.

This policy may be updated, with or without notice, from time to time by Gannett. The current version of this policy, as well as other referenced policies, may be viewed on Okta> MyLife@Gannett.

California Disability, Unemployment and Paid Family Leave Provisions

Policy Owner: Human Resources
Version: 20201201
Employee Scope: All new California employees

Overview

This employer is registered with the Employment Development Department (EDD) as required by the California Unemployment Insurance Code and is reporting wage credits to the EDD that are being accumulated for you to be used as a basis for:

Unemployment Insurance (UI)

(funded entirely by employers' taxes)

Unemployment Insurance (UI) is paid for by your employer and provides partial income replacement when you are unemployed or your hours are reduced due to no fault of your own. To claim UI benefit payments you must also meet all UI eligibility requirements, including that you must be available for work and searching for work.

How to File a New UI Claim

Use one of the following methods:

- Online: UI Online℠ is the fastest and most convenient way to file your UI claim. Visit UI Online (edd.ca.gov/UI_Online) to get started.
- Phone: Representatives are available at the following toll-free numbers, Monday through Friday between 8 a.m. to 12 noon (Pacific Standard Time) except during state holidays. English 1-800-300-5616 Cantonese 1-800-547-3506 Vietnamese 1-800-547-2058 Spanish1-800-326-8937 Mandarin 1-866-303-0706 TTY 1-800-815-9387
- Fax or Mail: When accessing UI Online to file a new claim, some customers will be instructed to fax or mail their UI application to the EDD. If this occurs, the Unemployment Insurance Application (DE 1101I), will display. For faster and more secure processing, fax the completed form to the number listed on the form. If mailing your UI application, use the address on the form and allow additional time for processing.

Important: Waiting to file your UI claim may delay benefit payments.

Disability Insurance (DI)

(funded entirely by employees' contributions)

Disability Insurance (DI) is funded by employees' contributions and provides partial wage replacement benefits to eligible Californians who are unable to work due to a non-work-related illness, injury, pregnancy, or disability.

Your employer must provide the Disability Insurance Provisions (DE 2515) brochure, to newly hired employees and to each employee who is unable to work due to a non-work-related illness, injury, pregnancy, or disability.

How to File a New DI Claim
Use one of the following methods:

- Online: SDI Online is the fastest and most convenient way to file your claim. Visit SDI Online (edd.ca.gov/SDI_Online) to get started.
- Mail: To file a claim with the EDD by mail, complete and submit a Claim for Disability Insurance (DI) Benefits (DE 2501) form. You can obtain a paper claim form from your employer, physician/practitioner, visiting a State Disability Insurance office, online at EDD Forms and Publications (edd.ca.gov/Forms), or by calling 1-800-480-3287.

Note: If your employer maintains an approved Voluntary Plan for DI coverage, contact your employer for assistance.
For more information about DI, visit State Disability Insurance (edd.ca.gov/disability) or call 1-800-480-3287. State government employees should call 1-866-352-7675. TTY (for deaf or hearing-impaired individuals only) is available at 1-800-563-2441.

Paid Family Leave (PFL)

(funded entirely by employees' contributions)
Paid Family Leave (PFL) is funded by employees' contributions and provides partial wage replacement benefits to eligible Californians who need time off work to care for seriously ill child, parent, parent-in-law, grandparent, grandchild, sibling, spouse, or registered domestic partner. Benefits are available to parents who need time off work to bond with a new child entering the family by birth, adoption, or foster care placement. Benefits are also available for eligible Californians who need time off work to participate in a qualifying event resulting from a spouse, registered domestic partner, parent, or child's military deployment to a foreign country.

Your employer must provide the Paid Family Leave (DE 2511) brochure, to newly hired employees and to each employee who is taking time off work to care for a seriously ill family members, to bond with a new child, or to participate in a qualifying military event.

How to File a New PFL Claim
Use one of the following methods:

- Online: SDI Online is the fastest and most convenient way to file your claim. Visit SDI Online (edd.ca.gov/SDI_Online) to get started.
- Mail: To file a claim with the EDD by mail, complete and submit a Claim for Paid Family Leave (PFL) Benefits (DE 2501F) form. You can obtain a paper claim form from your employer, a physician/practitioner, visiting a State Disability Insurance office, online at EDD Forms and Publications (edd.ca.gov/Forms), or by calling 1-877-238-4373.

Note: If your employer maintains an approved Voluntary Plan for PFL coverage, contact your employer for assistance.

For more information about PFL, visit State Disability Insurance (edd.ca.gov/disability) or call 1-877-238-4373. State government employees should call 1-877-945-4747. TTY (for deaf or hearing-impaired individuals only) is available at 1-800-445-1312.

Note

Some employees may be exempt from coverage by the above insurance programs. It is illegal to make a false statement or to withhold facts to claim benefits. For additional information, visit the EDD (edd.ca.gov).

California Domestic Violence Leave Notice

Policy Owner: Human Resources
Version: 20210301
Employee Scope: All new California employees

Overview

Rights of victims of domestic violence, sexual assault, stalking, crimes that cause physical injury or mental injury, and crimes involving a threat of physical injury; and of persons whose immediate family member is deceased as a direct result of a crime

Your Right to Take Time Off

- You have the right to take time off from work to obtain relief from a court, including obtaining a restraining order, to protect you and your children's health, safety or welfare.
- If your company has 25 or more workers, you can take time off from work to get medical attention for injuries caused by crime or abuse, receive services from a domestic violence shelter, program, rape crisis center, or victim services organization or agency as a result of the crime or abuse, receive psychological counseling or mental health services related to an experience of crime or abuse, or participate in safety planning and take other actions to increase safety from future crime or abuse.
- You may use accrued paid sick leave or vacation, personal leave, or compensatory time off that is otherwise available for your leave unless you are covered by a union agreement that says something different. Even if you don't have paid leave, you still have the right to time off.
- In general, you don't have to give your employer proof to use leave for these reasons.
- If you can, you should tell your employer before you take time off. Even if you cannot tell your employer beforehand, your employer cannot discipline you if you give proof explaining the reason for your absence within a reasonable time. Proof can be a police report, a court order, a document from a licensed medical professional, a victim advocate, a licensed health care provider, or counselor showing that you were undergoing treatment for domestic violence related trauma, or a written statement signed by you, or an individual acting on your behalf, certifying that the absence is for an authorized purpose.

Your Right to Reasonable Accommodation

- You have the right to ask your employer for help or changes in your workplace to make sure you are safe at work. Your employer must work with you to see what changes can be made. Changes in the workplace may include putting in locks, changing your shift or phone number, transferring or reassigning you, or help with keeping a record of what happened to you. Your employer can ask you for a signed statement certifying that your request is for a proper purpose, and may also request proof showing your need for an accommodation. Your employer cannot tell your coworkers or anyone else about your request.

Your Right to Be Free from Retaliation and Discrimination

Your employer cannot treat you differently or fire you because:

- You are a victim of domestic violence, sexual assault, stalking, a crime that caused physical injury or mental injury, or a crime involving threat of physical injury; or are someone whose immediate family member is deceased as a direct result of a crime.
- You asked for leave time to get help.
- You asked your employer for help or changes in the workplace to make sure you are safe at work.

You can file a complaint with the Labor Commissioner's Office against your employer if he/she retaliates or discriminates against you.

For more information, contact the California Labor Commissioner's Office. We can help you by phone at 213-897-6595, or you can find a local office on our website: www.dir.ca.gov/dlse/DistrictOffices.htm. If you do not speak English, we will provide an interpreter in your language at no cost to you. This Notice explains rights contained in California Labor Code sections 230 and 230.1. Employers may use this Notice or one substantially similar in content and clarity.

Labor Commissioner's Office Victims of Domestic Violence, Sexual Assault and Stalking Notice

California Family Care & Medical Leave & Pregnancy Disability Leave

Policy Owner: Human Resources
Version: 20230101
Employee Scope: All new California employees

Overview

Under California law, an employee may have the right to take job-protected leave to care for their own serious health condition or a family member with a serious health condition, or to bond with a new child (via birth, adoption, or foster care). California law also requires employers to provide job-protected leave and accommodations to employees who are disabled by pregnancy, childbirth, or a related medical condition.

Under the California Family Rights Act of 1993 (CFRA), many employees have the right to take job-protected leave, which is leave that will allow them to return to their job or a similar job after their leave ends. This leave may be up to 12 work weeks in a 12-month period for:

- the employee's own serious health condition;
- the serious health condition of a child, spouse, domestic partner, parent, parent-in-law, grandparent, grandchild, sibling, or someone else with a blood or family-like relationship with the employee ("designated person"); or
- the birth, adoption, or foster care placement of a child.

If an employee takes leave for their own or a family member's serious health condition, leave may be taken on an intermittent or reduced work schedule when medically necessary, among other circumstances.

Eligibility

To be eligible for CFRA leave, an employee must have more than 12 months of service with their employer, have worked at least 1,250 hours in the 12-month period before the date they want to begin their leave, and their employer must have five or more employees.

Pay and Benefits During Leave

While the law provides only unpaid leave, some employers pay their employees during CFRA leave. In addition, employees may choose (or employers may require) use of accrued paid leave while taking CFRA leave under certain circumstances. Employees on CFRA leave may also be eligible for benefits administered by the Employment Development Department.

Taking CFRA leave may impact certain employee benefits and seniority date. If employees want more information regarding eligibility for a leave and/or the impact of the leave on seniority and benefits, they should contact their employer.

Pregnancy Disability Leave

Even if an employee is not eligible for CFRA leave, if disabled by pregnancy, childbirth or a related medical condition, the employee is entitled to take a pregnancy disability leave of up to four months, depending on their period(s) of actual disability. If the employee is CFRA-eligible, they have certain rights to take both a pregnancy disability leave and a CFRA leave for reason of the birth of their child.

Reinstatement

Both CFRA leave and pregnancy disability leave contain a guarantee of reinstatement to the same position or, in certain instances, a comparable position at the end of the leave, subject to any defense allowed under the law.

Notice

For foreseeable events (such as the expected birth of a child or a planned medical treatment for the employee or of a family member), the employee must provide, if possible, at least 30 days' advance notice to their employer that they will be taking leave. For events that are unforeseeable, employees should notify their employers, at least verbally, as soon as they learn of the need for the leave. Failure to comply with these notice rules is grounds for, and may result in, deferral of the requested leave until the employee complies with this notice policy.

Certification

Employers may require certification from an employee's health care provider before allowing leave for pregnancy disability or for the employee's own serious health condition. Employers may also require certification from the health care provider of the employee's family member, including a designated person, who has a serious health condition, before granting leave to take care of that family member.

Want to learn more?

Visit: calcivilrights.ca.gov/family-medical-pregnancy-leave/

If you have been subjected to discrimination, harassment, or retaliation at work, or have been improperly denied protected leave, file a complaint with the Civil Rights Department (CRD).

To File A Complaint

Civil Rights Department
calcivilrights.ca.gov/complaintprocess
Toll Free: 800.884.1684 / TTY: 800.700.2320
California Relay Service (711)

Have a disability that requires a reasonable accommodation? CRD can assist you with your complaint.

For additional translations of this guidance, visit:
www.calcivilrights.ca.gov/posters/required

California Sexual Harassment Fact Sheet

Policy Owner: Human Resources
Version: 20230911
Employee Scope: All new California employees

Overview

Sexual harassment is a form of discrimination based on sex/gender (including pregnancy, childbirth, or related medical conditions), gender identity, gender expression, or sexual orientation. Individuals of any gender can be the target of sexual harassment. Unlawful sexual harassment does not have to be motivated by sexual desire. Sexual harassment may involve harassment of a person of the same gender as the harasser, regardless of either person's sexual orientation or gender identity.

There are two types of Sexual Harassment

1. "Quid pro quo" (Latin for "this for that") sexual harassment is when someone conditions a job, promotion, or other work benefit on your submission to sexual advances or other conduct based on sex.
2. "Hostile work environment" sexual harassment occurs when unwelcome comments or conduct based on sex unreasonably interferes with your work performance or creates an intimidating, hostile, or offensive work environment. You may experience sexual harassment even if the offensive conduct was not aimed directly at you.

The harassment must be severe or pervasive to be unlawful. A single act of harassment may be sufficiently severe to be unlawful.

Sexual Harassment includes many forms of offensive behaviors

Behaviors that may be sexual harassment:

1. Unwanted sexual advances
2. Offering employment benefits in exchange for sexual favors
3. Leering; gestures; or displaying sexually suggestive objects, pictures, cartoons, or posters
4. Derogatory comments, epithets, slurs, or jokes
5. Graphic comments, sexually degrading words, or suggestive or obscene messages or invitations
6. Physical touching or assault, as well as impeding or blocking movements

Actual or threatened retaliation for rejecting advances or complaining about harassment is also unlawful.

Employees or job applicants who believe that they have been sexually harassed or retaliated against may file a complaint of discrimination with CRD within three years of the last act of harassment or retaliation.

CRD serves as a neutral fact-finder and attempts to help the parties voluntarily resolve disputes. If CRD finds sufficient evidence to establish that discrimination occurred and settlement efforts fail, the Department may file a civil complaint in state or federal court to address the causes of the discrimination and on behalf of the complaining party. CRD

may seek court orders changing the employer's policies and practices, punitive damages, and attorney's fees and costs if it prevails in litigation.

Employees can also pursue the matter through a private lawsuit in civil court after a complaint has been filed with CRD and a Right-to-Sue Notice has been issued.

Employer Responsibility & Liability

All employers, regardless of the number of employees, are covered by the harassment provisions of California law. Employers are liable for harassment by their supervisors or agents. All harassers, including both supervisory and non-supervisory personnel, may be held personally liable for harassment or for aiding and abetting harassment.

The law requires employers to take reasonable steps to prevent harassment. If an employer fails to take such steps, that employer can be held liable for the harassment. In addition, an employer may be liable for the harassment by a non-employee (for example, a client or customer) of an employee, applicant, or person providing services for the employer. An employer will only be liable for this form of harassment if it knew or should have known of the harassment, and failed to take immediate and appropriate corrective action.

Employers have an affirmative duty to take reasonable steps to prevent and promptly correct discriminatory and harassing conduct, and to create a workplace free of harassment.

A program to eliminate sexual harassment from the workplace is not only required by law, but it is the most practical way for an employer to avoid or limit liability if harassment occurs.

Civil Remedies

- Damages for emotional distress from each employer or person in violation of the law
- Hiring or reinstatement
- Back pay or promotion
- Changes in the policies or practices of the employer

All employees must take the following actions to prevent harassment and correct it when it occurs:

1. Distribute copies of this brochure or an alternative writing that complies with Government Code 12950. This pamphlet may be duplicated in any quantity.
2. Post a copy of the Department's employment poster entitled "California Law Prohibits Workplace Discrimination and Harassment."
3. Develop a harassment, discrimination, and retaliation prevention policy in accordance with 2 CCR 11023. The policy must:
    - Be in writing.
    - List all protected groups under the FEHA.

- Indicate that the law prohibits coworkers and third parties, as well as supervisors and managers with whom the employee comes into contact, from engaging in prohibited harassment.
- Create a complaint process that ensures confidentiality to the extent possible; a timely response; an impartial and timely investigation by qualified personnel; documentation and tracking for reason able progress; appropriate options for remedial actions and resolutions; and timely closures.
- Provide a complaint mechanism that does not require an employee to complain directly to their immediate supervisor. That complaint mechanism must include, but is not limited to including: provisions for direct communication, either orally or in writing, with a designated company representative; and/or a complaint hotline; and/or access to an ombudsperson; and/or identification of CRD and the United States Equal Employment Opportunity Commission as additional avenues for employees to lodge complaints.
- Instruct supervisors to report any complaints of misconduct to a designated company representative, such as a human resources manager, so that the company can try to resolve the claim internally. Employers with 50 or more employees are required to include this as a topic in mandated sexual harassment prevention training (see 2 CCR 11024).
- Indicate that when the employer receives allegations of misconduct, it will conduct a fair, timely, and thorough investigation that provides all parties appropriate due process and reaches reasonable conclusions based on the evidence collected.
- Make clear that employees shall not be retaliated against as a result of making a complaint or participating in an investigation.

4. Distribute its harassment, discrimination, and retaliation prevention policy by doing one or more of the following:
   - Printing the policy and providing a copy to employees with an acknowledgement form for employees to sign and return.
   - Sending the policy via email with an acknowledgment return form.
   - Posting the current version of the policy on a company intranet with a tracking system to ensure all employees have read and acknowledged receipt of the policy.
   - Discussing policies upon hire and/or during a new hire orientation session.
   - Using any other method that ensures employees received and understand the policy.
5. If the employer's workforce at any facility or establishment contains ten percent or more of persons who speak a language other than English as their spoken language, that employer shall translate the harassment, discrimination, and retaliation policy into every language spoken by at least ten percent of the workforce.
6. In addition, employers who do business in California and employ 5 or more part-time or full-time employees must provide at least one hour of training regarding the prevention of sexual harassment, including harassment based on gender identity, gender expression, and sexual orientation, to each non- supervisory employee; and two hours of such training to each supervisory employee. Training must be provided within six months of assumption of employment. Employees must be trained every two years. Please see Gov. Code 12950.1 and 2 CCR 11024 for further information.

To File A Complaint

Civil Rights Department
calcivilrights.ca.gov/complaintprocess
Toll Free: 800.884.1684
TTY: 800.700.2320

California Workplace Discrimination Poster

Policy Owner: Human Resources
Version: 20241017
Employee Scope: All new California employees

Overview

The California Civil Rights Department (CRD) enforces laws that protect you from illegal discrimination and harassment in employment based on your actual or perceived:

- Ancestry
- Age (40 and above)
- Color
- Disability (physical, developmental, mental health/psychiatric, HIV and AIDS)
- Genetic information
- Gender expression
- Gender identity
- Marital status
- Medical condition (genetic characteristics, cancer, or a record or history of cancer)
- Military or veteran status
- National origin (includes language restrictions and possession of a driver's license issued to undocumented immigrants)
- Race (includes hair texture and hairstyles)
- Religion (includes religious dress and grooming practices)
- Reproductive health decision making
- Sex/gender (includes pregnancy, childbirth, breastfeeding and/or related medical conditions)
- Sexual orientation

Harassment

1. The law prohibits harassment of employees, applicants, unpaid interns, volunteers, and independent contractors by any person. This includes a prohibition against harassment based on any characteristic listed above, such as sexual harassment, gender harassment, and harassment based on pregnancy, childbirth, breastfeeding, and/or related medical conditions.
2. All employers are required to take reasonable steps to prevent all forms of harassment, as well as provide information to each of their employees on the nature, illegality, and legal remedies that apply to sexual harassment.
3. Employers with five or more employees and public employers must train their employees regarding the prevention of sexual harassment, including harassment based on gender identity, gender expression, and sexual orientation.

Discrimination/Reasonable Accommodations

1. California law prohibits employers with five or more employees and public employers from discriminating based on any protected characteristic listed above when making decisions about hiring, promotion, pay, benefits, terms of employment, layoffs, and other aspects of employment.

2. Employers cannot limit or prohibit the use of any language in any workplace unless justified by business necessity. The employer must notify employees of the language restriction and consequences for violation.
3. Employers cannot discriminate against an applicant or employee because they possess a California driver's license or ID issued to an undocumented person.
4. Employers must reasonably accommodate the religious beliefs and practices of an employee, unpaid intern, or job applicant, including the wearing or carrying of religious clothing, jewelry or artifacts, and hair styles, facial hair, or body hair, which are part of an individual's observance of their religious beliefs.
5. Employers must reasonably accommodate an employee or job applicant with a disability to enable them to perform the essential functions of a job.

Additional Protections

California Law offers additional protections to those who work for employers with five or more employees. Some exceptions may apply. These additional protections include:

1. Specific protections and hiring procedures for people with criminal histories who are looking for employment.
2. Protections against discrimination based on an employee or job applicant's use of cannabis off the job and away from the workplace.
3. Up to 12 weeks of job-protected leave to eligible employees to care for themselves, a family member (child of any age, spouse, domestic partner, parent, parent-in-law, grandparent, grandchild, sibling) or a designated person (with blood or family-like relationship to employee); to bond with a new child; or for certain military exigencies.
4. Up to five days of job-protected bereavement leave within three months of the death of a family member (child, spouse, parent, sibling, grandparent, grandchild, domestic partner, or parent-in-law).
5. Up to four months of job-protected leave to employees disabled because of pregnancy, childbirth, or a related medical condition, as well as the right to reasonable accommodations, on the advice of their health care provider, related to their pregnancy, childbirth, or a related medical condition.
6. Up to five days of job-protected leave following a reproductive loss event (failed adoption, failed surrogacy, miscarriage, stillbirth, or unsuccessful assisted reproduction).
7. Protections against retaliation when a person opposes, reports, or assists another person to oppose unlawful discrimination, including filing an internal complaint or a complaint with CRD.

Remedies/Filing A Compliant

1. The law provides remedies for individuals who experience prohibited discrimination, harassment, or retaliation in the workplace. These remedies can include hiring, front pay, back pay, promotion, reinstatement, cease-and-desist orders, expert witness fees, reasonable attorney's fees and costs, punitive damages, and emotional distress damages.
2. If you believe you have experienced discrimination, harassment, or retaliation, you may file a complaint with CRD. Independent contractors and volunteers: If you believe you have been harassed, you may file a complaint with CRD.

3. Complaints must be filed within three years of the last act of discrimination/harassment/retaliation. For those who are under the age of eighteen, complaints must be filed within three years after the last act of discrimination/harassment/retaliation or one year after their eighteenth birthday, whichever is later.

If you have been subjected to discrimination, harassment, or retaliation at work, file a complaint with the Civil Rights Department (CRD).

To File A Complaint

Civil Rights Department
calcivilrights.ca.gov/complaintprocess
Toll Free: 800.884.1684 / TTY: 800.700.2320
California Relay Service (711)

Have a disability that requires a reasonable accommodation? CRD can assist you with your complaint.

The Fair Employment and Housing Act is codified at Government Code sections 12900 - 12999. The regulations implementing the Act are at Code of Regulations, title 2, division 4.1
Government Code section 12950 and California Code of Regulations, title 2, section 11023, require all employers to post this document. It must be conspicuously posted in hiring offices, on employee bulletin boards, in employment agency waiting rooms, union halls, and other places employees gather. Any employer whose workforce at any facility or establishment consists of more than 10% of non-English speaking persons must also post this notice in the appropriate language or languages.

For translations of this guidance, visit: www.calcivilrights.ca.gov/posters/required

Change Management Policy

Policy Owner: IT Security and Data Privacy
Version: 20250101
Employee Scope: All US Gannett employees, independent contractors, agents and third parties who perform business functions for any business units which are owned and controlled by Gannett and or an affiliate of Gannett and that use Gannett Systems

Purpose

- This policy will cover the requirements needed to document, communicate, and manage changes associated with Gannett's Systems as defined in the Glossary of Cybersecurity Terms referenced below.
- The intent of this policy is to ensure a unified framework for change management. Therefore, changes will occur based on proper authorization through standardized methods, processes and procedures that keep business continuity, ensure security, minimize risk to Gannett and support regulatory compliance.
- This policy applies to all applications in all phases (development, testing, implementation, and production) and Gannett Systems, including servers, workstations, and network devices.

Definitions and Acronyms

When navigating this policy, it's important to grasp the terminology. Our Glossary of Cybersecurity Terms provides concise definitions for key concepts.

Policy

- All Gannett employees must follow a documented change management process including the components outlined in this policy.
- Changes to network or firewall configurations that affect network traffic as described by defined industry networking standards must be reviewed by the Security Review Council (SRC). SRC review may be sent using the instructions here.
- Changes to Financial Application software or product development is also governed by the Financial Application Software Development Policy.
- Changes to Gannett developed applications/products and third-party applications should be reviewed by the SRC prior to release or initial operational deployment.
- Changes must be fully documented including but not limited to changes or modifications related to implementing security patches, custom software and Commercial Off The Shelf (COTS) software and firewall or router configuration changes.
- Changes that can affect major business operations must go through a Change Advisory Board (CAB) prior to deployment. The CAB is assigned by each functional department to set change guidelines and boundaries such as change moratoria endorsed by technology, product, and business stakeholders to ensure the stability, robustness and reliability of Gannett services and systems.
- The change management process must include:
  - A process for properly documenting a change.
  - A review of the risk associated with the change.

  - A process for approving or denying the change.
  - A process for completing functionality testing.
  - A process for documenting the back out plan.
  - Appropriate separation of duties.
  - A process for communicating the occurrence of a change.
  - A process for communicating the completion of a change.
- Emergency Changes:
  - Any change that cannot go through a full change control process is considered an emergency change.
  - Emergency changes must have proper approval from the senior executive responsible for the technology that is undergoing the change.
  - Emergency changes must be fully tested and documented, which may occur after implementation of the change if timing urgencies prevent advance documentation or testing.
  - Emergency changes must be communicated to the applicable CAB and the applicable stakeholders as soon as possible.
  - After the emergency has abated, an emergency change may be reviewed for further remediation per the regular change management process as needed.

PCI (Payment Card Industry)/DSS Change Management Process

- Changes pertaining to systems, networks, applications and processes that are part of the CDE (Cardholder Data Environment) or in PCI scope must adhere to the Payment Card Industry Data Security Standards. (PCI DSS). The change management processes must include:
  - Review and Documentation of the change must be completed via an SRC review.
  - Identification of applicable PCI DSS requirements to the system or network.
  - Update PCI DSS scope as appropriate.
- Changes pertaining to financial information are regulated by the Sarbanes-Oxley Act (SOX) and must adhere to specific reporting, documentation, evidence and auditing requirements. Changes must adhere to Sarbanes-Oxley (SOX) Compliance Controls.
- Changes to all system components are managed securely and according to PCI DSS requirement 6.5.1 as follows:
  - Reason for, and description of, the change.
  - Documentation of security impact.
  - Documented change approval by authorized parties.
  - Testing to verify that the change does not adversely impact system security.
  - For bespoke and custom software changes, all updates are tested for compliance with Requirement 6.2.4 before being deployed into production. (6.2.4- refer to Financial Application Software Development Policy)
  - Procedures to address failures and return to a secure state.

Capacity Management

- Monitoring and adjusting the use of processing resources and system storage is essential to ensure that Gannett's requirements for system availability and performance are met.

- Human resource skills, availability, and capacity shall be reviewed and considered as a part of capacity planning and as part of the annual risk assessment process.
- Expanding processing or storage capacity by scaling resources, without altering the relevant network system, can be performed separately from the standard change management and code deployment process.

Enforcement and Exception

- Compliance with this policy is required under Gannett's Information Security Policies and Standards Enforcement Policy and Gannett may take actions in response to non-compliance as provided under the Enforcement Policy.
- Any exceptions to this policy must follow Gannett's Information Security Policies and Standards Exceptions Policy.

This policy may be updated occasionally by the Company. The current version of this policy, and the other policies referenced in this document, may be viewed on MyLife@Gannett.

Code of Business Conduct and Ethics of Gannett Co., Inc.

Policy Owner: Corporate Governance
Version: 20210301
Employee Scope: All employees

Overview

The following sets forth Gannett Co., Inc.'s Code of Business Conduct and Ethics (the "Code"), which has been approved by the Board of Directors of Gannett Co., Inc. ("Gannett" and, together with its direct and indirect subsidiaries, the "Company").

The purpose of the Code is to reinforce and enhance the Company's commitment to an ethical way of doing business. Our goal is not just to comply with the law and regulations that apply to our business; we also strive to abide by the highest standards of business conduct. Of course, the contents of this Code are not new. The policies set forth in the pages that follow are merely a part of the long-standing tradition of high ethical standards of the Company. The Company's directors, officers, and employees, are expected to comply with the policies set forth in the Code. Directors, officers, and employees of the Company should report to compliance officers designated by the Company from time to time or, in the absence of any such designation, to the legal department of the Company ("Compliance Personnel").

Read the Code carefully and make sure that you understand it, the consequences of non-compliance, and the Code's importance to the success of the Company. If any questions arise, the Company's directors, officers, and employees should speak to their supervisors or Compliance Personnel.

The Code cannot and is not intended to cover every applicable law or provide answers to all questions that might arise; for that we must ultimately rely on each person's good sense of what is right, including a sense of when it is advisable to seek guidance from others on the appropriate course of conduct.

Putting The Code of Business Conduct and Ethics To Work

1. **About the Code of Business Conduct and Ethics**

   We at the Company are committed to the highest standards of business conduct in our relationships with each other and in our business dealings. This requires that we conduct our business in accordance with all applicable laws and regulations and in accordance with the highest standards of business ethics. The Code helps each of us in this endeavor by providing a statement of the fundamental principles and key policies and procedures that govern the conduct of our business.

   Our business depends on the reputation of the Company and its employees to exhibit integrity and principled business conduct. Thus, in many instances, the policies set forth in this Code go beyond the requirements of the law.

   The Code is a statement of policies for individual and business conduct and does not, in any way, constitute an employment contract or an assurance of continued

employment. As employees of the Company, you are employed at-will even when you are covered by an express, written employment agreement. This means that, subject to applicable law and notice requirements you may have with the Company, you may choose to resign your employment at any time, for any reason or for no reason at all. Similarly, the Company may choose to terminate your employment at any time, for any legal reason or for no reason at all. Termination of employment (whether by resignation or otherwise) is subject to any covenants you may have with the Company governing your post- termination activities.

2. Meeting Our Shared Obligations

Each of us is responsible for knowing and understanding the policies and guidelines contained in this Code. If you have questions, ask them; if you have ethical concerns, raise them. Compliance Personnel are responsible for overseeing and monitoring compliance with this Code, and the other resources set forth in this Code are available to answer your questions, provide guidance and for you to report suspected misconduct. Our conduct should reflect the Company's values, demonstrate ethical leadership, and promote a work environment that upholds the Company's reputation for integrity, ethical conduct and trust.

A. Responsibility to Our Organization

i. Conflicts of Interest Generally

The identification and management of all conflicts of interest must be fundamental considerations in all of your business-related activities. Broadly speaking, a conflict of interest may be present whenever your interests are inconsistent with, or appear to be inconsistent with, those of the Company. Conflicts of interest, if not properly addressed, can cause serious harm to the Company. Even the mere appearance of a conflict of interest (i.e., where no conflict may actually exist) can result in potentially irreversible damage to the Company's reputation. As such, it is the responsibility of each of us to help in the effort to identify actual or potential conflicts of interest associated with the Company's business and promptly bring any such issues to the attention of Compliance Personnel.

ii. Personal Conflicts of Interest

In order to maintain the highest degree of integrity in the conduct of the Company's business and to maintain your independent judgment, you must avoid any activity or personal interest that creates or appears to create a conflict between your personal interests and the interests of the Company. A conflict of interest may arise when your private interests interfere in any way, or even appear to interfere, with the interests of the Company, including if you take actions or have interests that make it difficult for you to perform your work in respect of the Company objectively and effectively. You should never act in a manner that could cause you to lose your independence and objectivity or that could adversely affect the confidence of your colleagues, other persons with whom the Company conducts business, or the integrity of the Company or its procedures. Although we cannot list every conceivable conflict, the following

are some common examples that illustrate actual or apparent conflicts of interest that should be avoided: Improper Personal Benefits Derived from Association with the Company

Conflicts of interest arise when you or a member of your family receives improper personal benefits as a result of your position with or relation to the Company. You may not accept any benefits from the Company that have not been duly authorized and approved pursuant to Company policy and procedure, including any Company loans or guarantees of your personal obligations.

a. Financial Interests in Other Businesses
   You may not have an ownership interest in any other enterprise if that interest compromises or appears to compromise your loyalty to the Company. For example, you should not own an interest in any enterprise that is a significant competitor with the Company (owning shares of a publicly traded financial institution with multiple business lines shall not be considered a conflict for these purposes by reason of their having some overlapping areas of business) without first clearing any transaction in the securities of such issuer with Compliance Personnel. You may not own an interest in a company that does significant amounts of business with the Company (such as an entity which is a significant source of Company-related investments) without the prior written approval of Compliance Personnel.
b. Business Arrangements with the Company
   Without prior written approval from Compliance Personnel, you may not sell to or purchase from the Company any securities or other property, or personally participate in a joint venture, partnership or other business arrangement with the Company.
c. Outside Employment, Directorships, or Activities with a Competitor of the Company
   Other than with the prior written consent of Compliance Personnel, simultaneous employment with any other entity, serving as a director of a significant competitor of the Company, serving as a director of any entity in which the Company is invested, or engaging in any activity that one would reasonably expect to advance a competitor's interests over that of the Company is strictly prohibited. As such, it is imperative that, prior to agreeing to serve in any such capacity, you consult with and obtain written approval from (I) Compliance Personnel, and (II) your direct supervisor. Please note that the Company may require that the employee obtain indemnities from the company at issue and satisfy other conditions as a condition to approval. In general, approval for this type of activity will be rare. Ultimately, it is your responsibility to consult with your manager and with Compliance Personnel to determine whether a planned activity will compete impermissibly with any of the Company's business activities before you pursue the activity in question.

d. Charitable, Government and Other Outside Activities
The Company encourages participation in projects and causes that further the welfare of our local communities. However, you must obtain the prior written approval of Compliance Personnel before serving as a director or trustee of any charitable, not-for-profit, for-profit, or other entity or before running for election or seeking appointment to any government-related position other than a labor union.

e. Family Members Working in the Industry
You may find yourself in a situation where your spouse or significant other, your children, parents, or in-laws, or someone else with whom you have a familial relationship is employed by a competitor of or entity with a significant business relationship with the Company. Such situations are not prohibited, but they call for extra sensitivity to security, confidentiality and conflicts of interest.
There are several factors to consider in assessing such a situation, including, without limitation, the relationship between the Company and the competitor or entity; the nature of your responsibilities in respect of the Company and those of the other person; and the access each of you has to the confidential information of the organization with which you are associated. Such a situation, however harmless it may appear to you, can create problems for the Company or you. The very appearance of a conflict of interest can create problems, regardless of the propriety of your behavior.
To remove any such doubts or suspicions, you must disclose your specific situation to Compliance Personnel to assess the nature and extent of any concern and how it can be resolved.

iii. Potential Conflicts of Interest
There are a variety of situations in which the Company itself may be viewed as having a conflict of interest. Ultimately, each of us is responsible for helping to identify potential conflicts of interest relating to the Company and promptly raising them with Compliance Personnel who are responsible for managing such conflicts.

iv. Corporate Opportunities
Except as provided in our Amended and Restated Certificate of Incorporation, as amended and in effect from time to time, those individuals who are executive officers of the Company owe a duty to the Company to advance its legitimate interests when the opportunity to do so arises. As such, you may not take for yourself opportunities that are expressly offered to you based on the fact that you are associated with the Company, unless approved by Compliance Personnel; take for yourself any limited investment opportunity; use corporate property, information or position for personal gain; or compete with the Company. No director of the Company shall be deemed an officer of the Company by reason of holding such position (without regard to whether such

position is deemed an officer of the Company under the Amended and Restated Bylaws of the Company, as amended and in effect from time to time).

v. Entertainment, Gifts and Gratuities

The receipt or provision of gifts or entertainment may create the appearance of a conflict of interest or otherwise appear to improperly influence decision making by you or by a person with whom the Company is conducting business or seeks to conduct business. In certain circumstances, the receipt or provision of gifts or entertainment may also be in violation of law. Even where there is no violation of the law, you are prohibited from receiving or giving gifts or entertainment if it could give the impression of being done for an improper purpose or to compromise your judgment, regardless of its value. As such, you may not accept, provide or solicit gifts, entertainment, favors, special accommodations or other things of value other than in accordance with the any applicable Company policies. To be clear, this policy covers both giving and receiving gifts or entertainment and also prohibits the use of personal funds or resources to engage in an activity that is otherwise prohibited if done with the Company's funds or resources.

Gifts of cash or cash equivalents (including gift certificates, securities) in any amount are prohibited and must be returned promptly to the donor. Loans (not including loans at market rates from financial institutions made in the ordinary course of business) from any counter-party, or entity in which the Company has an interest, are prohibited.

vi. Protection and Proper Use of Company Assets

We each have a duty to protect the Company's assets and ensure their efficient use. Theft, carelessness and waste have a direct impact on the Company's profitability. We should take measures to prevent damage to and theft or misuse of Company property. When you leave the Company, all Company property must be returned to the Company. Except as specifically authorized, Company assets, including Company time, funds, equipment, materials, resources and proprietary information, must be used for business purposes only.

vii. Company Books and Records

You must complete all documents relating to Company business accurately and in a timely manner. When applicable, documents must be properly authorized. You must record the Company's financial activities in compliance with all applicable laws and accounting standards. The making of false or misleading entries, records or documentation is strictly prohibited. You must never create a false or misleading report or make a payment or establish an account on behalf of the Company with the understanding that any part of the payment or account is to be used for a purpose other than as described by the supporting documents.

viii. Record Retention Regarding Lawsuits or Government Investigations

If you become aware of any "Pending Legal Matter" (a "Pending Legal Matter" is any existing, threatened or imminent lawsuit, claim or government or regulatory investigation involving the Company), you must immediately contact Compliance Personnel. Once you become aware of a Pending Legal Matter, you must take immediate and affirmative action to preserve all records that are potentially relevant to the Pending Legal Matter, including, but not limited to, drafts, working copies, any electronic data (including e-mail, Word documents, Excel spreadsheets, etc.) and handwritten notes. Compliance Personnel will subsequently take steps to identify and preserve records which may be relevant to such Pending Legal Matter. Such records shall be retained indefinitely or until Compliance Personnel advises otherwise, whether or not this Code or another policy of the Company would otherwise provide for the destruction of such records in the ordinary course of business.

As appropriate, Compliance Personnel will notify all relevant persons who may have custody of relevant records and instruct them to preserve all such records until further notice. Once you are notified by Compliance Personnel of a record preservation directive, or otherwise become aware of a Pending Legal Matter, you must immediately and affirmatively take steps to preserve, as described in the preceding paragraph, all potentially relevant records. Destruction of such records, even if inadvertent, could seriously prejudice you or the Company and could in certain cases subject you and the Company to substantial criminal and civil liability, fines and penalties. Any questions regarding whether a record is relevant to a Pending Legal Matter should be directed to Compliance Personnel.

ix. Confidential Information

You may learn, to a greater or lesser degree, facts about the Company's business, plans, or operations that are not known to the general public or to competitors (collectively, referred to herein as "Confidential Information"). Confidential Information includes information relating to (a) the Company's business (including, without limitation, strategies employed, actual and contemplated investments, the financial performance, including but not limited to performance data, or of any investment thereof, contractual arrangements, plans, tactics, policies, products, software, programs, know-how, intellectual property, market data and methods, financial reports, cost and performance data, balance sheets, portfolio information, contacts, income statements, cash flow statements, statements of shareholder equity, debt arrangements, equity structure, accounts receivable reports, accounts payable reports, and asset holdings), (b) all corporations or other business organizations in which the Company has or has had an investment and (c) possible transactions with third parties, which the Company may be under an obligation to maintain as confidential.

- You must maintain the confidentiality of information entrusted to you by the Company except when disclosure is authorized or legally mandated. If you possess or have access to Confidential Information or trade secrets, you must:

- Not use the Confidential Information for your own benefit or the individual benefit of persons inside or outside of the Company.
- Carefully guard against disclosure of Confidential Information to people outside the Company. For example, you should not discuss such matters with family members or business or social acquaintances or in places where the Confidential Information may be overheard, such as taxis, public transportation, elevators or restaurants.
- Not disclose Confidential Information to any other person unless the person is an officer, director, or employee of the Company, or is otherwise subject to a confidentiality agreement with the Company regarding such information, and has a legitimate business need to know.

Please note that Confidential Information may be received by the Company in a variety of ways, and all information may be considered confidential regardless of the method of delivery. The most common methods through which Confidential Information is delivered by third parties is via hard copy documents, email, and verbally. Of course, regardless of whether the party sending you information considers it confidential, you are still bound by your confidentiality agreement with the Company and are therefore prohibited from sharing such information with outside parties.

In addition, Confidentiality Agreements are commonly used when the Company needs to disclose confidential information to others. A Confidentiality Agreement puts the person receiving Confidential Information on notice that he or she must maintain the secrecy of such information. If, in doing business with persons not associated with the Company, you foresee that you may need to disclose Confidential Information, you are required to contact Compliance Personnel.

Your obligation to treat information as confidential does not end when you leave the Company. Upon the termination of your relationship with the Company, you must return everything that belongs to the Company, including all documents and other materials containing Confidential Information. You must not disclose Confidential Information to a new employer or to other persons after terminating your association with the Company. Nothing contained herein limits in any way any other confidentiality obligations imposed upon you by agreement with the Company or by law.

You may not disclose to the Company the confidential information of any previous employer or company you are associated with, nor may you encourage any other Company employees, directors, or officers (or prospective employees, directors or officers of the Company) to disclose the confidential information of their previous employer (or current employer, as the case may be).

x. Trademarks, Copyrights and Other Intellectual Property

a. Trademarks

Our logo and the name “Gannett Co., Inc.” are examples of trademarks. You must always engaged in fair use our trademarks and advise your supervisor

or Compliance Personnel if you suspect that others may be infringing on such trademarks. Likewise, you must not infringe on the trademarks of third parties. This policy does not apply to use of the Company's name, logo, or other trademark by employees to identify the Company in the course of engaging in activity protected under Section 7 of the National Labor Relations Act or other activity related to employees' terms and conditions of employment.

b. Copyright Compliance
All software or programs created by you in connection with your association with the Company or provision of services to the Company are "works for hire" and are the sole property of the Company. You understand that you have no right, title or interest in any intellectual property created by you in connection with your employment with the Company or provision of services to the Company unless otherwise expressly agreed to in writing by Compliance Personnel.
Works of authorship such as books, articles, drawings, computer software and other such materials may be covered by copyright laws. It is a violation of those laws and of the Company's policies to make unauthorized copies of or derivative works based upon copyrighted materials. The absence of a copyright notice does not necessarily mean that the materials are not copyrighted.
The Company licenses the use of much of its computer software from outside companies. In most instances, this computer software is protected by copyright. You may not make, acquire or use unauthorized copies of computer software. Any questions concerning copyright laws should be directed to Compliance Personnel.

c. Intellectual Property Rights of Others
It is Company policy not to infringe upon the intellectual property rights of others. When using the name, trademarks, logos or printed materials of another entity, including any such uses on the Company's website, it must be done in accordance with applicable law.

xi. Responding to Inquiries from the Press and Others
Only the Chief Executive Officer or a person: (a) designated by the Chief Executive Officer; or (b) authorized to do so in the course of his or her duties, may speak with the press, securities analysts, other members of the financial community, shareholders or groups or organizations (collectively, "Media") as a Company representative. Requests for financial or other information about the Company from the Media, the press, the financial community, or the general public should be referred to the head of the Company's Investor Relations Group.

xii. Responding to Inquiries from the Government or Other Regulatory Authorities

All requests for information from any regulatory organization or the government should be referred promptly to Compliance Personnel.

xiii. Fair Dealing

The Company depends on its reputation for quality, service and integrity. The way we deal with the sources of our investments, financing opportunities, and our investors molds our reputation, builds long-term trust and ultimately determines our success. We must never take unfair advantage of others through manipulation, concealment, affirmative misrepresentation of material facts, abuse of privileged information, or any other unfair dealing practice.

xiv. Insider Trading

You are prohibited by Company policy from buying or selling securities for any purpose at a time when you are in possession of "material non-public information." Such prohibited conduct is known as "insider trading." Passing such information on to someone who may, in turn, buy or sell securities – known as "tipping" – is also illegal. Information is "material" if there is a reasonable likelihood that it would be considered important to an investor in making an investment decision regarding a securities transaction. Further details on the policy are contained in the Company's policy on insider trading (with respect to the Company's directors, officers, or employees). If any questions arise about whether a particular transaction may constitute insider trading, the Company's directors, officers, and employees should consult with Compliance Personnel.

B. Interacting With Government

i. Anti-Corruption Policy Includes Prohibition on Gifts to Government Officials and Employees

You are prohibited from giving, offering, promising, soliciting or agreeing to receive, accepting, or authorizing, a gift or anything of value, whether tangible or intangible, to or from a third party, including government officials, in contravention of the Company's Anti- Corruption Policy as further described below. This prohibition includes such actions taken with respect to government officials, political parties, party officials or candidates for political office. Such actions may be in violation of the U.S. Foreign Corrupt Practices Act (the "FCPA"), the U.K. Bribery Act of 2010 (the "Bribery Act"), and the laws of many other countries.

You are prohibited from providing gifts, meals or anything of value to government officials or employees, including employees of city, state or municipal entities or their pension plans, or members of their families without prior written approval from Compliance Personnel.

ii. Political Contributions and Activities

Laws of certain jurisdictions, including applicable anti-bribery laws as well as the Company's anti-corruption policy, may prohibit the use of Company funds, assets, services, or facilities on behalf of a political party or candidate. Payments of Company funds to any political party, candidate or campaign may

be made only if permitted under applicable law and approved in writing and in advance by Compliance Personnel.

In addition, your work time may be considered the equivalent of a contribution by the Company. Therefore, you will not be paid by the Company for any time spent running for public office, serving as an elected official, or campaigning for a political candidate. Nor will the Company compensate or reimburse you, in any form, for a political contribution that you intend to make or have made.

iii. Lobbying Activities

Laws of some jurisdictions require registration and reporting by anyone who engages in a lobbying activity. Generally, lobbying includes: (a) communicating with any member or employee of a legislative branch of government for the purpose of influencing legislation; (b) communicating with certain government officials for the purpose of influencing government action; or (c) engaging in research or other activities to support or prepare for such communication.

So that the Company may comply with lobbying laws, you must notify Compliance Personnel before engaging in any activity on behalf of the Company that might be considered "lobbying" as described above.

iv. Bribery of Foreign Officials

Company policy, the FCPA, the Bribery Act, and the laws of many other countries prohibit the Company and its directors, officers, employees, or agents from giving or offering to give money or anything of value to a foreign official, a foreign political party, a party official or a candidate for political office in order to influence official acts or decisions of that person or entity, to obtain or retain business, or to secure any improper advantage. A foreign official is an officer or employee of a government or any department, agency, or instrumentality thereof, or of certain international agencies, such as the World Bank or the United Nations, or any person acting in an official capacity on behalf of one of those entities. Officials of government-owned corporations are considered to be foreign officials.

Payments need not be in cash to be illegal. The FCPA prohibits giving or offering to give "anything of value." Over the years, many non-cash items have been the basis of bribery prosecutions, including travel expenses, golf outings, automobiles, and loans with favorable interest rates or repayment terms. Indirect payments made through agents, contractors, or other third parties are also prohibited. You cannot avoid liability by "turning a blind eye" when circumstances indicate a potential violation of the FCPA.

The Company strictly prohibits you from giving, offering, promising, soliciting or agreeing to receive, accepting, or authorizing, a gift or anything of value, whether tangible or intangible, to or from a third party, which could reasonably be considered an attempt to gain an unfair business advantage or which would otherwise reflect poorly on the Company. The Company takes a "zero-tolerance" approach with regards to violations of this anti-corruption policy. To be clear, you are prohibited from using personal funds or resources to engage in an activity that is otherwise prohibited if done with funds or resources of the

Company. Furthermore, the Company mandates that its books and accounting records be maintained so that that they accurately and fairly reflect all transactions and dispositions of each of their assets.

v. Compliance with Applicable Securities Laws

In addition to the general principles of conduct stated in this Code and the specific trading restrictions and reporting requirements described in applicable Company personal trading policies, this Code requires that you comply with applicable federal securities laws. These laws include the Securities Act of 1933 (the "Securities Act"), the Exchange Act, the Sarbanes-Oxley Act of 2002, the Investment Company Act of 1940, the Investment Advisers Act of 1940, Title V of the Gramm-Leach-Bliley Act of 1999, any rules adopted by the Securities and Exchange Commission under any of these statutes, the Bank Secrecy Act as it applies to private investment funds and investment advisers, and any rules adopted thereunder by the Securities and Exchange Commission or the Department of the Treasury.

C. Implementation of the Code

i. Responsibilities

While each of us is individually responsible for putting the Code to work, we need not go it alone. The Company has a number of resources, people and processes in place to answer your questions and guide you through difficult decisions.

Additional copies of this Code are available from Compliance Personnel and on the Company's website.

ii. Seeking Guidance

This Code cannot provide definitive answers to all questions. If questions arise regarding any of the policies discussed in this Code or if any doubt arises as to the best course of action in a particular situation, the Company's directors, officers, and employees should seek guidance from their supervisors or from Compliance Personnel.

iii. Reporting Violations

In the case of known or suspected violations of applicable laws or regulations, the Code, or any of the Company's related policies, the Company's directors, officers, and employees must immediately report that information to their supervisors or Compliance Personnel. No one will be subject to retaliation because of a good faith report of suspected misconduct. In addition, the Company has adopted a Whistleblower Policy which is available on the Company's website.

iv. Investigations of Suspected Violations

All reported violations will be promptly investigated and treated confidentially to the greatest extent possible. It is imperative that reporting persons not conduct their own preliminary investigations. Investigations of alleged

violations may involve complex legal issues, and acting on your own may compromise the integrity of an investigation and adversely affect you and the Company.

v. Discipline for Violations

The Company intends to use every reasonable effort to prevent the occurrence of conduct not in compliance with this Code and to halt any such conduct that may occur as soon as reasonably possible after its discovery. Persons who violate this Code or other Company policies and procedures may be subject to disciplinary actions, up to and including termination of their association with the Company. In addition, similar disciplinary measures may also be taken against anyone who directs or approves infractions or has knowledge of them and does not promptly report and correct them in accordance with Company policy.

vi. Waivers of the Code

The Company will waive application of the policies set forth in this Code only where circumstances warrant granting a waiver, and then only in conjunction with an appropriate monitoring of the particular situation. Waivers of this Code for directors or executive officers of public companies managed by affiliates of the Company may be made only by the board of directors as a whole or the audit committee of the board of such companies, and must be promptly disclosed as required by law or regulation. Similarly, waivers of this Code for the Company's directors or executive officers may be made only by our Board of Directors as a whole or the Audit Committee of our Board, and must be promptly disclosed as required by law or regulation.

vii. No Rights Created

This Code is a statement of the fundamental principles and key policies and procedures that govern the conduct of Company employees, directors, and officers. It is not intended to and does not create any rights in any employee, officer, director, person with whom the Company has a business relationship, competitor, investor or any other person or entity.

viii. Remember

Ultimate responsibility to assure that we as a company comply with the many laws, regulations and ethical standards affecting our business rests with each of us. You must become familiar with and conduct yourself strictly in compliance with those laws, regulations and standards and the Company's policies and guidelines pertaining to them.

Credit Card Environment and Processing Policy

Policy Owner: IT Security and Data Privacy
Version: 20250101
Employee Scope: All US employees from all environments involved in the processing of credit card data

Purpose

The purpose of this policy is to outline the required practices for the storing, processing, and transmitting of credit card data that will enable Gannett to comply with the Payment Card Industry Data Security Standard (PCI DSS) for Gannett and third-party systems, devices, networks, applications, and processes that are in scope to report PCI DSS compliance.

Definitions and Acronyms

When navigating this policy, it's important to grasp the terminology. Our Glossary of Cybersecurity Terms provides concise definitions for key concepts.

Scope

This policy applies to (1) all credit card data and (2) all environments involved in the processing of credit card data including Gannett and third-party environments, both for physical card-present transactions and computerized transactions including all relevant systems, networks, applications, devices, and processes (the "Cardholder Data Environment" or "CDE").

Policy

General

- Accountability for maintaining PCI DSS compliance is a shared responsibility among these key groups:
  - Finance Division
  - Information Security
  - Owners of systems or applications that store, transmit or process credit card data.
- Network segmentation must be established for networks/systems determined to be part of the CDE to ensure PCI DSS compliance.
- An annual security risk assessment must be completed for all in-scope elements of the CDE to ensure PCI DSS compliance.
- The cardholder's name, primary account number (PAN), and expiration date are only stored for legitimate business purposes Storage of CVV2, track data or pin block data (sensitive authentication data) is prohibited.
- The retention of cardholder data should be limited to that required for legitimate business purposes and regulatory requirements.
- Credit card numbers must be encrypted wherever they are stored or transmitted from Gannett Systems, and the full number must be masked when displayed on any Gannett or third-party user screens, reports, statements, or other documents.
- Sensitive authentication data should not be stored after authentication and should be rendered unrecoverable once the authorization process has been completed.

- Only individuals with a documented and approved business requirement can access the full unencrypted credit card account number described in the Data Protection Policy.
- A list of roles with an approved business requirement to access the full unencrypted credit card account number shall be maintained and reviewed annually.
- Gannett personnel accessing any part of the PCI DSS Environment must do so using company-owned equipment.
- All individuals with incident response job responsibilities will receive annual training on incident response procedures specific to credit card data.

Audit Logs and Security Events

- Audit logs must be enabled in the CDE as required by PCI DSS.
- Audit trail files must be secured to prevent unauthorized modifications through access control mechanisms, physical segregation, and/or network segregation to ensure completeness, accuracy, and integrity.
- Access to audit trail files should be limited to authorized Gannett personnel that need this access to perform their job function's roles and responsibilities.
- Audit trail files should be promptly saved to a secured, centralized log server or media that is difficult to alter.
- File-integrity monitoring or change detection software is required for audit logs.
- Where applicable, audit logs for external-facing technologies such as wireless, firewalls and DNS should be written to a secure, centralized, internal log server or media.
- A process must be in place to review logs, at least daily, for unauthorized access to the CDE including:
  - Review of all security events.
  - Logs of all system components that store, process, or transmit cardholder data.
  - Logs of all servers and system components that perform security functions including firewalls, intrusion detection/intrusion prevention systems (IDS/IPS) authentication servers, e-commerce redirection servers.
- Audit logs must be retained at a minimum for one year and with at least three months immediately available online.
- Procedures must be in place to address and manage exceptions associated with audit logs and security events identified during the review process.
- Must have a process for the timely detection and reporting of failures of critical security controls including firewalls, IDS/APS, FIM, anti-virus logical access control and segmentation controls.
- Must have a process to periodically review logs, based on the associated risk, for all other system components to identify potential issues or unauthorized access to sensitive data through other systems components.

Secure Transmission

- Inbound and outbound transmissions of cardholder data must use an encrypted/secure protocol for transport including SFTP (Secure File Transfer Protocol), FTP/S, and HTTPS.
- Key encryption keys generated and used as part of the CDE must, at a minimum, be as strong as the data-encrypting keys they protect.

- Only trusted keys and certificates are accepted in the transmission of cardholder data across open, public networks.
- The encryption strength used for the transmission of cardholder data over open, public networks must be appropriate for the encryption methodology in use.
- The transmission protocol must be configured to use only secure configurations and not accept insecure versions or configurations.
- Unprotected PANs (primary account numbers) must not be sent via end-user messaging technologies.

Securing Card-Swipe Devices

- A list of card-swipe devices shall be maintained.
- Card-swipe devices will be periodically inspected for signs of tampering or substitution.
- Training will be provided to Gannett personnel with authorized access to card- swipe devices to recognize suspicious behavior and report tampering or substitution of devices.

Enforcement and Exception

- Compliance with this policy is required under Gannett's Information Security Policies and Standards Enforcement Policy and Gannett may take actions in response to non-compliance as provided under the Enforcement Policy.
- Any exceptions to this policy must follow Gannett's Information Security Policies and Standards Exceptions Policy.

This policy may be updated occasionally by the Company. The current version of this policy, and the other policies referenced in this document, may be viewed on MyLife@Gannett.

Cybersecurity Incident Reporting Policy

Policy Owner: IT Security and Data Privacy
Version: 20250101
Employee Scope: All US employees from all Company business units and affiliates of the Company (including Joint Operating Agencies and joint ventures that use Gannett Systems).

Purpose

This policy describes how to report suspicious activity and cybersecurity Events (as defined below under Policy – Definitions).

Gannett policy requires all suspicious activity and cybersecurity Events to be reported internally, and applicable laws and regulations may require cybersecurity Incidents (as defined below under Policy – Definitions) to be reported to those impacted and/or to regulators.

Gannett has a Cybersecurity Incident Response Plan for responding to Incidents, which is posted at MyLife@Gannett.

Definitions and Acronyms

When navigating this policy, it's important to grasp the terminology. Our Glossary of Cybersecurity Terms provides concise definitions for key concepts.

Scope

This policy covers all Gannett Systems and networks, including resources used for the collection, processing, routing, maintenance, use, sharing, dissemination, or disposition of electronic information. This includes Gannett managed cloud platforms, and vendor provided cloud services (SaaS) and other vendor service types that access Gannett owned or managed data.

Policy

Reporting and Response

Cybersecurity Events must be reported as follows:

1. Everyone at Gannett has a responsibility to report suspicious activity and cybersecurity Events immediately to the appropriate authority.
   a. Report cybersecurity Events or suspicious activity to byteback@gannett.com.
   b. Urgent Events:
      - Use the high importance flag on your email for urgent 24x7x365 response.
      - If the email system is not working, escalate to your manager.
2. Gannett's Cybersecurity Incident Response Team (CIRT) will review Events reported and respond appropriately to determine whether any of these Events should be identified as an Incident as defined above.

Enforcement and Exception

- Compliance with this policy is required under Gannett's Information Security Policies and Standards Enforcement Policy and Gannett may take actions in response to non-compliance as provided under the Enforcement Policy.
- Any exceptions to this policy must follow Gannett's Information Security Policies and Standards Exceptions Policy.

This policy may be updated occasionally by the Company. The current version of this policy, and the other policies referenced in this document, may be viewed on MyLife@Gannett.

Data Backup Policy

Policy Owner: IT Security and Data Privacy
Version: 20250101
Employee Scope: All employees who work with data stored on any Gannett owned or licensed electronic device or Gannett controlled cloud environment at all Gannett business units

Purpose

- The Data Backup Policy exists to make certain that applications and data can be recovered if lost or damaged and to provide the basic building blocks for business continuity.
- This policy will provide guidance for backup storage locations and access controls.

Scope

The scope of this policy includes data stored on any Gannett owned or licensed electronic device or Gannett controlled cloud environments at all Gannett business units.

Definitions and Acronyms

When navigating this policy, it's important to grasp the terminology. Our Glossary of Cybersecurity Terms provides concise definitions for key concepts.

Policy

- Vendor backup and data retention policies for vendor-hosted software as a service (SaaS) system must be reviewed for compliance with the F/ARM Financial Accounting and Reporting Manual, as applicable.
- Each location that is designated as a backup location must have a documented backup and restore plan for their electronic systems that are necessary for their business operations and compliant with the F/ARM Financial Accounting and Reporting Manual, as applicable.
- The backup and restore plan must include the appropriate procedures for off-site storage and recovery of backed up systems or data.
    - Storage of backup media in an employee's or individual independent contractor's car or home is not acceptable off-site storage and is prohibited.
    - Off-site storage should provide industry standard environmental and physical security.
    - See the Data Protection Policy for policy on classification, storage and transport of backup media containing sensitive data.
    - Distribution controls should be in place to ensure that all backup media is logged and sent via an auditable delivery method to internal and/or external users.
- Each location that is designated as a backup location must follow their written backup plan.
- A review of backup schedules and retention periods (SLAs) must be in place to confirm compliance with the Record Retention Policy; necessary remediation of non- compliant SLAs must be performed and logged.
- Each location designated as a backup location must periodically (at least annually) test

their restore procedures for all systems where practical.
- Each location must review the backup storage location security at least annually.
- Only individuals authorized by appropriate management are responsible for backup management and offsite media processes.
- Each location must periodically review the media/data inventory at least annually.
- The Data Erasure Standard shall govern media and document destruction standards.

Enforcement and Exception

- Compliance with this policy is required under Gannett's Information Security Policies and Standards Enforcement Policy and Gannett may take actions in response to non-compliance as provided under the Enforcement Policy.
- Any exceptions to this policy must follow Gannett's Information Security Policies and Standards Exceptions Policy.

This policy may be updated occasionally by the Company. The current version of this policy, and the other policies referenced in this document, may be viewed on MyLife@Gannett.

Data Protection Policy

Policy Owner: IT Security and Data Privacy
Version: 20250101
Employee Scope: All US employees who work with all data on Gannett Information Technology (IT) Systems in all Gannett locations.

Purpose

This policy identifies the responsibility for the authority that owns or controls certain Gannett data ("Data Authority") to (1) determine the sensitivity level of Gannett customer, employee, and other information and (2) take actions to protect that data from unauthorized access based on the determined sensitivity level. The data covered by this policy comprises certain information owned, managed, or retained by Gannett that requires a higher level of data protection and access controls (collectively, "Sensitive Data"). Sensitive Data may include data in the following categories:

1. **Non-Public Company Information (NPI):** The Company's sensitive, confidential, trade secret, proprietary business and financial information and confidential non-public client information which if disclosed in an unauthorized manner could cause a material adverse impact to the Company's business operations, finances, reputation, and/or security (excluding PI (Personal Information) and PHI (Protected Health Information) as defined below).
2. **Personal Information (PI):** "Personal Information" or "Personal Data" as used in Section 9 of the Gannett Privacy Policy and as defined under applicable data privacy laws, means any information that identifies, relates to, describes, references, or is reasonably capable of being associated with an identified or identifiable natural person.
3. **Protected Health Information (PHI)** (a subset of PI)**:** Information or data concerning an individual's health condition, provision of health care or payment for the provision of health care, including protected health information as defined by 45 CFR 160.103
4. **Sensitive Personal Information** (a subset of PI): Information or data defined as "special category data"" or "sensitive data" under various data protection laws that require additional protection and/or grant additional rights to data subjects as to the collection or processing of such information or data, for example, ethnicity, political affiliation, (new laws may come into effect that add other types of sensitive personal information, please consult Gannett Legal if you have any questions about whether particular data elements qualify as Sensitive Personal Information).

Definitions and Acronyms

When navigating this policy, it's important to grasp the terminology. Our Glossary of Cybersecurity Terms provides concise definitions for key concepts.

Scope

This policy covers all data on Gannett Information Technology (IT) Systems in all Gannett locations (see Glossary).

Policy

All Gannett company data (regardless of level of data sensitivity) must not be stored on personally owned devices, including but not limited to home computers, removable storage devices and mobile devices unless the device has a Company issued device management tool installed.

Sensitivity levels are to be determined by the data element(s) that make up the information. Level 1 applies to information with the highest amount of sensitivity. Level 4 applies to information with the lowest amount of sensitivity.

Level 1 — Highest Sensitivity Requiring Encryption in Transit and at Rest

Data regarded as highly sensitive and/or critical to the Company, where unauthorized access, modification, disclosure, or destruction of such data would constitute great harm to Gannett and/or would require notice to individuals or other third parties under applicable law including:

- NPI data that is required by applicable legislation or governmental authorities, industry governing bodies (such as NIST (National Institute of Standards and Technology), ISO, PCI (Payment Card Industry)) and/or internal compliance controls to require encryption both at rest and in transit
- PHI and PI data, where required by applicable privacy legislation, contractual obligations and/or compliance controls

Examples of Level 1 – Highest Sensitivity

- Name and Social Security Numbers (SSN) or last four numbers of an individual's SSN
- Payment card cardholder data
- Any information defined as Sensitive Personal Information under applicable data privacy laws such as ethnic, race, religion, culture, political views, sexual orientation.

Minimum standard protection requirements

- Must be encrypted when transmitted and stored.
- Backup media must have appropriate physical security during in-house storage, in transit and at off-site facilities.
- Must be properly marked both at rest in Gannett databases and when physically in transit and at off-site facilities.
- Confidential data should be labeled "confidential" whenever paper copies are produced for distribution.
- In addition to the above requirements, credit card data has specific requirements for protection as defined within the Payment Card Industry-Data Security Standard (PCI-DSS). As a Level 1 merchant, Gannett is required to comply with the following:
  a. Only individuals with a documented and approved business requirement can access the full unencrypted credit card account number. Access is defined as the ability to view or programmatically access the full credit card account number.
  b. Credit card account numbers must be masked.
  c. Storage of CVV2, track data or PIN block data is prohibited.
  d. Test or development systems must never use actual credit card numbers. Only dummy credit card numbers may be used.

e. Non-electronic documents containing card account numbers must be destroyed by cross shredding.
f. Copying, moving, or storing of credit card account numbers to local hard drives or removable electronic media is prohibited without appropriate authorization by IT Compliance and Security leadership (including Gannett's PCI Internal Security Assessor).
g. In addition, Gannett has processes in place to prevent the transmission of emails or sharing of OneDrive or SharePoint documents that contain sensitive information such as credit card numbers or social security numbers.

Level 2 — High Sensitivity Requiring Encryption in Transit Only
Confidentiality of data is preferred, but information contained in data may be subject to open records disclosure.

Examples of Level 2 – High Sensitivity
- Non-Published Financial forecasting data
- Information such as IP (Internet Protocol) Address, Device ID, email address, phone number, home address that is linked to an individual.
- Employee termination data or performance reports

Minimum standard protection requirements
- Requires Encryption in Transit Only. Data should be encrypted when transmitted across a network.
- Confidential data should be labeled "confidential" whenever paper copies are produced for distribution.
- Backup media containing high sensitivity data must have appropriate physical security during in-house storage, in transit and at off-site facilities.

Level 3 — Moderate Sensitivity
Level 3 data that is important to Gannett and not typically publicly available, and therefore must be protected against acts that are malicious and/or destructive. However, disclosure problems are usually not significant.

Examples of Level 3 – Moderate Sensitivity
- Customer's purchasing propensity data
- Aggregated or Pseudonymous

Minimum standard protection requirements
- Level 3 data should have appropriate measures to protect against unauthorized use, access, or modification. Appropriate protection measures are determined by the applicable Data Authority in consultation with IT Compliance, Security and/or Legal, Labor and HR (Human Resources) as needed.

Level 4 — Low Sensitivity
Data that requires no protection, or a minimal amount of protection. This level includes information that is publicly available. At this level, any disclosures could be expected not to have an adverse effect.

Examples of Level 4 – Low Sensitivity
- Content containing public information such as state employee salaries or public criminal records.
- Company registration number or email that does not contain personal data like info@company.com
- Anonymized data

Minimum standard protection requirements
- Level 4 data should have appropriate measures to protect against unauthorized use, access, or modification. Appropriate protection measures are determined by the applicable Data Authority in consultation with IT Compliance and Security and/or Legal, Labor and HR as needed.

The minimum standard protection requirements for each sensitivity level of data when being used or handled in a specific context (e.g., Sensitive Data sent in an email message). Please note that these protection standards are not intended to supersede any regulatory or contractual requirements for handling data. Some specific data sets, such as employee records data, credit/debit card data, healthcare data, and financial account data, may have stricter requirements in addition to the minimum standard requirements.

Data Retention
Data should only be retained for as long as it is required to achieve the purpose for which the data was collected and is being processed.
Internal data retention, where Gannett is the data controller, shall be governed by the Record Retention Policy and Gannett Data Privacy Policy.
Data retention, where Gannett is the data processor, shall be governed by the Data Processing Agreement signed by the data controller and the data processor.
Gannett shall honor the Data Subject Rights covered by state, federal and regional legislation based on the location of the Data Subject including, but not limited to data access, data deletion, data correction.
Gannett shall ensure that all restricted and confidential data is securely deleted from company devices prior to, or at the time of, disposal.

Enforcement and Implementation
Roles & Responsibilities
- It is the responsibility of the appropriate Data Authority in consultation with Gannett Legal as needed to classify a sensitivity level for Sensitive Data on IT Systems to ensure that appropriate security measures and access controls are in place.
- It is the responsibility of the Data Authority to communicate the appropriate sensitivity level and any associated business rules to the data custodian(s) who are responsible

for the safe custody, transport and storage of Sensitive Data and implementation of the business rules based on the designated sensitivity level.
- The Data Authority is responsible for limiting the collection of personal information to what is necessary for the business purpose(s) identified and ensuring it is collected by fair and lawful means.

Enforcement and Exception

- Compliance with this policy is required under Gannett's Information Security Policies and Standards Enforcement Policy and Gannett may take actions in response to non-compliance as provided under the Enforcement Policy.
- Any exceptions to this policy must follow Gannett's Information Security Policies and Standards Exceptions Policy.

This policy may be updated occasionally by the Company. The current version of this policy, as well as policies referenced in this document, may be viewed on MyLife@Gannett.

Endpoint Protection Policy

Policy Owner: IT Security and Data Privacy
Version: 20250101
Employee Scope: All US employees who work with all Gannett Endpoints that are used by Gannett personnel (including employees, contractors, and/or third parties who access Gannett Resources where Gannett provides Endpoints) at any Gannett facility, that have access to Gannett networks, or that store any Gannett information.

Purpose

This policy establishes the requirements for malware detection, host-based Intrusion Detection Systems (IDS)/Intrusion Prevention Systems (IPS), Endpoint protection, and Endpoint detection and response capabilities (EDR) on Gannett Endpoints (as defined below).

- Malware and compromised devices can expose Gannett to risks, including lost productivity, data loss, compromise of network environment, host computer systems and services, reputational harm, and legal action.
- Endpoints are any remote computing device that communicates back and forth with a network to which it is connected including but not limited to, servers and end-user devices (workstations, tablets, laptops, and mobile devices).
- Agents are dedicated software program deployed to each endpoint.

Definitions and Acronyms

When navigating this policy, it's important to grasp the terminology. Our Glossary of Cybersecurity Terms provides concise definitions for key concepts.

Policy

Malware Detection

Endpoints must have technology (either Agents that reside on the device or scanning by technology external to the device) to detect malware in real time or on a scheduled basis.

Host based IDS/IPS

Technology to monitor and analyze network traffic, processes running on the systems, and modifications to files to detect anomalies and prevent compromises.

Endpoint Protection

- Agents are to be installed on Endpoints to detect malware and malicious behaviors.
- Agents are required to be on a vendor supported version for the latest threat detection capabilities.
- Endpoints should support full system encryption in accordance with Gannett's Acceptable Encryption Policy.

Endpoint Detection and Response (EDR)

- Agents must be installed on devices for threat investigations and to support malicious Indicator of Compromise (IOC) hunting activity.
- Agents must support USB blocking and network quarantine.

Threat Detection

- Malicious threat
  - When a malicious threat (for example, known malware) is detected, the policy action should kill and quarantine.
- Suspicious threat
  - When a suspicious threat (for example, some unexpected or unusual activity) is detected, the policy action should alert for analysis.
- Threat Exceptions
  - In the event endpoint protection or EDR agents cannot be installed, there must be a documented and approved exception in accordance with the Information Security Exception Policy.
  - Exceptions must have compensating controls and/or associated risk mitigations.

Enforcement and Exception

- Compliance with this policy is required under Gannett's Information Security Policies and Standards Enforcement Policy and Gannett may take actions in response to non-compliance as provided under the Enforcement Policy.
- Any exceptions to this policy must follow Gannett's Information Security Policies and Standards Exceptions Policy.

This policy may be updated from time to time by the Company. The current version of this policy, as well as other referenced policies, may be viewed on MyLife@Gannett.

Equal Opportunity

Policy Owner: Human Resources
Version: 20230911
Employee Scope: All new employees

Policy

Gannett is committed to equal opportunity for all. We are committed to building a company whose people reflect the true diversity of our community. The company's goal is to recruit, hire and maintain a diverse workforce. Equal employment opportunity is not only good business, but it is the law. All personnel actions, including, but not limited to, recruitment, selection, hiring, training, transfer, promotion, termination, compensation and benefits conform to this basic policy.

We provide equal employment opportunities to all qualified applicants and employees without regard to actual or perceived sex (including pregnancy, childbirth, breastfeeding or related medical conditions), race, religion (including religious dress and grooming practices), color, gender (including gender identity and gender expression), national origin or ancestry, physical or mental disability, medical condition, genetic information, genetic predisposition or carrier status, height, weight, marital status, familial status, registered domestic partner status, age, union membership status, enrollment in any public assistance program, sexual orientation, military and veteran status or any other basis protected by federal, state, local law, ordinance or regulation.

Legal Disclaimer: Nothing in this policy shall be construed as creating any contract (express or implied), duty or obligation on the part of the company to take any actions beyond those required of an employer by existing law. Gannett reserves the right to amend, modify or cancel this policy at any time, at Gannett's sole discretion.

Nothing in this policy shall apply to conduct that is protected under applicable federal, state, or local laws. To the extent that any provision in this policy is inconsistent with federal, state or local law, then the applicable federal, state or local law takes precedence over this policy. Adherence to this policy is required by all employees. When there is a conflict between the language of this policy and a local Collective Bargaining Agreement (CBA), the CBA may take precedence with regard to members of the applicable, local collective bargaining unit.

Financial Application Software Development Policy

Policy Owner: IT Security and Data Privacy
Version: 20250101
Employee Scope: All US employees making software changes of any kind including without limitation, new development, modifications, enhancements, updates and/or support related development.

Purpose

This policy is being implemented to protect Gannett from unauthorized, malicious, or faulty modifications to financial application software.

Definitions and Acronyms

When navigating this policy, it's important to grasp the terminology. Our Glossary of Cybersecurity Terms provides concise definitions for key concepts.

Scope

- This policy covers Gannett software changes of any kind including without limitation, new development, modifications, enhancements, updates and/or support related development such as bug fixes ("Development") that are done by Gannett employees, contractors or other third parties.
- The applications in scope are only those defined as "**Key Financial Applications** K," which are applications where
  - the copyright belongs to Gannett or the configuration or other administrative functions are controlled by Gannett and
  - significant financial processing occurs, (such as where required for SOX (Sarbanes-Oxley) compliance as defined by Gannett and 3rd party auditors) and
  - the application can add, alter, or delete financial source data, and/or involve the reporting of financial source data, and/or execute within the PCI (Payment Card Industry) cardholder data environment.

Policy

Development associated with Key Financial Applications must follow the Financial Application Development Standard. This standard addresses the following Development phases:

- Project initiation
- Planning and Analysis
- Design Requirements
- Design
- Development
- Testing
- Training
- Deployment
- Cutover

Please see the System and Software Implementation and Development Standard for a

detailed breakdown of Development steps and deliverables required when performing Development associated with Key Financial Applications.

PCI Policy

For Key Financial Applications that are in-scope for the Payment Card Industry Data Security Standards (PCI DSS), Development must be based on industry standards and best practices and must be compliant with the current version of the PCI DSS-without exception:

Requirement 6: Develop and Maintain Secure Systems and Software.

6.1 Processes and mechanisms for developing and maintaining secure systems and software are defined and understood.

6.1.1 All security policies and operational procedures that are identified in Requirement 6 are:

- Documented.
- Kept up to date.
- In use.
- Known to all affected parties

6.1.2 Roles and responsibilities for performing activities in Requirement 6 are documented, assigned, and understood.

6.2 Bespoke and custom software are developed securely.

6.2.1 Bespoke and custom software are developed securely, as follows:

- Based on industry standards and/or best practices for secure development.
- In accordance with PCI DSS (for example, secure authentication and logging).
- Incorporating consideration of information security issues during each stage of the software development lifecycle.

6.2.2 Software development personnel working on bespoke and custom software are trained at least once every 12 months as follows:

- On software security relevant to their job function and development languages.
- Including secure software design and secure coding techniques.
- Including, if security testing tools are used, how to use the tools for detecting vulnerabilities in software.

6.2.3 Bespoke and custom software is reviewed prior to being released into production or to customers, to identify and correct potential coding vulnerabilities, as follows:

- Code reviews ensure code is developed according to secure coding guidelines.
- Code reviews look for both existing and emerging software vulnerabilities.
- Appropriate corrections are implemented prior to release.

6.2.3.1 If manual code reviews are performed for bespoke and custom software prior to release to production, code changes are:

- Reviewed by individuals other than the originating code author, and who are knowledgeable about code-review techniques and secure coding practices.
- Reviewed and approved by management prior to release.

6.2.4 Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attacks and related vulnerabilities in bespoke and custom software, including but not limited to the following:

- Injection attacks, including SQL, LDAP, XPath, or other command, parameter, object, fault, or injection-type flaws.
- Attacks on data and data structures, including attempts to manipulate buffers, pointers, input data, or shared data.
- Attacks on cryptography usage, including attempts to exploit weak, insecure, or inappropriate cryptographic implementations, algorithms, cipher suites, or modes of operation.
- Attacks on business logic, including attempts to abuse or bypass application features and functionalities through the manipulation of APIs, communication protocols and channels, client side functionality, or other system/application functions and resources. This includes cross-site scripting (XSS) and cross-site request forgery (CSRF).
- Attacks on access control mechanisms, including attempts to bypass or abuse identification, authentication, or authorization mechanisms, or attempts to exploit weaknesses in the implementation of such mechanisms.
- Attacks via any "high-risk" vulnerabilities identified in the vulnerability identification process, as defined in Requirement 6.3.1.

6.3 Security vulnerabilities are identified and addressed.
6.3.1 Security vulnerabilities are identified and managed as follows:

- New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs).
- Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact.
- Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment.
- Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.

6.3.2 An inventory of bespoke and custom software, and third-party software components incorporated into bespoke and custom software is maintained to facilitate vulnerability and patch management.
6.3.3 All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows:

- Patches/updates for critical vulnerabilities (identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release.
- All other applicable security patches/updates are installed within an appropriate time frame as determined by the entity's assessment of the criticality of the risk to the environment as identified according to the risk ranking process at Requirement 6.3.1.

6.4 Public-facing web applications are protected against attacks.
6.4.1 For public-facing web applications, new threats and vulnerabilities are addressed on an ongoing basis and these applications are protected against known attacks as follows:

- Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods as follows:

  - At least once every 12 months and after significant changes.
  - By an entity that specializes in application security.
  - Including, at a minimum, all common software attacks in Requirement 6.2.4.
  - All vulnerabilities are ranked in accordance with requirement 6.3.1.
  - All vulnerabilities are corrected.
  - The application is re-evaluated after the corrections.

OR

- Installing an automated technical solution(s) that continually detects and prevents web-based attacks as follows:
  - Installed in front of public-facing web applications to detect and prevent web-based attacks.
  - Actively running and up to date as applicable. – Generating audit logs.
  - Configured to either block web-based attacks or generate an alert that is immediately investigated.

6.4.2 For public-facing web applications, an automated technical solution is deployed that continually detects and prevents web-based attacks, with at least the following:

- Is installed in front of public-facing web applications and is configured to detect and prevent web-based attacks.
- Actively running and up to date as applicable.
- Generating audit logs.
- Configured to either block web-based attacks or generate an alert that is immediately investigated.

6.4.3 All payment page scripts that are loaded and executed in the consumer's browser are managed as follows:

- A method is implemented to confirm that each script is authorized.
- A method is implemented to assure the integrity of each script.
- An inventory of all scripts is maintained with written business or technical justification as to why each is necessary.

6.5 Changes to all system components are managed securely.

6.5.1 Changes to all system components in the production environment are made according to established procedures that include:

- Reason for, and description of, the change.
- Documentation of security impact.
- Documented change approval by authorized parties.
- Testing to verify that the change does not adversely impact system security.
- For bespoke and custom software changes, all updates are tested for compliance with Requirement 6.2.4 before being deployed into production.
- Procedures to address failures and return to a secure state.

6.5.2 Upon completion of a significant change, all applicable PCI DSS requirements are confirmed to be in place on all new or changed systems and networks, and documentation is updated as applicable.

(each of the following activities, at a minimum, has potential impacts on the security of the CDE and must be considered and evaluated to determine whether a change is a significant change for an entity in the context of related PCI DSS requirements:

- New hardware, software, or networking equipment added to the CDE.

- Any replacement or major upgrades of hardware and/or software in the CDE.
- Any changes in the flow or storage of account data.
- Any changes to the boundary of the CDE and/or to the scope of the PCI DSS assessment.
- Any changes to the underlying supporting infrastructure of the CDE (including, but not limited to, changes to directory services, time servers, logging, and monitoring).
- Any changes to third-party vendors/service providers (or services provided) that support the CDE or meet PCI DSS requirements on behalf of the entity).

6.5.3 Pre-production environments are separated from production environments and the separation is enforced with access controls.
6.5.4 Roles and functions are separated between production and pre-production environments to provide accountability such that only reviewed and approved changes are deployed.
6.5.5 Live PANs are not used in pre-production environments, except where those environments are included in the CDE and protected in accordance with all applicable PCI DSS requirements.
6.5.6 Test data and test accounts are removed from system components before the system goes into production.

- Security patches and software modifications are documented as described in the Change Management Policy.

Enforcement and Exception

- Compliance with this policy is required under Gannett's Information Security Policies and Standards Enforcement Policy and Gannett may take actions in response to non-compliance as provided under the Enforcement Policy.
- Any exceptions to this policy must follow Gannett's Information Security Policies and Standards Exceptions Policy.

This policy may be updated occasionally by the Company. The current version of this policy, and other policies referenced in this document, may be viewed on MyLife@Gannett.

Gannett Accounts Payable Policy

Policy Owner: Finance
Version: 20241015
Employee Scope: All US and Canada payments processed via Infor Payables, HSBC, Concur Expense or to individuals or firms who are not employees of the company and does not apply to payroll-related payments

1. Introduction:

Gannett's Shared Services Center (SSC) is responsible for all US and Canada supplier's invoices and payments, as well as the employee expense reimbursement submission process as outlined below. The Accounts Payable team within the SSC is available to assist new managers and employees that may need assistance with Gannett's invoice to pay process, expense reporting or other accounts payable related needs.

You can contact the SSC by email for the following needs:

1. Accounts Payable: aphelpdesk@support.gannett.com
2. General Ledger: NSSC-GL@gannett.com
3. Procurement Card Support: cardsupport@gannett.com
4. Expense Report Support: expensereports@gannett.com

AP related links, forms and instructional documents may be found here (The Hub - INFOR). Internal controls are documented in the Internal Controls Portal (ICP) for Accounts Payable.

The Accounts Payable Policies referred herein apply to all US and Canada payments processed via Infor Payables, HSBC, Concur Expense or to individuals or firms who are not employees of the company and does not apply to payroll-related payments. These policies are not intended to address every conceivable situation or replace the sound judgment of the accounting staff that is confronted with the day-to-day decisions.

In addition to this policy, certain processes and responsibilities identified herein may also be governed by other Gannett policies and procedures available at Mylife@Gannett link.

1. Procurement Policy and all Procurement Policy Notices
2. Request For Proposal (RFP) Policy
3. Travel Policy

The policies noted below establish standards for approving and paying invoices in an efficient and economical fashion with no diminishment of internal control.

2. Authoritative Literature:

ASC 405-20, Extinguishments of Liabilities, addresses the extinguishment of liabilities.

3. Definitions:

Infor Payables - Our invoice approval workflow and payment processing solution used across the organization to support our daily procure to pay activities. This system is managed by the SSC. Infor may be accessed through Okta, the Single Sign On (SSO) platform.

Coupa – Coupa is a procurement application that provides Gannet with a cloud-based spend management tool. Coupa facilitates compliance with purchasing programs, interfaces with Ceridian and enables one over one approval which ensures that approval chains are followed before orders are placed with suppliers. Coupa can be accessed through Okta, the Single Sign On (SSO) platform.

Concur Expense – Gannett's integrated expense reimbursement and reporting application. Employees with out-of-pocket business expense reimbursement requests or Corporate Credit Card transactions, are required to submit those expenses with appropriate documentation through Concur. Approved out of pocket reimbursement requests will be processed for payment through Corporate Payroll. All approved expenses are passed to the General Ledger. Concur Expense may be accessed through Okta, the Single Sign On (SSO) platform.

Form W-8 – A form that is required for all new international vendors. It is a tax form is filled out by foreign entities (citizens and corporations) and used in order to claim exempt status from certain tax withholdings. The form is also used to declare an entity's status as non-resident alien or foreign national who works outside of the United States.

Form W-9 - A form that is required for all new domestic vendors. The official name is the "Request for Taxpayer Identification Number and Certification" and is used in the United States income tax system by a third party who must file an information return with the Internal Revenue Service (IRS). When required, the information on the Form W-9 and the payments made are reported on a Form 1099.

Gannett Procurement Card - Cards in Accounts Payable used to pay invoices from Infor Payables, rather than issuing payment by check or ACH, or to make point of sale purchases. A Gannett P-Card is the preferred method of payment for all business expenditures. An overview of the Gannett Pcard program can be found here: P-card Program. Questions related to the Gannett Pcard programs may be directed to: cardsupport@gannett.com. P-card policies and card application can be found here: Gannett Expense Management. P-Cards may be used in the following ways:

1. Individual cards in the hands of designated key operating personnel with regular/ongoing purchasing responsibilities
2. Vendor cards held by suppliers with whom we do significant repeat business
3. HSBC virtual card program used by enrolled vendors to collect payment via online banking portal

Gannett Corporate Card – Cards used by employees for travel and entertainment expenses. Expense reports for these payments are processed using Concur Expense.

Symbeo – Our outsourced scanning provider. Vendors may send invoices by mail, email or fax. Symbeo cannot read hand-written information. NOTE: The preferred method of submission is email, which requires invoice attachment in either Word or PDF format. Regardless of method, the billing address should always be formatted with the appropriate site name and mail stop.

Vendor – Refers to suppliers, contractors and consultants providing goods and services to Gannett. For all new vendors, the correct tax form must accompany a new vendor set-up.

4. Procurement and Accounts Payable:

Supplier or Service Provider Invoice Submission

Supplier-provided products and services are an integral component to Gannett business operations. Therefore, it is important to ensure that a clear and consistent invoice submission policy is established. The following policy shall be communicated to all suppliers by the respective Gannett business owner.

To ensure prompt payment, it is required that; 1) supplier to be setup in Infor Payables and be in good standing and meeting expectations; and 2) vendor to submit a proper invoice with applicable line item detail and the following data elements:

1. Correct “Gannett Name” and “Bill to Address” (Full Legal Name of the Gannett Bill to Company required)
2. Full Name of the Gannett employee requesting the goods or services
3. Vendor remit-to address, and billing department email address and telephone number
4. Complete description of goods or services provided, including service period
5. Gannett Purchase Order number (if applicable)
6. Invoice amount in stated currency (USD Only)
7. Corresponding Gannett PO line item number, line item rate, quantity, description and/or material number of good / services delivered (if applicable)
8. Shipping and/or Packing slip reference number (if applicable)
9. Sales, Use, or Value Added (VAT) Tax (if applicable)

If any of the above required invoice detail is omitted or missing, Accounts Payable may withhold payment and/or return the invoice to the vendor for resubmission. Invoices may be sent in either Word or PDF. Multiple invoices can be sent in one document, as long as proper separation between invoices exists (each invoice is clearly marked with an invoice # and the word “Invoice”). Email attachments for multiple invoices or large graphics should be kept under 50 pages or 5 MB.

Our preferred method of invoice submission is email, however postal delivery is permitted.

EMAIL: scanone@gannett.com
US MAIL: Site Name
Mail Stop XXXXXXXX (Company & Business Unit Number)
PO Box 6035
Portland, OR 97228-6035
*Symbeo's name should never be listed in the Bill-To

Supplier Shipping Document Submission
Gannett's purchase of goods includes but is not limited to, parts, material, equipment, tools or supplies. All require proper shipping documents to complete receipt processing. All product shipments to Gannett Facilities require Vendor Packing Slips or Freight Forwarder Shipping Documents.

Shipping documents (e.g. packing slip) for delivered goods to Gannett facilities require the following:
1. Unique shipping and/or packing slip document number
2. Purchase order number (if applicable)
3. PO line item number, Line item detail (i.e. part number, quantity, price, etc.)
4. Name of the Gannett employee requesting the goods

Supplier Payment
Gannett's standard payment terms for good and services is Net 45 days from the date of the invoice. Exceptions to this policy include but are not limited to; subscriber and advertiser refunds as well as newspaper delivery contractor payments, payments for utilities and tax obligations which are paid immediately upon approval. Our preferred mode of payment is either Automatic Clearing House (ACH) or through our corporate card program described above.

Accounts Payable will issue physical checks under limited circumstances. If checks are required, please reach out to the Accounts Payable at aphelpdesk@support.gannett.com.

Payment Requests
Accounts Payable processes Payment Requests only when a supplier invoice or other billing documentation cannot be provided and processed through Infor Payables. The Payment Request Form (found here: https://webapps.us.ad.gannett.com/pr/) includes the following information:
1. Supplier's complete name
2. Remit to address
3. Total payment due (in USD)
4. Complete general ledger account coding
5. Payment due date (ASAP is not acceptable)

Attach all documents, such as agreements, notices, email or spreadsheets that support the amount payable in the Support Documents section of the Form. Preparer should also attach any documentation which must be submitted along with the payment in the

Remittance Documents section of the Form. If remittance documents are attached and required to accompany payment, the user MUST select Special Handling by choosing "Include Attachments" in the drop-down box on the form.

In certain cases, the online Payment Request form is not an efficient means for requesting a payment. Such as multiple like-kind tax payments to varying entities, newsprint payments and garnishments. In this case, the fully completed excel template and related support documentation shall be emailed to Accounts Payable, along with approval based on hierarchy outlined below.

To allow for timely payment, submit the Payment Request form to Accounts Payable no later than two (2) weeks before the payment is due. Accounts Payable will route the completed Payment Request for approval to the appropriate Gannett manager via Infor Payables workflow. In cases where multiple payment requests (10+) are needed, an AP Upload form can be utilized, and email approvals are acceptable. Use of verbal approvals, initials, or stamped approvals will not be accepted.

New Vendor Setup

Accounts Payable is solely responsible for entering new and or updated supplier information into the Infor AP Vendor Master File. Accounts Payable staff will gather required documentation and create new supplier records or enter changes to existing suppliers in the Infor Payables Vendor Master file. This centralized process ensures that Gannett has adequate internal controls over the process-when adding and updating vendor information in the system. The following are basic requirements for new vendor data or existing vendor file data changes:

1. Copy of supplier's invoice and other pertinent information
2. Documentation confirming the change from an existing account such as a public announcement that the supplier issued to validate the change. Note that for direct deposit setup or change, official banking documentation required, such as a voided check or bank letter. Changes to existing vendor accounts require verbal verification from the supplier.
3. Completed W-9 form or substitute W-9 and Direct Deposit form, for US Companies only
4. Completed W-8 form for Foreign Companies receiving payment from Gannett US Entities only. Foreign suppliers will need to determine which type of form applies to them.

Questions on vendor setup can be directed to vendormaster@support.gannett.com.

AP Invoice Coding

General ledger account coding is the responsibility of the department reviewing and/or approving invoices. Any reclassification of incorrect GL coding will be made for material items (>$5,000) only. All invoices processed by Accounts Payable must be coded with active General Ledger accounting strings in order to complete the approval workflow in Infor Payables. Account coding represents the Company, Business Unit, Department, Product, Expense Type and Channel and/or Project (if applicable).

Invoice Approval
The invoice approval and payment processes are two distinct processes that lead to the actual disbursement of corporate funds.

The invoice approval process (by business owners) confirms the receipt of product and/or acceptance of service and also confirms that the price and quantity are consistent with negotiated terms and conditions, thus authorizing the Accounts Payable department to process and pay the submitted invoice.

Invoices must be approved by the appropriate level of management as outlined in this policy. If operationally necessary, invoice approval responsibility may be delegated by the responsible Manager within Infor Payables to another authorized approver. Approving managers are required to approve invoices within 5 business days of receipt to ensure prompt payment. Invoices which are not approved or rejected within 15 business days will be systematically escalated to the manager of the invoice approver.

Each invoice must be reviewed by the approving authority for the following:
1. Invoice matches the intended business commitment
2. Price (unit and total), quantity, service and terms
3. Confirm receipt of goods and services
4. Correct Bill to Entity
5. Account coding

General Approval Levels
The following table describes the approval levels by position, and by dollar amount, unless an express exception has been requested and is on file with Accounts Payable. Invoice approver hierarchy will be used for all Infor Payables workflows, based on the approver or staff printed on the invoice and the table below. Invoice approver and their supervisory hierarchy will approve all invoices regardless of invoice cost center expense. These autoflows are initiated and maintained by the Accounts Payable team.

Invoice Approval Thresholds	
Under $5K	Supervisor
< or = $10K	Manager
< or = $25K	Director
< or = $100K	Sr Director
< or = $250K	Vice President, Corporate Assistant Controller
< or = $1M	SVP and Corporate Controller
< or = $2.5M	Gannett Executive Team
< or = $10M	CFO, President Gannett Media, President DMS
> or = $10M	CEO

Out of policy exceptions must be approved as follows:	
< or = $100K	Vice President, SSC
< or = $250K	SVP, SSC or Corporate Controller
> $250K	CFO

The following types of payments are not processed by Accounts Payable and are outside the scope of this Invoice Approval Policy.

1. Payroll
2. Payment transfers between legal entities
3. Dividends and Intercompany loans
4. Corporate Treasury initiated wires

Invoice Rejection

Invoice approvers may reject or request to change invoice coding on any invoice.

Accounts Payable will only pay the current amount due on the invoices. Any charges listed as "balance forward" will require a separate invoice(s). Accounts Payable will not adjust the original invoice amount. If Gannett owes more or less than what the invoice states, the invoice approver should reject the invoice with comments in Infor Payables and contact the supplier to request a new correct invoice reflecting the accurate charge.

If Gannett is due a credit from the supplier, the invoice approver should request a credit memo from the supplier, and the supplier should submit the credit memo to Gannett via Symbeo, using the same submission methods as noted above for invoices. Accounts Payable will forward the credit memo to the approver listed on the invoice using Infor Payables workflow for approval. The approved credit memo will be offset against future payments to the supplier.

Urgent Payment

Payments are distributed multiple days each week from the SSC, so there should be no need for special out of cycle payment runs. In business situations where an emergency payment is deemed necessary, please reach out to the Accounts Payable team at aphelpdesk@support.gannett.com, Attention: Senior Manager AP, Urgent Payment to discuss alternative payment options.

Employee Reimbursable Expenses

Gannett Required Travel and Entertainment (T&E) - For a complete document of all travel policies including mileage, please see the Gannett Travel Policy.

Gannett Corporate Legal Policies and Procedures

Policy Owner: Legal
Version: 20250602
Employee Scope: All employees

I. INTRODUCTION

A. Legal Department's Role

The role of Gannett Co., Inc.'s ("**Gannett**") legal department (the "**Legal Department**") is to provide legal counsel, advice and services which enable Gannett and its subsidiaries (collectively, the "**Company**") to achieve its business objectives in an efficient and lawful manner without exposing itself to inappropriate legal risks. The members of the Legal Department aim to carry out the corporate mandates received and respond promptly to the legal requirements generated by the activities of the business units. The Legal Department strives to protect the Company's legal rights and to defend the Company when its conduct is challenged, while providing the functional support strategies required to develop and enhance corporate and business strategies.

B. Department Contact List

The Legal Department is based at 175 Sully's Trail, Suite 203, Pittsford, New York 14534. Contact information for members of the Legal Department is as follows:

1. Polly Grunfeld Sack
   Senior Vice President, Chief Legal Officer, and Secretary
   psack@gannett.com
2. Aboli Alurkar
   Senior Director, Assistant General Counsel, Global Privacy & AI
   aalurkar@gannett.com
3. Clay Arnold
   VP, Deputy General Counsel
   carnold@gannett.com
4. Chantal Corsaro
   Legal Assistant
   ccorsaro@gannett.com
5. Sheryl Costa
   Legal Operations Director
   scosta@gannett.com
6. Garrett J. Cummings
   Senior Deputy General Counsel and Assistant Secretary
   gcummings@gannett.com
7. Tom Curley
   Deputy General Counsel, Litigation/First Amendment
   tcurley@gannett.com
8. Mark Faris
   News Litigation Manager
   mfaris@gannett.com

9. Donna Gonzales
   Deputy General Counsel, AI/Technology
   dgonzales@gannett.com
10. Kayla Klos
    VP, Chief Securities Officer
    kklos@gannett.com
11. Edwin Larkin
    VP, Chief Litigation Officer
    Elarkin2@gannett.com
12. Rachel Militello
    Legal Assistant
    Rmilitello2@gannett.com
13. Brendan Smith
    Deputy General Counsel M&A/Securities
    bsmith32@gannett.com
14. Cher Tate
    VP, Chief AI Compliance Officer/Chief Privacy Counsel
    ctate1@gannett.com
15. Jennifer Thomas
    Deputy General Counsel AI/Privacy, General Counsel LocaliQ
    jthomas5@gannett.com
16. Monica L. Treviso
    Senior Paralegal
    mtreviso@gannett.com
17. Stacey White
    Legal Assistant
    swhite@gannett.com
18. Yelena Zharskaya
    Senior Legal Assistant
    Yzharskaya2@gannett.com

C. List of Notaries

For business or personal reasons, the following individuals are available for notarial services (Note: All notaries are located in the state of New York and all documents must be notarized in New York):

1. Sheryl Costa
   Legal Department
   scosta@gannett.com
2. Garrett J. Cummings
   Legal Department
   gcummings@gannett.com
3. Monica L. Treviso
   Legal Department
   mtreviso@gannett.com

II. CONTRACTS

Contracts are a necessary part of doing business. The Company deals with legal contracts from vendors, contractors, suppliers, consultants, licensees, licensors and others (collectively, "**Vendors**" and individually "**Vendor**") on a daily basis. The Company also enters into contractual arrangements with current, former and prospective employees. It should be understood from the outset that many contracts drafted by Vendors are very one-sided and written in confusing language. The terms and conditions of these contracts, however, can generally be negotiated to some extent to make provisions mutual, to delete extremely harsh or unfair provisions, or to increase the legal protections and minimize potential liability to the Company and maximize the Company's rights. In some cases the contracts even need to be negotiated to reflect the business and operational realities of the deal.

The Company strictly prohibits the Company, any of its employees, and/or any Vendor from performing any obligations and/or exercising any rights under a contract until that contract has been: (1) reviewed and approved by the: (a) business owner; (b) Legal Department, and (c) Vendor; and (2) fully executed by all parties.

A. What Constitutes a Contract?[2]

A contract can be an oral[3], written, or implied agreement between two or more parties to do or not do a particular thing. A contract can also be created by an exchange of emails, text messages, or through a "course of dealing" between the parties[4]. A course of dealing refers to the pattern of conduct or repeated interactions between the parties over time that indicates a mutual understanding and an intent to form a binding agreement—even in the absence of a formal, written document. Courts recognize that such ongoing interactions, particularly when the parties have consistently acted in accordance with specific terms, can give rise to enforceable obligations.

For a contract to exist, there must be a common understanding among the parties as to the essential terms, mutual obligations, and "legal consideration," meaning that something of value is exchanged. "Value" in this context is not limited to money; it may include services, goods, forbearance (agreeing not to do something), or other benefits. For example, a court can find that an agreement may be a binding contract even though neither party pays money to the other.

Contracts may be called many different things. For example: "Memoranda of Understanding," "Termination Agreement," "License Agreement," "Lease Agreement," "Rental Agreement," "Purchase and Sale Agreement," "Non-Disclosure Agreement," "Confidentiality Agreement," "Consulting Agreement," "Service Agreement," "Power of Attorney," "Settlement Agreement," "Settlement and Release Agreement," "Promissory Note," "Independent Contractor," "Letter of

[2] For purposes of these policies and procedures, discussion of contracts will be limited to Vendor contracts, but the same analysis can be applied to employee contracts.
[3] For purposes of these policies and procedures, discussion is limited to written agreements. It is extremely important, however, to realize that a contract could be formed orally.
[4] That is why it is essential to have a fully executed contract in place before any "work" begins.

Intent," "Master Service Agreement," "Statements of Work", "Purchase Orders", "End User License Agreement", "Bill of Sale," "Advertising Agreement," "Software as a Service (SaaS) Agreement", "Letter of Intent," "Employment/Job Offers," "Relocation Agreements," "E-mail exchanges setting terms" and "Subscriber Agreement".

The concept of a "contract" is quite broad, so you should assume that **any** written agreement, including a text or email exchange discussing deal terms, with a Vendor or employee **could be** a binding contract.

B. Review and Approval of Contracts

Any contract which purports to commit or restrict the Company to a course of action **must** be reviewed and approved by the Legal Department. The primary objective behind having the Legal Department review and approve contracts is to mitigate the Company's exposure to liability. In order to accomplish this objective, the Company **requires** that every contract be reviewed and approved by the Legal Department **before** it is fully executed by the parties.

When the Legal Department receives a contract from or through the business owner (generally, an employee of the Company), the goal is to review and return the contract as soon as possible. However, due to the fact that each contract has a unique set of facts and circumstances the review of contracts may require in-depth analysis and review. Therefore, ***adequate time*** must be allowed for the Legal Department to complete its review and approval process. To demonstrate, here is a partial list of questions that must be considered by the Legal Department for each Vendor contract submitted for review and approval.

1. Does the contract seek to limit Vendor's liability?
2. Does the contract involve either party handling personal information?
3. Does the contract subject the Company to tort liability?
4. Does the contract provide for the Company to "indemnify" Vendor, or otherwise assume responsibility for paying Vendor's liabilities?
5. Does the contract contain an acceleration clause or provision that all payments are immediately due upon breach of the contract or default?
6. Does the contract contain late payment penalties or finance charges?
7. Does the contract contain clauses that would make it subject to either the substantive law or the jurisdiction (also referred to as "forum" or "venue") of another state?
8. Does the contract require binding arbitration or any mandatory dispute resolution?
9. Does the contract allow Vendor to assign its right to payment to a third party without subjecting the third party to all the defenses and claims the Company would have against Vendor?
10. Does the contract contain confidentiality or non-disclosure provisions?
11. Are payment terms net 30 (meaning that payment is due 30 days later) upon receipt and/or approval of invoice?

12. Does the contract provide for the Company to pay attorney fees, court costs, or other litigation expenses of other parties if there is a dispute?
13. Does the contract provide for automatic renewal, or renewal unless the Company takes affirmative action to terminate?
14. Does the contract provide for personal liability of the signer or any other employee of the Company?
15. Does the contract incorporate other terms or documents or information by reference, or refer to information outside the contract?
16. Does the contract create rights in parties other than the Company and Vendor?
17. Does the contract allow Vendor to repossess property or take action outside of court proceedings in response to a breach of contract by the Company?
18. Does the contract provide Vendor with ownership or other rights (often called a "security interest" or "UCC statement") in the property being purchased by the Company?
19. Does the contract provide for payments beyond the current fiscal year?
20. If the contract is for personal services (*e.g.,* carriers, consulting, etc.), has independent contractor status been established?
21. Does the contract allow the price or other terms to be changed in the future?
22. Does the contract allow Vendor to use the Company's name in any advertising, endorsement, or promotion?
23. Does the contract allow Vendor to terminate the contract?
24. Does the contract require the Company to obtain insurance or a bond?
25. Does the contract require the Company to "ensure" or use "best efforts" or otherwise guarantee anything (*e.g.*, security of property or confidentiality of information)?

In addition to the Legal Department's review, a contract may be subject to review and approval of other departments. For example, the Company's Tax Department will have to review and approve certain contracts for tax purposes. The Company's Finance Department will have to review and approve certain contracts for accounting/budgeting purposes and the Insurance Department will have to review certain contracts to ensure all parties have the necessary and proper insurance. Accordingly, "adequate time" for review and approval may, in some cases, include the time necessary for these additional departmental reviews and approvals.

To assist in reducing review time, employees are encouraged to check with the Legal Department to determine if there is an approved template that may be used for the contract.

C. Who has Authority to Execute Contracts?

As mentioned above, the form of **all contracts must be reviewed and approved by the Legal Department**. After the contract is reviewed and approved by the Legal Department (and the Vendor) it must be executed by an authorized person. Authority to execute contracts for the Company is limited to those persons designated in the Company's Signature Authorization Policy, found here. In addition to the authority granted by the Signature Authorization Policy, the Board of

Directors, in its sole and absolute discretion, may delegate temporary and/or permanent signing authority, via resolution, to a person who otherwise does not have the authority to execute contracts for the Company under the Signature Authorization Policy. ***Anyone else who enters into a contract that purports to bind the Company is acting without authority and could be held personally liable for the contract.***

D. Periodic Review of Contracts.

It is the responsibility of: **(1)** the business owner of a contract; or **(2)** the relevant department responsible for administering a contract, to periodically review their contracts during the term to recognize and act upon upcoming renewal or extension deadlines (especially when there is an auto renew feature) and ensure that it is still valid, appropriate, and accurately reflects the Company's current business operations, systems, and practices. Circumstances may change over time, such as system updates or operational shifts, which could impact the contract's continued alignment with the Company's needs and obligations. Proactive review and, where necessary, updates if possible (via agreed upon amendments) to the contract or termination of the contract (if allowed by the contract terms) will help mitigate risks, ensure continued compliance, and protect the Company's interests.

E. Retention of Executed Contracts.

The original and/or a copy of a fully executed contract (*i.e.*, a contract signed by all parties to the contract) **must** be forwarded to the Legal Department for filing purposes. The contract will be retained in accordance with the Company's Records Retention Policy (See Article VI below).

III. CORPORATE MATTERS

A. Lotteries; Sweepstakes; Contests; Raffles; Games of Chance.

ALL LOTTERIES, SWEEPSTAKES, CONTESTS, RAFFLES, AND/OR GAMES OF CHANCE (COLLECTIVELY, "PROMOTIONS") **MUST BE REVIEWED BY THE LEGAL DEPARTMENT PRIOR TO BEING LAUNCHED OR PROMOTED**. THESE PROMOTIONS ARE SUBJECT TO COMPLEX REGULATORY REQUIREMENTS AT BOTH FEDERAL AND STATE LEVELS, AND FAILURE TO COMPLY CAN RESULT IN SIGNIFICANT LEGAL AND FINANCIAL RISKS FOR THE COMPANY. LEGAL REVIEW WILL ENSURE THAT ALL PROMOTIONS COMPLY WITH APPLICABLE LAWS AND REGULATIONS, INCLUDING ELIGIBILITY RULES, PRIZE DISCLOSURES, AND ADVERTISING REQUIREMENTS.

There are strict laws on both the state and Federal levels (as well as abroad) which have the effect barring private lotteries. A lottery is a promotion that has three elements: (1) prizes; (2) winners chosen by chance; and (3) consideration. The federal government and many states regulate prize promotions, that is, promotional programs which invite members of the public to submit an entry and which award prizes to fewer than all the entrants. These promotions fall into two basic categories: sweepstakes and contests of skill. The descriptions below cover only basic concepts and general rules. There are many other details and nuances surrounding this area of law, which is why all the official rules and any official

advertising for any prize promotions must be submitted to the Legal Department for review. The objective of the Legal Department is to review and turn around rules for contests and sweepstakes as fast as possible once we receive them. Employees must allow ***adequate time*** for the rules to be reviewed and to obtain the necessary bonding and/or registration, if required, upon receipt by the Legal Department.

1. Sweepstakes. A sweepstakes is a promotional device in which prizes are offered to participants selected on a random basis. The primary issue in structuring and executing a sweepstakes is to avoid becoming an illegal lottery. Avoidance is accomplished by eliminating the element of consideration. That means you will never have to pay cash or any other form of consideration/value to enter legitimate sweepstakes and purchasing a product will not improve your odds. "Consideration" is not limited to money and other things of value. Consideration also includes: (a) requiring someone to exert extraordinary effort (e.g., travel an unreasonable distance to obtain a sweepstakes entry form); or (b) to buy a good, service and/or product to enter the sweepstakes (e.g., buy a newspaper and receive a sweepstakes entry form). All sweepstakes and chance promotions must have a set of official rules, which constitute the contract between the sponsor and the consumers participating in the promotion. Once the official rules are published and posted, they must be followed exactly and cannot be changed during the course of the promotion, except under extreme and unusual circumstances. If the promotion will have an online aspect, there are also additional considerations and disclosures that should be made.

2. Skill Contests. Skill contests are a promotional marketing tool requiring participants to use specific skills to solve or complete a specified objective in order to qualify for an award. In a bona fide skill contest, it is the element of chance that is eliminated. Therefore, it is often possible to require consideration, such as an entry fee for participation. Some examples of contests that are typically held to be skill contests include the following: essay contests, photography contests, athletic contests, art contests, cooking contests. All skill contests must have an official set of rules. Once the official rules are published and posted, they must be followed exactly and cannot be changed during the course of the promotion, except under extreme and unusual circumstances.

B. Releases/Indemnification Documents.

The Legal Department **must** review and approve any release or indemnification document **before** it is executed. A draft should be sent to the Legal Department with a copy to the Corporate Insurance Department as far in advance as possible.

C. Intellectual Property.

"Intellectual property" is an omnibus term for a group of intangible personal property rights, and refers primarily to patents, copyrights, trademarks and trade secrets. Due to the nature of the Company's business, the Legal Department deals mainly with trademarks. A trademark is any word, name (including mastheads), symbol, device or any combination of these, which identifies goods in a way to

distinguish them from the goods of others. They can be protected under federal, state or common law. The Legal Department, with the assistance of outside counsel, is available to screen new marks prior to adoption. Before actually using a potential new trademark, it must be submitted to the Legal Department for review and to determine the most cost efficient protection regime.

D. Bankruptcy Issues.

Today's struggling economy has led to many bankruptcy filings that affect the Company. The Legal Department has procedures in place to process matters related to bankruptcy. If you receive any documents in connection with a bankruptcy you must immediately forward such documents to the Legal Department. The Legal Department may follow up with you regarding the bankruptcy. If you are contacted by the Legal Department, it is very important that you provide any and all records requested by the Legal Department so that it can: (1) file a timely proof of claim; and/or (2) answer a complaint asserting a preference claim (or prior demand), on behalf of the Company.

Should you have any questions regarding: (1) a Vendor's bankruptcy; (2) a complaint asserting a preference claim; or (3) your relations with a financially troubled Vendor(s), please contact a member of the Legal Department.

E. Collection Issues.

Collections become increasingly difficult, expensive and unlikely the longer a bill has been outstanding. Getting help from an agency early in the process for appropriate cases can make the difference between successful collection and a bad debt write-off. Please remember that sending an account to collections without good reason may alienate your customer. The Legal Department recommends you do all you can to facilitate and/or encourage the customer paying prior to handing over the account. Please contact the Collections Department when the customer is unresponsive to reminder notices or denies responsibility for the account. **Employees are prohibited from engaging outside counsel without prior approval from the Company's Chief Legal Officer.** The Legal Department has engaged a law firm specializing in collection issues whose fees are based on money actually collected, so there is no risk or out of pocket cost to the Company (other than nominal court filing fees). Third party intervention will send a powerful message to the debtor that the Company is serious about getting paid.

F. Banking Resolutions / Certificates.

Banking resolutions are required by virtually every bank or financial institution for opening up corporate financial and checking accounts. Please contact the Company's Treasurer for the preparation and execution of these resolutions.

G. Personal Legal Services.

The attorneys in the Legal Department have only one client: the Company. They are not permitted to provide personal legal advice to the Company's employees

regarding, for example, apartment leases, parking fines or tickets, domestic relations issues, the preparation of wills, real estate deeds, etc.

H. The Company's Letterhead.

The Company's letterhead stationery, including the Company's stationery with your name on it, is to be used for business purposes only. Please do not use the Company's letterhead for personal purposes.

IV. OUTSIDE ATTORNEYS

The Company's Chief Legal Officer is responsible for the legal affairs of the Company. The Company uses the services of outside counsel from time to time when special expertise is needed or when geographical considerations require the use of local counsel. **THE COMPANY'S CHIEF LEGAL OFFICER MUST APPROVE THE RETENTION OF ANY OUTSIDE COUNSEL.**

V. LITIGATION

A. Litigation and Pre-Litigation.

IF YOU ARE SERVED WITH DOCUMENTS FROM A COURT OR LAW FIRM IMMEDIATELY CONTACT THE LEGAL DEPARTMENT.

All litigation and pre-litigation matters should be referred to the Legal Department as soon as possible. When an employee of the Company: (1) learns that a claim has been made against the Company; (2) learns that circumstances indicate that a claim likely will be made; or (3) receives a threat of litigation (even if follow through is unlikely), he or she must notify the Legal Department immediately.

Under no circumstances should a cease and desist letter be sent out without discussing the matter first with the Company's Chief Legal Officer. A cease and desist letter is one whereby an unlicensed or unauthorized user of the Company's name (including on a website or in a domain name) is told to immediately stop such unauthorized use.

B. Governmental Investigations.

When an employee of the Company receives a request from any governmental agency for documents, testimony, an interview or other information, he or she **must** notify the Legal Department immediately.

C. Subpoenas.

IF AN EMPLOYEE IS SERVED WITH A SUBPOENA HE OR SHE MUST IMMEDIATELY CONTACT THE LEGAL DEPARTMENT.

The Company often receives subpoenas requiring the timely production of records or information pertaining to specific employees or entities involved in potential or ongoing litigation. A subpoena is a legal document compelling the production of certain designated materials that may be relevant to a pending judicial proceeding. Subpoenas are usually issued by the clerk of the court in the name of the judge

presiding over the case, and will usually be on the letterhead of the court where the case is filed, naming the parties to the case, and being addressed by name to the employee whose testimony is being sought. It will contain the language "You are hereby commanded to report in person to the clerk of this court" or similar, describing the specific location, scheduled date and time of the appearance. A subpoena may require an employee to do any of the following:

1. Produce papers, records, books, or other physical items (including electronic records) for inspection and/or copying;
2. Appear and testify in person at a trial, hearing, or other court proceeding; and/or
3. Appear in person for a deposition before trial and/or produce documents at the deposition.

ANY AND ALL RESPONSES TO A SUBPOENA, INCLUDING DECISIONS TO FIGHT OR "QUASH" A SUBPOENA, **MUST** BE REVIEWED AND APPROVED BY THE LEGAL DEPARTMENT.

D. The Attorney-Client Privilege (Privileged and Confidential Documents).

Communications between the Legal Department and employees of the Company relating to the Company's legal affairs may be protected from disclosure by the attorney-client privilege if the Company is involved in litigation and other legal proceedings. Both state and federal law recognize the attorney-client privilege which maintains the confidentiality of documents prepared for the purposes of providing the Company's employees with legal advice or providing the Company's attorneys with information as to which legal advice is sought. In order to preserve the attorney-client privilege, employees must be certain to copy a member of the Legal Department on all communications in connection with any and all contentious matters or potential legal disputes. In addition, employees must not make any conclusions of law in the communications.

Accordingly, all documents (e.g., memoranda, e-mails) sent to the Legal Department or any other person in the Company in response to a request from the Company or the Company's attorney for information about a legal matter should be labeled with the phrase **"Privileged and Confidential/Prepared at Counsel's Request."** Failure to do so may result in a waiver of the privilege and subsequent disclosure of the information.

VI. RECORDS RETENTION AND LITIGATION MEMORANDUM

A. Records Retention.

The Company has implemented a Records Retention Policy in an effort to: **(1)** retain important records for reference and future use; **(2)** delete records that are no longer necessary for the proper functioning of the Company; **(3)** organize important records for efficient retrieval; and **(4)** ensure that the employees of the Company know what records should be retained, the length of their retention, means of storage, and when and how they should be destroyed. A copy of the Records Retention Policy can be found here.

The Company **expects** all employees to fully. comply with the Company's records retention policy. If, however, any of the Company's records are relevant to a legal dispute[5], or a potential legal dispute, then the employees **must** preserve those records until the Company's Chief Legal Officer determines the records are no longer relevant.

If an employee suspects or has knowledge of a legal dispute or a potential legal dispute, he/she **must immediately** contact the Company's Chief Legal Officer at (585) 598-0030 regarding such legal dispute or potential legal dispute.

All questions regarding the retention of the Company's records should be addressed to the Company's Chief Legal Officer.

B. Litigation Hold Memorandum

If a legal dispute is filed or imminent, or a legal document request has been made upon the Company, **ALL DESTRUCTION OF RECORDS RELATED TO SUCH LEGAL DISPUTE OR DOCUMENT REQUEST MUST CEASE IMMEDIATELY**. Only the Company's Chief Legal Officer may suspend the records retention policy to require that records relating to the legal dispute be retained and organized (the "Litigation Hold Process"). An understanding of the Litigation Hold Process is very important. Should an employee fail to follow the Litigation Hold Process, he/she and/or the Company may be subject to fines and penalties, among other sanctions.

The Company's Chief Legal Officer may suspend the records retention policy: **(1)** by issuing a Litigation Hold Memorandum ("LHM"); or **(2)** by use of any other communication, followed up with a LHM.

A LHM is a formal communication issued by the Company's Chief Legal Officer to those employees who: **(1)** are directly or indirectly involved in the litigation or potential litigation; and/or **(2)** can identify, preserve and forward all relevant records related to the litigation or potential litigation. The purpose of the LHM is to ensure that relevant records are not destroyed and to protect the Company and/or its employees from liability and possible sanctions.

If an employee has any questions regarding the Litigation Hold Process and/or the LHM, he/she **must** immediately contact the Company's Chief Legal Officer at (585) 598-0030 for assistance.

VII. CONCLUSION

The Company's business is an exciting and challenging work environment. The Legal Department wants each employee to exercise care when transacting business on behalf of the Company. Employees can prevent many of the legal uncertainties in

[5] Legal dispute shall include, but not be limited to, the following: (1) Arbitration; (2) Mediation; (3) Agency Investigation; and/or (4) Lawsuit/Litigation.

business transactions by simply adhering to these policies and procedures and communicating with the Legal Department.

Gannett RFP Policy

Policy Owner: Finance
Version: 20210801
Employee Scope: All employees

1. Purpose:

An RFP is a document that solicits offers through a bidding process for the procurement of a commodity, service, or asset. An RFP is required when the commodity, service, or asset exceeds $500,000 in annual spend, or could affect multiple business units. The RFP solicitation must result in proposals from at least (3) vendors and should include a certified diverse supplier when available. There may be exceptions to this proposal minimum requirement if there are not enough vendors that provide the commodity, service, or asset.

3. The RFP Process:

Business units must submit detailed specifications for the commodity, service, or asset, including anticipated annual volume, user license counts, types of access required, business units involved, and what existing or upcoming programs or relationships may be related to the purchase. Exceptions will be made for benefits payments, investment banking fees, legal fees, newsprint, and utilities in deregulated gas and electricity markets. These purchases will continue to be negotiated for best outcomes and are exempt from the RFP process.

4. Exception Process:

An exception request to the RFP process must be submitted with enough time for an RFP to be conducted. The exception must be submitted in writing and must first be approved by the Corporate Controller and then by the Chief Financial Executive. Departments are required to contact Gannett Supply to facilitate the RFP creation and sourcing process. Please find the RFP template by following this link to SharePoint: RFP Template. Gannett Supply will coordinate with Business Development on RFP requests.

5. Diverse Suppliers:

Gannett supplier diversity commitment statement:
Our sourcing activities align with our employment inclusion and anti-discrimination policies. We expect the same level of respect and inclusion by our supplier organizations as we do our own employees.

Internally, we partner closely with Gannett ERGs (Employee Resource Groups) to promote opportunities for diverse suppliers, and externally Gannett is a member of NMSDC, the National Minority Supplier Development Council. This membership further enables Gannett to engage with diverse suppliers and match potential opportunities across the company. Gannett is benchmarking diverse supplier spend and is working to expand our program each year.

Handling Email Messages That Include Credit Card Information Policy

Policy Owner: IT Security and Data Privacy
Version: 20250101
Employee Scope: All US employees who work with all inbound and outbound emails that contain credit card data.

Purpose

The purpose of this policy is to outline the required practices for the handling of email messages that contain credit card information that will enable Gannett to comply with the Payment Card Industry Data Security Standard (PCI DSS).

Definitions and Acronyms

When navigating this policy, it's important to grasp the terminology. Our Glossary of Cybersecurity Terms provides concise definitions for key concepts.

Policy

General

- Outbound emails from Gannett must not contain customer credit card information
- Internal email between Gannett employees must not contain customer credit card information
- Inbound emails that contain credit card data must comply with the following:
  - Deleted and purged from the mailbox immediately upon discovery
  - Payments cannot be posted to an account when received via email.
  - Customers must be notified, via a separate email (not including the original email with credit card data), that Gannett does not accept credit card payment via email.
  - Notify the customer with proper credit card payment methods. (I.e phone number to call or website address for credit card payments)

Enforcement and Exception

- Compliance with this policy is required under Gannett's Information Security Policies and Standards Enforcement Policy and Gannett may take actions in response to non-compliance as provided under the Enforcement Policy.
- Any exceptions to this policy must follow Gannett's Information Security Policies and Standards Exceptions Policy.

This policy may be updated occasionally by the Company. The current version of this policy, and other policies referenced in this document, may be viewed on MyLife@Gannett.

HIPAA Privacy Notice

Policy Owner: Human Resources
Version: 20241030
Employee Scope: All employees from the following Divisions and Sub-Divisions. Divisions included: People, Legal. Sub-Divisions included: Accounting/Controller, Advertising products, Applications, Corporate Development, Delivery & Automation, DMS Engineering, Facilities, Field Accounting & Finance, Finance Executive, Financial Planning & Analysis, Freemium, Infrastructure & Security, Internal Audit, Payroll, Presence Product & Buy Online, ReachLocal, Reporting API & Graders, Shared Services, Tax, Tech Operations, Treasury, UX & Design.

Overview

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

This Notice of Privacy Practices ("Notice") describes rights and responsibilities related to individually identifiable health information used by Gannett Media Corp. and its affiliates (the "Company") and held by the group health plan components of the Gannett Media Corp. Welfare Benefits Plan and the Gannett Media Corp. Post-65 Retiree Medical Plan and Health Reimbursement Arrangement (collectively, the "Plan") under the Health Insurance Accountability Act of 1996, as amended ("HIPAA"). The group health plan components of the Gannett Media Corp. Welfare Benefits Plan include the Medical Program, Vision Program, Dental Program, Employee Assistance Program, and Health Care Flexible Spending Account Program. Other benefits provided under the Plan (for example, life insurance) are not subject to HIPAA and this Notice does not apply to those benefits. The Plan is sponsored by Gannett Media Corp.

This Notice describes how the Plan may use and disclose health information that identifies you and relates to: (i) your past, present or future physical or mental health condition; (ii) the provision of health care to you; and/or (iii) the past, present or future payment for the provision of health care to you ("protected health information" or "PHI"). PHI does not include health information that is held by the Company in its role as your employer (for example, health information held for purposes of your employment records). This Notice does not apply to information that does not directly identify an individual (you) and cannot reasonably be used indirectly to identify you.

This Notice also describes your privacy rights, the Plan's duties with respect to your PHI, your right to file a complaint, and how to contact the Plan to obtain additional information.

Note: if you are covered by an insured health coverage option offered under the Plan (e.g., an HMO), you will receive a separate Notice of Privacy Practices from the insurer carrier or HMO for that Plan option.

(1) Treatment, that is, the Plan can use your health information and share it with professionals who are treating you or with third parties to help coordinate or manage

your health care. For example, the Plan may share information with your doctor about your diagnosis and treatment plan to help arrange additional services.

(2) Payment, that is, the Plan can use and disclose your PHI when the Plan pays for health services. This includes determining eligibility for Plan benefits, providing pre-authorizations, facilitating payment for the treatment and services received, determining benefit responsibility under the Plan, and coordinating coverage. For example, the Plan may share information with your healthcare provider to determine whether the Plan will cover a particular treatment.

(3) Health Care Operations, that is, the Plan may use and disclose your PHI to administer, monitor and operate the Plan, and contact you when necessary. For example, the Plan may submit your health information to external auditors or agencies to assess the quality of a health plan. The Plan may also submit your health information to a stop-loss insurance carrier or to obtain pricing information.

(4) To Business Associates, that is, the Plan may contract with third party individuals or entities ("Business Associates") to provide business services to the Plan, such as administrative services, claim processing, or audit services. The Plan requires Business Associates (and any subcontractors of Business Associates) to agree, in writing, to maintain the confidentiality of PHI and to notify the Plan if there is a security incident. For example, the Plan may disclose PHI to a third-party administrator to process claims for benefits.

(5) To the Company, that is, to Company employees who are involved with Plan administration. In general, only Company employees assisting in carrying out treatment, payment and health care operations, will access your PHI without your written authorization. However, some Company employees will have access to information regarding your enrollment in the Plan or enrollment in a specific benefit to allow for payroll processing of premium payments.

(6) Public Safety and Health, that is, the Plan may share your PHI for certain public health activities, such as preventing disease, helping with medical product recalls, reporting adverse reactions to medications, reporting to public authorities suspected abuse, neglect or domestic violence, or preventing or reducing a serious and imminent threat to your health or safety, or the health and safety of the public or another person.

(7) As Required by Law, that is, the Plan may share your PHI if required by federal, state, or local law.

(8) Government Audits, that is, the Plan may disclose your PHI to an administrative agency when the agency requires it, including the Department of Health and Human Services if it wants to see that the Plan is complying with federal privacy law.

The Plan's Uses and Disclosures of Your PHI

The Plan may use or disclose your PHI to carry out the following functions without your authorization.

Other than the uses described above, the Plan will not disclose your PHI to other Company employees or departments, or use your PHI for any employment-related actions and decisions without your written authorization.

(1) Respond to Lawsuits and Disputes, that is, the Plan may share your PHI in response to a court or administrative order, a subpoena, discovery request, or other lawful process.
(2) Workers' Compensation, that is, the Plan may share your PHI for workers' compensation or similar programs, but only as authorized by, and to the extent necessary to comply with, laws relating to workers' compensation and similar programs that provide benefits for work-related injuries or illness.
(3) Health Oversight, that is, the Plan may disclose your PHI to a health oversight agency for oversight activities authorized by law, such as audits, investigations, inspections, licensure or disciplinary actions, and other activities necessary for the government to monitor the health care system, government programs such as Medicare and Medicaid, and compliance with civil rights laws.
(4) Law Enforcement, that is, the Plan may disclose your PHI if asked to do so by a law enforcement official under certain limited circumstances.
(5) Military, that is, the Plan may disclose your PHI as required by military or veterans' authorities if you are or were a member of the uniformed services.
(6) National Security and Intelligence Activities, that is, the Plan may disclose your PHI to authorized federal officials for national security activities authorized by law.
(7) Organ and Tissue Donations, that is, if you are an organ donor, the Plan may share your PHI to organ procurement organizations or other entities that are engaged in the procurement, banking, or transplantation of cadaver organs, eyes, or tissue for purposes of donation and transplantation.
(8) Coroners, Medical Examiners, and Funeral Directors, that is, the Plan may disclose your PHI to a coroner, medical examiner, or funeral director, when an individual dies, as necessary for them to carry out their duties.
(9) Research, that is, the Plan can share your PHI for health research with additional safeguards for your privacy. These safeguards include determination by an Institutional Review Board or privacy board that risks to privacy are low relative to the scientific benefit. Some examples of safeguards may include removing sensitive information and providing adequate data security.

The Plan will not use genetic information to decide whether to provide you coverage or the price of coverage, but this does not apply to long term care plans.
The Plan will not disclose your PHI for marketing purposes or sell your PHI to third parties without authorization from you or as permitted under applicable law.
Other uses and disclosures of PHI not described in this Notice will be made only by your written authorization.

Your Rights

This Section explains your rights and some of the Plan's responsibilities to help you. To make a request, or for more information about these rights, email the Plan at hipaacompliance@gannett.com, or call the Plan at 855.442.4236.

(1) Rights About Sharing Your PHI with Family or Representatives. You have the right to tell the Plan your choices about what to share with your personal representative or family members. The Plan may disclose PHI to your personal representative or family

member (i) where the PHI relates to their involvement with your health care treatment or payment for such treatment, (ii) where PHI includes information about your location, general condition or death, and (iii) in certain limited emergency circumstances. In addition, if you are not able to tell the Plan your preference, for example, if you are unconscious, we may share your PHI if we believe it is in your best interest (for example, when needed to lesson a serious or imminent threat to health or safety). However, if you do not want your family member or personal representative to receive information please email the Gannett Benefits Department (hipaacompliance@gannett.com) and request the Disclosure Objection Form.

(2) Right to Request Restrictions. You have the right to request restrictions or limitations on uses of your PHI. You may ask the Plan to not use or disclose certain PHI to carry out treatment, payment or health care operations. You may also request that any part of your PHI not be disclosed to family members or personal representatives identified by you who are involved in your care or the payment for your care. The Plan is generally not required to agree to your request; however, if the Plan does agree to your requested restriction, the Plan will notify you and fulfill this commitment unless the information is needed in an emergency situation, or you revoke the restriction. You should not assume that the Plan has accepted a requested restriction until the Plan confirms its agreement to that restriction in writing. There are some restrictions that are not permitted even with the Plan's agreement.

To request restrictions, please email hipaacompliance@gannett.com and request the Disclosure Objection Form. You must identify: (i) what information you want to limit; (ii) whether you want to limit use, disclosure, or both; and (iii) to whom you want the limits to apply.

(3) Right to Request Communications by Alternative Means. You have the right to request that the Plan contact you in a specific way for communications of PHI (for example, home or office phone) or to send mail to a different address. The Plan will accommodate all reasonable requests if you state that disclosure of your PHI could endanger you. Your request must also specify how or where you wish to be contacted. The Plan will notify you if it agrees to your request for confidential communication. You should not assume that the Plan has accepted your request until the Plan confirms its agreement in writing.

Send requests for restrictions and to receive communications by alternative means or at alternative locations to hipaacompliance@gannett.com.

(4) Right to Inspect and Copy. You have the right to inspect and copy paper or electronic copies of your PHI to the extent that it is contained in a "designated record set." A "designated record set" includes enrollment, payment, billing, claims adjudication and case or medical management record systems maintained by or for the Plan and other information used by or for the Plan to make decisions about your treatment, payment, and health care.

If you request an electronic copy of your PHI maintained by the Plan, then the Plan will grant the request as long as the records can readily be produced in that format. This right extends for as long as the Plan maintains the PHI, but does not apply to certain information defined by law, such as psychotherapy notes or information compiled for use in a civil, criminal, or administrative action. If the Plan denies your request to see and obtain a copy of your PHI, the Plan will tell you why in writing and provide you with instructions for requesting a review of the denial. The requested information will be provided within 30 days if the information is maintained on site, or within 60 days if the information is maintained offsite (or sooner if required under applicable state law). A single 30-day extension, for a total response time of 60 days, is allowed if the Plan is unable to comply with the 30-day deadline. You or your personal representative may request access to the PHI in your designated record set by sending an email request for access to hipaacompliance@gannett.com.

If you request a copy of your PHI, the Plan may charge a reasonable, cost-based fee for copying and, if applicable, postage associated with your request.

(5) Right to Amend. You have a right to amend PHI. You have the right to request that the Plan correct your PHI or a record about you in a designated record set (as described in (5) above) that is inaccurate or incomplete for as long as the PHI is maintained in the designated record set. The Plan has 60 days after the request is made to act on the request. A single 30-day extension is allowed if the Plan is unable to comply with the deadline. The Plan may deny any request that does not include a reason for the request. If the request is denied, the Plan must tell you why. The request may be denied if, for example, your PHI in the Plan's records was not created by the Plan, or if the Plan determines the records containing your PHI are accurate and complete. You or your personal representative may then submit a written statement disagreeing with the denial and have that statement included with any future disclosure of your PHI. Requests for amendment of PHI in a designated record set should be include a statement explaining the reason for the amendment and sent to hipaacompliance@gannett.com.

(6) Right to an Accounting of Disclosures. You have a right to obtain a list of certain disclosures (an "Accounting") of your PHI made by the Plan for the six years prior to the date of your request. Most of the disclosures that the Plan makes of your PHI do not fall under this Accounting requirement because routine disclosures (those related to payment of your claims, for example) generally are excluded from this requirement.

To request an Accounting of disclosures of your PHI, you must submit your request to hipaacompliance@gannett.com. Your request must state the time period you want the Accounting to cover (which must be within the six years prior to the date of your request) and indicate in what form you want the Accounting to be provided (for example, on paper or electronically). If the Accounting cannot be provided within 60 days, the Plan may request an additional 30 days if the Plan gives you a written statement of the reasons for the delay and the date by which the Accounting will be provided.

The first Accounting of disclosures you request within a consecutive 12-month period will be free. If you request more than one Accounting within a consecutive 12-month period, the Plan will charge a reasonable, cost-based fee to fill additional requests.

(7) Right to Receive a Notification of a Breach. You have a right to receive notification in the event of a breach of your PHI. You have the right to be notified if there is a breach of your PHI without unreasonable delay and no later than sixty (60) days following the discovery of the breach by the Plan (or a Business Associate). The notice will include:

- a brief description of what happened, including the date of the breach and the discovery of the breach;
- a description of the type of PHI that was involved in the breach;
- any steps you should take to protect yourself from potential harm resulting from the breach;
- a brief description of the investigation into the breach, mitigation of harm to you and protection against further breaches; and
- contact procedures to answer your questions.

(8) Right to have a Personal Representative Act on Your Behalf. You have a right to designate one or more persons to act on your behalf as your Personal Representative. If you have a Personal Representative, that person can exercise your rights and make choices about your PHI. The Plan will request documentation to confirm that the person has the authority to act on your behalf to access your PHI or to take any action for you. Contact hipaacompliance@gannett.com for more information about how to designate a personal representative.

(9) Right to Paper Copy of this Notice. You have a right to request a paper copy of this Notice at any time by sending an email to hipaacompliance@gannett.com. You have a right to a paper copy of the Notice even if you have agreed to receive this Notice electronically. You may obtain a copy of this Notice on the Plan's website as well. The website address is: www.gannettbenefits.com Login, then click on: > Health & Insurance > Reference Library > Legal Notices > HIPAA Notice of Privacy Policy and Procedures.

In addition to the foregoing rights that you have directly relating to the Plan, you also have the right to request that your provider not disclose your PHI to the Plan if you have paid for a service out-of-pocket in full, and the disclosure is not otherwise required by law. The request for restriction made to the Plan by a provider at your request will only be applicable to that particular service. You must request a restriction for each service thereafter from your provider if you wish it not to be disclosed to the Plan.

The Plan's Duties

The Plan is required by law to maintain the privacy and security of your PHI. The Plan is required to follow the duties and privacy practices described in this Notice and provide a copy to you. The Plan reserves the right to change its privacy practices and to apply the

changes to any PHI received or maintained by the Plan. If a privacy practice is materially changed, a revised version of this Notice and its effective date will be provided to all current Plan participants and will be posted to the Plan's website. When using or disclosing PHI, or when requesting PHI from another covered entity, the Plan will make reasonable efforts not to use, disclose or request more than the minimum amount of PHI necessary to accomplish the intended purpose of the use, disclosure or request, taking into consideration practical and technological limitations. However, the minimum necessary standard will not apply to uses or disclosures that are required by the Plan's compliance with legal requirements.

Your Right to File a Complaint with the Plan or the Secretary

If you believe that your privacy rights have been violated, you have the right to complain to the Plan and to the Secretary of the Department of Health and Human Services. Any complaints to the Plan and requests for further information should be made by email or in writing to the following individual:

Gannett Benefits Department
Gannett Media Corp.
HIPAA Privacy Officer
Email: hipaacompliance@gannett.com
Phone: 855.442.4236

You may also file a complaint with the Secretary of the U.S. Department of Health and Human Services, Hubert H. Humphrey Building, Room 509F, HHH Building, 200 Independence Avenue S.W., Washington, D.C. 20201 and telephone number 877.696.6775 or through the link: www.hhs.gov/ocr/privacy/hipaa/complaints

The Plan encourages you to express any concerns you may have regarding the privacy of your information. The Plan will not retaliate against you for filing a complaint.

This Notice represents the Plan's efforts to summarize the privacy regulations under HIPAA. In the event of a discrepancy between the terms or requirements of this notice and the privacy regulations themselves, the terms of the regulations shall prevail.

Information Security Policies and Standards Enforcement Policy

Policy Owner: IT Security and Data Privacy
Version: 20250101
Employee Scope: All US employees

Purpose

This policy

- defines enforcement of Gannett Information Security Policies and Standards.
- provides the potential consequences for failure to comply with the Gannett Information Security Policies and Standards.

Some policies may include specific enforcement provisions that apply instead of, or in addition to, this policy, where applicable and as noted in the applicable policy.

Definitions and Acronyms

When navigating this policy, it's important to grasp the terminology. Our Glossary of Cybersecurity Terms provides concise definitions for key concepts.

Policy

- Any enforcement actions for Gannett employees will be determined by Gannett's People Resources leadership in consultation with Legal as appropriate.
- Enforcement of Gannett Information Security Policies may include any or all of the following actions in any sequence and at any time (depending on the totality of the circumstances as determined by Gannett):
  - Revocation or reduction of access
  - Disciplinary action, up to and including, termination
  - Prosecution or civil legal action
- In some instances, immediate termination may be appropriate.

Enforcement and Exception

- Compliance with this policy is required under Gannett's Information Security Policies and Standards Enforcement Policy and Gannett may take actions in response to non-compliance as provided under the Enforcement Policy.
- Any exceptions to this policy must follow Gannett's Information Security Policies and Standards Exceptions Policy.

This policy may be updated occasionally by the Company. The current version of this policy, as well as policies referenced in this document, may be viewed on MyLife@Gannett.

Information Security Policies and Standards Exceptions Policy

Policy Owner: IT Security and Data Privacy
Version: 20250101
Employee Scope: All US employees

Purpose

All Gannett employees, accessing Gannett IT (Information Technology) Systems are expected to understand and adhere to Gannett Information Security Policies and Standards. Although deviation from policies is not recommended, as business requirements evolve or technical limitations require, flexibility is necessary to support situations when business necessity or technical limitations can and should take precedence over policies.
This policy provides the exception criteria, process, and procedures to accommodate technical limitations or business use case scenarios not covered by current Gannett Information Security Policies and Standards.

Definitions and Acronyms

When navigating this policy, it's important to grasp the terminology. Our Glossary of Cybersecurity Terms provides concise definitions for key concepts.

Scope

This applies to all Gannett employees, and all Gannett Information Security Policies and Standards.

Policy

Exception Criteria

- An exception must be requested when it is determined that an Information Security Policy or Standard cannot be followed for specific business use situations or scenarios, or technical limitations.
- Any deviation from or exceptions to the published Information Security Policy or Standard requires documented approval by designated leaders of the Technology Compliance department based upon a valid technical limitation or justifiable business use case.

Exception Process

- A request for an exception should be completed and submitted to the Gannett IT Security Policy Exception Portal located : https://gannett.service-now.com/sp?id=sc_cat_item&table=sc_cat_item&sys_id=378764b61bfcc1dc7f78ec217e4bcb00 in Service Catalog - Gannett Service Portal (service-now.com). Documentation of the risk, proposed risk mitigation and business need/justification must be included in the exception request.
- The exception review process must log all findings and results in a central repository that is accessible to all Gannett staff involved in the assessment of the exception request.

- The Technology Compliance team or their designee will review exception requests for completeness and will follow up with requesters, as necessary.
- If deemed necessary, the Technology Compliance team will engage the Security Review Council (SRC) for a technical assessment of the request.
- The SRC will perform and document a risk assessment of the request, the proposed mitigation, and the benefit of allowing the exception. This could involve one or more meetings with the requester.
- The SRC will make its recommendation to the Technology Compliance team upon completion of its risk assessment.
- The Technology Compliance team will approve, deny, or require additional compensating controls (risk mitigation steps) for the exception.
- If there is significant business benefit in expedited approval of an exception (or significant business risk in delaying approval), the exception may be tentatively approved by one of the following:
  - A member of SRC leadership
  - A member of the Technology Compliance leadership Team
- The person or group that granted an expedited tentative approval must inform the Technology Compliance team within 24 hours.
- Any expedited tentative approval must be reviewed by the Technology Compliance team promptly, not to exceed 30 days from the issuance of the expedited approval.
- Expedited tentative approval does not exempt the exception from having to follow the complete exception review process, which may lead to either denial (revocation of tentative approval), full approval, or additional compensating controls.
- Exceptions will be reviewed no less than annually, which will include engaging with the requester, review and reapproval by the Technology Compliance Leadership team, or a determination to amend the affected policy to include the exception.

Enforcement and Exception

- Compliance with this policy is required under Gannett's Information Security Policies and Standards Enforcement Policy and Gannett may take actions in response to non-compliance as provided under the Enforcement Policy.
- Any exceptions to this policy must follow Gannett's Information Security Policies and Standards Exceptions Policy.

This policy may be updated occasionally by the Company. The current version of this policy, as well as policies referenced in this document, may be viewed on MyLife@Gannett.

Information Security Risk Management Policy

Policy Owner: IT Security and Data Privacy
Version: 20250101
Employee Scope: All US employees

Purpose

The Information Security Risk Management Policy is intended to help manage security and privacy risks, and to facilitate compliance with applicable laws and regulations, as well as protect the confidentiality, integrity, and availability of Information Technology (as defined below) and its customers' proprietary and confidential information and personal information of its consumers and employees entrusted to its care (collectively "Information and Technology Resources") and enable informed decisions regarding risk tolerance and acceptance. This document provides guidelines for managing security and privacy risks, and:

- To ensure that managing system-related security and privacy risk is consistent with the mission and business objectives of the organization and risk management strategy established by the senior leadership.
- To achieve privacy protection for individuals and security protection for information and information systems through the implementation of appropriate risk response strategies.
- To facilitate the integration of security and privacy requirements and controls into the enterprise architecture, acquisition processes, and systems engineering processes.

"Information Technology" is defined as all Gannett systems, including computers, laptops and mobile devices (e.g., smartphones and tablets) provided by Gannett, and software owned, leased, operated, processed, and/or exchanged, as well as servers, networks, data centers, infrastructure, databases, and other information technology, owned, used, or operated by or on behalf of Gannett (e.g. cloud services).

Definitions and Acronyms

When navigating this policy, it's important to grasp the terminology. Our Glossary of Cybersecurity Terms provides concise definitions for key concepts.

Scope

This policy and supporting procedures encompass all Information and Technology Resource components and assets that are controlled by Gannett, or a third-party on behalf of Gannett, and applies to any system or system components, both internally and externally, that interact with these Information and Technology Resources.

- Internal system components are those owned, operated, maintained, and controlled by Gannett and includes but is not limited to all network devices (firewalls, routers, switches, load balancers, other network devices), servers (both physical and virtual servers, along with the operating systems and the underlying application(s) that reside on them) and any other system components deemed in scope.
- External system components are those owned, operated, maintained, and controlled by any entity other than Gannett, but for which such external resources may impact the

confidentiality, integrity, and availability of Gannett Information and Technology Resources.
- While Gannett does not have the ability to provision, harden, secure, and deploy another organization's system components, Gannett will follow best practices by obtaining all relevant information demonstrating that such systems are safe and secure.

Risk Management Roles and Responsibilities

Implementing and adhering to organizational policies and procedures is a collaborative effort, requiring a true commitment from all personnel, including executive leaders, management, and employees along with vendors, contractors, and other relevant third parties. Additionally, by being aware of one's roles and responsibilities as it pertains to Gannett information systems, all relevant parties are helping promote the confidentiality, integrity, and availability principles for information security with the growing of cybersecurity challenges.

Chief Information Security Officer	Responsible for implementing systems and specifications to facilitate compliance with this policy. Responsible for developing and maintaining security policies, procedures, and control techniques to address security requirements. Establishes an information security risk management strategy for the organization that includes business feedback of risk tolerance.
Security Team	Responsible for ensuring that risk assessments are comprehensive, accurate, transparent, and void of conflict. The team is responsible for ensuring that key perspectives and inputs are at the table when assessing impact, threat, and risk and that remediation efforts and resource requests are clearly and comprehensively presented to senior management and key stakeholders.
Legal	Responsible for providing legal advice to guide and direct the information security program's compliance with applicable laws, and mitigation of legal risks, legal review of the Company's privacy and risk management policies and incident response activities.
Chief Privacy Officer	Documents privacy compliance requirements and is assigned as the owner of the privacy program in the organization. Responsible for ensuring that privacy considerations are factored into the risk management program.
Management	Responsibilities include providing overall direction, guidance, leadership, and support for the entire information systems environment, while also assisting other applicable personnel in their day-to-day operations.
System Owners	Responsible for addressing the operational interests of the user community (i.e., users who require access to the system to satisfy mission, business, or operational requirements) and for ensuring compliance with security requirements. Decides who has access to the system (and with what types of privileges or access rights).

All Employees	Responsibilities include adhering to the organization's information security policies, procedures, practices, and not undertaking any measure to alter such standards on any Gannett system components. Users are to report instances of non-compliance to management, specifically those by other users. Users, while undertaking day-to-day operations, may also notice issues that could impede the safety and security of Gannett system components and are to also report such instance immediately to management/leadership.

Policy

Gannett will develop and maintain an Information Security Risk Management process and other tools and mechanisms to frame, assess, respond, and monitor information security related risks.

Risk Assessments

Risk assessments to applicable Information and Technology Resources must be conducted at least annually. Additionally, when significant changes at Gannett occur, a risk assessment must be performed to assess the impact those changes have on organizational risk. The following is a list of events that may require engaging the risk management team (the Security Team) to ensure an assessment is made:

- Introduction of new projects and processes
- External factors, such as regulatory, litigation, consumer pressure, environmental, geopolitical, and economic stability
- Changes in the scope of current products, processes, or projects
- Any event that changes the scope of data being collected or processed
- Significant change to the business model or a pivot
- Leadership or management change that could affect risk appetite
- Major changes to any critical Information and Technology Resources
- Changes to or introductions of business relationships, vendors, and partnerships
- Mergers and acquisitions
- Using risk assessment results to inform and guide decision makers on the protection of PHI/ePHI and PI/PII

Security and Privacy by Design

Gannett policy also applies the concepts of security and privacy by design to all stages of design, development, deployment, and management of relevant projects with an impact on Information and Technology Resources or the privacy rights of individuals. Privacy and security by design refers to considering privacy and security at every level of all such projects. This ongoing consideration ensures better design and planning compared to only reviewing privacy and security considerations at the end of a project before it goes live.

Risk Transparency

Addressing the possibility of fraudulent or inaccurate claims or activities in risk assessments is another factor in successfully managing risk at Gannett. All individuals who participate in risk management must ensure that they act ethically, honestly, and transparently. Ensuring that conflicting pressures or incentives do not influence

assessment results and outcomes is ultimately the responsibility of the VP - Information Security and Compliance. That said, everyone must play a part in ensuring that risk assessments performed at Gannett are mindful of:

- Opportunities where fraud or inaccuracy could occur
- Incentives or pressures to commit fraudulent acts or underplay risks to the business
- How fraudulent or inaccurate reports could be justified at various levels of management

If a concern arises, it must be brought to the VP - Information Security and Compliance (CISO), Legal or senior management.

Risk management Process

The Risk Management system is dynamic and is designed to adapt to Gannett's developments and any changes to the organization's risk profile over time. The Risk Management system is based on a structured and systematic process which considers Gannett's internal and external risks. The Risk Management system includes the Risk Management Policy and is continuous throughout the lifecycle as risks are identified and in turn treated. The main elements of the risk management process are as follows:

Communicate and Consult

Communicate and consult with internal and external stakeholders as appropriate at each stage of the risk management process and concerning the process as a whole.

Establish the Context

Establish the external, internal, and risk management context in which the rest of the process will take place. The criteria against which risk will be evaluated should be established and the structure of the analysis defined.

Identify Risks

Gannett will identify risks (threats or opportunities) following established procedures and the Risk Management Policy and document the risk in the security and risk assessment register. Identify where, when, why, and how events could prevent, degrade, delay, or enhance the achievement of Gannett's objectives.

Record Risks

Any risks identified should be documented on a security and risk assessment register, to be maintained by the VP – Information Security and Compliance (CISO) or designee. Document the net effect of all identified threats and opportunities, by assessing:

- Likelihood of threats and opportunities (risks) to occur
- Impact of each risk
- Treatment of Risk (Mitigation or Acceptance)

Evaluate Risks and Respond

Compare the estimated levels of risk against the pre-established criteria and consider the balance between potential benefits and adverse outcomes. This enables decisions to be made about the extent and nature of treatments required. Gannett will review the security

and risk assessment register and plan actions or responses that are designed to mitigate threats and maximize opportunities.

Monitor and Review
After the risk responses and implementation has been completed, the performance of the risk management solution will be monitored, measured, and reviewed at least on an annual basis as determined by the Information Security Team and other risk owners. Plans are likely to change over time as business initiatives change. Risk may come from any internal or external event that may affect the ability to operate efficiently and effectively.

Internal Risks are those risks that specifically relate to Gannett business and are generally within the organization's control. This includes risks such as personnel, strategic, operational, and financial risk.

External Risks are those risks that are outside the control of Gannett. This includes risks such as the COVID19 virus and its ability to morph into other variants, legislative and congressional decisions, court rulings, litigation, US military command decisions, and market conditions.

Enforcement and Exception

- Compliance with this policy is required under Gannett's Information Security Policies and Standards Enforcement Policy and Gannett may take actions in response to non-compliance as provided under the Enforcement Policy.
- Any exceptions to this policy must follow Gannett's Information Security Policies and Standards Exceptions Policy.

This policy may be updated occasionally by the Company. The current version of this policy, as well as policies referenced in this document, may be viewed on MyLife@Gannett.

Information Technology Physical Security Policy

Policy Owner: IT Security and Data Privacy
Version: 20250101
Employee Scope: All US employees who work with all Gannett Devices which are owned and/or controlled by Gannett and/or an affiliate of Gannett including entities managed by Gannett pursuant to a Joint Operating Agreement, or joint ventures. This includes Gannett Devices that are owned and/or controlled by Gannett and deployed outside of Gannett properties.

Purpose

- This policy defines the physical security requirements for Gannett owned and/or controlled technology devices and assets such as servers, network equipment, desktop computers, printers, laptops, and other mobile systems ("Gannett Devices") to protect against malicious events, including without limitation loss or unauthorized access.
- This policy will not address most physical security issues regarding non-malicious events (unexpected power outages, natural disasters, etc.).

Definitions and Acronyms

When navigating this policy, it's important to grasp the terminology. Our Glossary of Cybersecurity Terms provides concise definitions for key concepts.

Policy

General Policy

- Use the Sensitive Data Protection Policy to help determine the appropriate level of physical security. Higher levels of sensitive data require higher levels of physical security.
- All Gannett Devices must be labeled and periodically inventoried and tracked.
- Assets associated with information and information processing facilities that store, process, or transmit classified information shall be identified and an inventory of these assets shall be created and maintained.
- Assets maintained in the inventory shall be owned by a specific individual or group within Gannett.
- Annual security reviews of physical locations include server rooms and/or any other areas where production equipment is housed.
- Building/room access controls. Any areas with Gannett Devices or Systems should have some method to monitor and/or control access:
  - At a minimum, areas should be periodically monitored.
  - Whenever possible, access should be locked (keys, smart cards, biometrics, etc.)
  - Modify access requirements when necessary.
  - Revoke physical access identification for terminated personnel and visitors.
  - For areas in scope for PCI (Payment Card Industry), access controls and/or video cameras should be used to monitor physical access to entry and exit points.
  - Retention of data from video cameras or other access controls must be stored for at least three months.
  - Procedures and processes to manage and to clearly identify visitors and new

Gannett onsite personnel from existing Gannett personnel through identification such as ID badges should be in place.
    - Visitors must be authorized before access may be granted and visitor identification must be set to expire according to the authorized access period.
    - Visitors must wear the visitor identification while on Gannett premises and return the issued identification when the authorized period has expired or upon departure.
    - Visitors must always be escorted in areas where cardholder data is processed or maintained.
    - Documentation to record visitors' physical access to Gannett facilities, computer rooms and data centers where cardholder data is stored or transmitted must be used.
    - Visitor log documentation retention must be set for at least three months and the logs must contain the visitor's name, company name, and the name of the Gannett personnel providing physical access authorization.
  - Vendors must be monitored when performing maintenance on computing devices.
    - When maintenance is performed on computing devices where the device cannot be monitored, sensitive data must be removed. Examples include sending laptops or hard drives to a vendor for maintenance. (See the Sensitive Data Protection Policy for information on how to protect data.)
  - When disposing of or reallocating computing and storage devices, all Gannett data must be removed using techniques compliant with the Data Erasure Standard.
    - For systems in-scope for PCI compliance, destruction of the storage media must be documented.

Server and Network Equipment

- Servers, network equipment and their console equipment should have greater physical security than public use areas. These factors should be followed:
  - Device physical access controls. Measures must be implemented to prevent unauthorized physical access to servers and network devices. These include but are not limited to:
    - Installation in a rack. A rack locking mechanism should be used when available.
    - Any unused physical ports (USB, monitor, serial, interfaces, etc.) should be disabled.
    - Unnecessary exposure of network and power cables, wireless access points, gateways, and handheld devices should be limited as much as possible.
  - Building/room physical access controls. Measures must be used to ensure that only authorized personnel have access.
  - Reduce risks from environmental hazards (temperature/moisture extremes, electrical power, fire, etc.) by:
    - Reviewing environment considerations when installing new server and network equipment.
    - Whenever possible, install systems to control and/or monitor environmental conditions.
  - Some network equipment, such as LAN switches or wireless access points, may require installation in public use areas. As much additional protection should be

used, including but not limited to:
- Installing network equipment in locked cabinet or cage.

Removable Media
- Data stored on removable media (backup tapes, CDs, USB drives) must have the same level of physical security as the Gannett Device it originated from.

Desktop Systems
- The following measures must be used for systems accessed by end-users:
  - Additional hardware security measures should be considered for higher risk systems or higher risk situations.
  - When available, automated methods must be used to lockout a system when the session has been idle for more than 15 minutes. The lockout must require the user to re-enter their password to reactivate the session.

Laptops and other Mobile Devices
- Laptops and mobile devices must not be left unattended in public access areas.
- Laptops and mobile devices must not be checked with luggage when travelling; they must be included as a carry-on bag in the passenger compartment.

Vendor Owned and/or Controlled Devices
- Vendor physical security policies and practices applicable to vendor owned and/or controlled devices used to provide services to Gannett must be reviewed for compliance with this Information Technology Physical Security Policy, as applicable (which may be provided by review of available audit or attestation documentation).

Enforcement and Exception

- Compliance with this policy is required under Gannett's Information Security Policies and Standards Enforcement Policy and Gannett may take actions in response to non-compliance as provided under the Enforcement Policy.
- Any exceptions to this policy must follow Gannett's Information Security Policies and Standards Exceptions Policy.

This policy may be updated occasionally by the Company. The current version of this policy, as well as policies referenced in this document, may be viewed on MyLife@Gannett.

Insider Trading

Policy Owner: Legal
Version: 20240701
Employee Scope: All employees

POLICY ON INSIDER TRADING

In the course of conducting the business of Gannett Co., Inc. and its subsidiaries (collectively, the "Company"), you may come into possession of material information about the Company or other entities that is not available to the investing public ("material nonpublic information"). You have a legal and ethical obligation to maintain the confidentiality of material nonpublic information. In addition, it is illegal and a violation of Company policy to purchase or sell securities of the Company or any other entity while you are in possession of material nonpublic information about the Company or that other entity. The Company has adopted this policy on insider trading (the "Policy") in order to ensure compliance with the law and to avoid even the appearance of improper conduct by anyone associated with the Company. We have all worked hard to establish the Company's reputation for integrity and ethical conduct, and we are all responsible for preserving and enhancing this reputation. If you have any questions or uncertainties about this Policy or a proposed transaction, please ask the Chief Legal Officer.

SCOPE OF COVERAGE

The restrictions set forth in this Policy apply to all Company officers, directors and employees (collectively, "Insiders"), wherever located, and to (i) their spouses, minor children, and anyone else sharing the same household (collectively, "Family Members"); (ii) any other person or entity over which the officer, director or employee exercises substantial influence or control; and (iii) any trust or other estate in which an officer, director or employee has a substantial beneficial interest or as to which they serve as trustee or in a similar fiduciary capacity (collectively (ii) and (iii), "Controlled Entities").

This Policy and its prohibitions apply in relation to any material, nonpublic information you obtain in the course of the Company's business concerning the Company or other companies. If you acquire material, nonpublic information, you may not trade in the securities of the Company or any other company on the basis of such information or disclose or "tip" any such information until after such information has been disclosed to the public. Material, non-public information about other companies should be treated in the same way as comparable information relating to the Company.

This Policy applies to transactions in securities, including without limitation, common stock, preferred stock, bonds and other debt securities, options to purchase common stock, convertible debentures and warrants, as well as derivative securities, such as exchange-traded put or call options or swaps. See the sections entitled "Special Transactions" and "Prohibited Transactions" for further discussion of certain types of securities and transactions.

KEY EMPLOYEES

When discussed in this Policy, "Key Employees" shall mean:

- each member of the Company's Board of Directors;
- the Company's Section 16 Officers;

- Company employees with the job level of Executive Vice President and above; and
- any other employee who is notified by the Company that they are considered a Key Employee for the purposes of this Policy.

INDIVIDUAL RESPONSIBILITY

Persons subject to this Policy are individually responsible for complying with this Policy and ensuring the compliance of any Family Member or Controlled Entity whose transactions are subject to this Policy. Accordingly, you should make your Family Members aware of the need to confer with you before they trade in securities, and you should treat all such transactions for the purposes of this Policy and applicable securities laws as if the transactions were for your own account. In all cases, the responsibility for determining whether an individual is in possession of material nonpublic information rests with that individual, and any action on the part of the Company or any other employee pursuant to this Policy (or otherwise) does not in any way constitute legal advice or insulate an individual from liability under applicable securities laws.

MATERIAL NONPUBLIC INFORMATION

What is Material Information?

Information is generally regarded as material if:

- There is a substantial likelihood that a reasonable investor would consider the information important in determining whether to trade in a security; or
- The information, if made public, likely would affect the market price of a company's securities.

Information may be material even if it relates to future, speculative or contingent events and even if it is significant only when considered in combination with publicly available information. Material information can be positive or negative. Nonpublic information can be material even with respect to companies that do not have publicly traded stock, such as those with outstanding bonds or bank loans.

Depending on the facts and circumstances, information that could be considered material includes, but is not limited to:

- Earnings announcements or estimates, or changes to previously released announcements or estimates;
- Other unpublished financial results or forecasts;
- Write-downs and additions to reserves for bad debts;
- Expansion or curtailment of operations;
- Significant changes in capital investment plans;
- Major litigation or government actions;
- Significant labor disputes;
- Mergers, acquisitions, tender offers, joint ventures or changes in assets;
- Changes in analyst recommendations or debt ratings;
- Events regarding the Company's securities (e.g., defaults on senior securities, calls of securities for redemption, repurchase plans, stock splits, changes in dividends,

changes to the rights of securityholders, or public or private sales of additional securities);
- Changes in control of the Company or extraordinary management developments;
- Changes in the Company's pricing or cost structure;
- Extraordinary borrowing or other financing transactions out of the ordinary course;
- Liquidity problems;
- Changes in auditors or auditor notification that the Company may no longer rely on an audit report;
- Cybersecurity incidents;
- Development of a significant new product, process, or service;
- New inventions or discoveries; and
- The gain or loss of a significant customer or supplier.

What is Nonpublic Information?
Information is considered to be nonpublic unless it has been adequately disclosed to the public, which means that the information must be publicly disseminated and sufficient time must have passed for the securities markets to digest the information.

It is important to note that information is not necessarily public merely because it has been discussed in the press, which will sometimes report rumors. You should presume that information is nonpublic unless you can point to its official release by the Company in at least one of the following ways:
- Public filings with the Securities and Exchange Commission; or
- Issuance of a press release that is widely disseminated in a manner making it generally available to investors.

You may not attempt to "beat the market" by trading simultaneously with, or shortly after, the official release of material information.

Twenty-Twenty Hindsight. If securities transactions ever become the subject of scrutiny, they are likely to be viewed after-the-fact with the benefit of hindsight. As a result, before engaging in any transaction you should carefully consider how the transaction may be construed in the bright light of hindsight.

"TIPPING" MATERIAL NONPUBLIC INFORMATION IS PROHIBITED

In addition to trading while in possession of material nonpublic information, it is also illegal and a violation of this Policy to convey such information to another party ("tipping") if you know or have reason to believe that the other party will misuse such information by trading in securities or passing such information to others who will trade. This applies regardless of whether the "tippee" is related to the Insider or is an entity, such as a trust or a corporation, and regardless of whether you receive any monetary benefit from the tippee.

SPECIAL TRANSACTIONS

The trading restrictions in this Policy do not apply in the case of the following transactions, except as specifically noted:

- **Employee Stock Purchase Plan**: The trading restrictions in this Policy do not apply to purchases of Company stock in an employee stock purchase plan, if any, resulting from periodic payroll contributions to the plan under an election made at the time of enrollment in the plan. The trading restrictions also do not apply to purchases of Company securities resulting from lump sum contributions to any employee stock purchase plan, provided that you elected to participate by lump sum payment at the beginning of the applicable enrollment period. The trading restrictions do apply, however, to an election to participate in any employee stock purchase plan for any enrollment period, changes in payroll contributions and to sales of Company stock purchased under the plan.
- **401(k) Plan**: The trading restrictions in this Policy do not apply to purchases of Company stock in a 401(k) plan, if any, resulting from periodic contributions of money to the plan pursuant to payroll deduction elections. The trading restrictions do apply, however, to elections made under a 401(k) plan to (a) increase or decrease the percentage of periodic contributions that will be allocated to the Company stock fund, (b) make an intra-plan transfer of an existing account balance into or out of the Company stock fund, (c) borrow money against a 401(k) plan account if the loan will result in a liquidation of some or all of a Company stock fund balance, and (d) pre-pay a plan loan if the pre-payment will result in allocation of loan proceeds to the Company stock fund.
- **Stock Option Plans**: While the trading restrictions in this Policy do apply to sales of Company common stock received upon the exercise of stock options in which the proceeds are used to fund the option exercise price (i.e., a cashless exercise of options) or related taxes, the trading restrictions in this Policy do not apply to exercises of stock options where no Company common stock is sold in the market to fund the option exercise price or related taxes (i.e. a net exercise or where cash is paid to exercise the option) or to the exercise of a tax withholding right pursuant to which a person has elected to have the Company withhold shares subject to an option to satisfy tax withholding requirements.
- **Restricted Stock Awards**: The trading restrictions in this Policy do not apply to the vesting of restricted stock, or the exercise of a tax withholding right pursuant to which you elect to have the Company withhold shares of stock to satisfy tax withholding requirements upon the vesting of any restricted stock. The trading restrictions do apply, however, to any market sale of restricted stock.
- **Dividend Reinvestment Plan**: The trading restrictions in this Policy do not apply to purchases of Company securities under a dividend reinvestment plan, if any, resulting from your reinvestment of dividends paid on Company securities. The trading restrictions do apply, however, to voluntary purchases of Company securities resulting from additional contributions you choose to make to a dividend reinvestment plan, and to your election to participate in the plan or change your level of participation in the plan. The trading restrictions also apply to your sale of any Company securities purchased pursuant to any dividend reinvestment plan.

GIFTS OF SECURITIES

Bona fide gifts of securities are not transactions subject to this Policy, unless the person making the gift has reason to believe that the recipient intends to sell the Company

securities while the officer, director, or employee is aware of material nonpublic information, or the person making the gift is subject to other Company directed trading restrictions (in which case preclearance from the Chief Legal Officer is required). All Key Employees must notify the Chief Legal Officer at least five business days before the date a bona fide gift of securities is made.

PROHIBITED TRANSACTIONS

Due to the heightened legal risk associated with the following transactions, individuals subject to this Policy may not engage in the following:

- **Margin Accounts and Pledges**: Because a margin sale or foreclosure sale may occur at a time when the pledgor is aware of material nonpublic information or otherwise is not permitted to trade in Company securities, you may not hold Company securities in a margin account or otherwise pledge Company securities as collateral for a loan.
- **Hedging Transactions**: You may not engage in hedging transactions such as (but not limited to) zero-cost collars, equity swaps, forward sale contracts, and short-selling the Company's securities. Hedging transactions may allow a director, officer, or employee to continue to own Company securities, but without the full risks and rewards of ownership. This may lead to the director, officer, or employee no longer having the same objectives as the Company's other shareholders.

TRADING PLANS

Notwithstanding the prohibition against insider trading, Rule 10b5-1 under the Securities Exchange Act of 1934, as amended ("Rule 10b5-1") and Company policy permit employees and others subject to this Policy to trade in Company securities regardless of their awareness of material nonpublic information if the transaction is made pursuant to an approved pre-arranged written trading plan ("Trading Plan") that was entered into when the person was not in possession of material nonpublic information and that complies with the requirements of Rule 10b5-1. Anyone subject to this Policy who wishes to enter into a Trading Plan must submit the Trading Plan to the Chief Legal Officer for approval at least five business days prior to the planned entry into the Trading Plan. In general and among other things, Trading Plans must:

- be adopted by a person when they are not in possession of material nonpublic information about the Company and not subject to a blackout period under this Policy;
- have a cooling-off period consistent with Rule 10b5-1, meaning that the first trade under the Trading Plan cannot be executed until:
    - for Key Employees: the later of (i) 90 days after adopting the Trading Plan; or (ii) two business days following disclosure of the financial results for the for the fiscal quarter in which the Trading Plan was adopted or modified (but not to exceed 120 days following the Trading Plan adoption or modification);
    - for other employees: 30 days after adopting the Trading Plan;
- include a certification that the person is adopting the Trading Plan in good faith and not as part of a plan or scheme to evade the prohibitions of Rule 10b5-1, will act in good faith for the duration of the Trading Plan, and that, as of the adoption date, the person is not in possession of any material nonpublic information regarding the Company; and
- give a third party the discretionary authority to execute such purchases and sales, outside the person's control, so long as such third party does not possess any material

nonpublic information about the Company, or explicitly specify the security or securities to be purchased or sold, the number of shares, the prices and/or dates of transactions, or other formula(s) describing such transactions.

You may not enter into overlapping Trading Plans (subject to certain exceptions) and may only enter into one single-trade Trading Plan during any consecutive 12-month period (subject to certain exceptions).

Once the Trading Plan is approved and adopted, you must not exercise any subsequent influence over the amount of securities to be traded, the price at which they are to be traded or the date of the trade. You may amend or replace a Trading Plan only during periods when trading is permitted in accordance with this Policy, and you must submit any proposed amendment or replacement of a Trading Plan to the Chief Legal Officer for approval at least five business days prior to adoption. You must provide notice to the Chief Legal Officer prior to terminating a Trading Plan. You should understand that modifications or terminations of a Trading Plan likely restart the cooling-off period and may call into question your good faith in entering into the Trading Plan (and therefore may jeopardize the availability of the affirmative defense against insider trading allegations).

In addition to Trading Plans under Rule 10b5-1, you must contact the Chief Legal Officer if you wish to enter into a written arrangement to trade in the Company's securities that does not fall under Rule 10b5-1. Any such plan is subject to the same approval process as detailed above.

BLACKOUT PROVISIONS; PRECLEARANCE & REPORTING REQUIREMENTS

Blackout Periods

Insiders (and their Family Members and Controlled Entities) may only trade in the Company's securities for their own account during the Company's designated window periods, which are open when the Company is not in a blackout period (except by means of a Trading Plan established in compliance with this Policy). The Company's blackout periods begin 15 days prior to the end of each fiscal quarter of the Company and end upon the market closing on the second full day of trading following the public release by the Company of its quarterly or year-end financial results.

In addition, directors, officers, and certain employees may be instructed not to trade in the Company's securities due to certain specific events, which will trigger an "event-specific blackout." If this happens, you may not engage in any trade of any type under any circumstances during the event-specific blackout until you are informed that the event-specific blackout no longer applies. Because the existence of an event-specific blackout may itself be material nonpublic information, you must not inform anyone of the existence of this type of trading restriction. Further, any person that is made aware of the reason for an event-specific prohibition on trading shall not disclose the reason for the prohibition. The failure of the Chief Legal Officer or the Company's legal department to notify you of an event-specific blackout will not relieve you of the obligation not to trade while in possession of material nonpublic information.

The Chief Legal Officer may make limited exceptions to trading during blackout periods upon a tangible demonstration of a personal hardship by an Insider and the conclusion that the person requesting the exception is not in possession of material nonpublic information. All determinations in this regard will be final and not subject to further review. Hardship exceptions are granted infrequently and only in exceptional circumstances.

Even if a blackout period is not in effect, at no time may you trade in Company securities if you are in possession of material nonpublic information about the Company.

Preclearance & Reporting Requirements
All Key Employees (including Family Members and Controlled Entities), must have any transaction in the Company's securities pre-cleared by the Chief Legal Officer, except for trades under a Trading Plan established in compliance with this Policy. A request for pre-clearance should be submitted to the Chief Legal Officer at least five business days before the proposed transaction (or such shorter period as the Chief Legal Officer may determine) and any transaction subject to the pre-clearance request may not be effected unless given clearance to do so.

To request pre-clearance, contact the Chief Legal Officer with the following information: the type of trade, anticipated amount of Company securities in the trade, and who would be making the trade (i.e., the Key Employee, a Family Member or Controlled Entity). The Chief Legal Officer is under no obligation to approve a transaction submitted for pre-clearance and may determine not to permit the transaction. Such persons seeking clearance may not be informed of the reason they may not trade. If a person seeks pre-clearance and is denied, the person must not initiate the transaction in Company securities for which pre-clearance was denied and should not inform any other person of the denial.

When a request for pre-clearance is made, the requestor should carefully consider whether they may be aware of any material nonpublic information about the Company, and should describe fully those circumstances to the Chief Legal Officer. The requestor should also indicate whether they have effected any non-exempt "opposite-way" transactions within the past six months, and should be prepared to report the proposed transaction on an appropriate Form 4 or Form 5, if applicable. The requestor should also be prepared to comply with SEC Rule 144 and file a Form 144, if necessary, at the time of any sale. Any pre-clearance approval (unless revoked) is valid only for two business days following the day on which it was granted. If a transaction for which pre-clearance has been granted is not effected within such period, the transaction must be pre-cleared again.

All transactions by Key Employees (including Family Members and Controlled Entities), must be pre-cleared and notification of the effectiveness of such pre-cleared transaction must be given to the Chief Legal Officer no later than the date of the transaction.

SAFEGUARDING CONFIDENTIAL INFORMATION

If material information relating to the Company or its business has not been disclosed to the general public, such information must be kept in strict confidence and should be discussed only with persons who have a "need to know" the information for a legitimate

business purpose. The utmost care and circumspection must be exercised at all times in order to protect the Company's confidential information. In addition to the prohibitions set forth in the Company's Code of Business Conduct and Ethics on the use of confidential information the following practices should be followed to help prevent the misuse of confidential information:

- Avoid discussing confidential information with colleagues in places where you may be overheard by people who do not have a valid need to know such information, such as on elevators, in restaurants and on airplanes.
- Take great care when discussing confidential information on speaker phones or on cellular phones in locations where you may be overheard.
- Do not discuss confidential information with relatives or social acquaintances.
- Do not give your computer IDs and passwords to any other person. Password protect computers and log off when they are not in use.
- Always put confidential documents away when not in use and, based upon the sensitivity of the material, keep such documents in a locked desk or office. Do not leave documents containing confidential information where they may be seen by persons who do not have a need to know the content of the documents.
- Be aware that the Internet and other external electronic mail carriers are not secure environments for the transmission of confidential information.
- Comply with the specific terms of any confidentiality agreements of which you are aware.

Upon termination of your employment, you must return to the Company all physical and electronic copies of confidential information as well as all other material embodied in any physical or electronic form that is based on or derived from such information, without retaining any copies.

RESPONDING TO REQUESTS FOR INFORMATION

You may find yourself the recipient of questions concerning various activities of the Company. Such inquiries can come from the media, securities analysts and others regarding the Company's business, rumors, trading activity, current and future prospects and plans, acquisition or divestiture activities and other similar important information. Under no circumstances should you attempt to handle these inquiries without prior authorization. Only Company individuals specifically authorized to do so may answer questions about or disclose information concerning the Company.

- Refer requests for information regarding the Company from the financial community, such as securities analysts, brokers or investors, to the head of the Company's Investor Relations.
- Refer requests for information regarding the Company from the media or press to the Company's Chief Communications Officer.
- Refer requests for information from the Securities Exchange Commission or other regulators to the Chief Legal Officer.

POST-TERMINATION TRANSACTIONS

This Policy continues to apply to transactions in Company securities even after termination of service with the Company. If an individual is in possession of material nonpublic

information when their service terminates, that individual may not trade in Company securities or in the securities of any other company on the basis of such information, until that information has become public or is no longer material.

CONSEQUENCES OF NON-COMPLIANCE

Failure to observe this Policy could lead to severe adverse consequences for the Company and for you. Insider trading violations are pursued vigorously by federal and state enforcement authorities. Consequences for an individual trading on inside information (or tipping others) is severe, and could include significant civil penalties, criminal fines and imprisonment, immediate termination for cause, and irreparable reputational damage.

In addition, the Company may also be subject to civil and criminal penalties for failing to take appropriate steps to prevent insider trading, and trading in the Company's securities could be halted or suspended. Further, even the appearance of impropriety relating to insider trading in the Company's securities could impair investor confidence in the Company.

The Board will be responsible for making, or may delegate the responsibility to make, determinations on a case-by-case basis of whether this Policy has been violated and, if so, the appropriate action to be taken by the Company in response. Sanctions for violations of this Policy may include whatever appropriate action the Board or delegated authority deems advisable, including immediate termination of employment or other appropriate disciplinary action. Such determinations will be final and not subject to further review.

REPORTING VIOLATIONS/SEEKING ADVICE

You should refer suspected violations of this Policy to the Chief Legal Officer. In addition, if you receive:

- material nonpublic information that you are not authorized to receive or that you do not legitimately need to know to perform your employment responsibilities, or
- confidential information and are unsure if it is within the definition of material nonpublic information or whether its release might be contrary to a fiduciary or other duty or obligation,

you should not share it with anyone. Consulting your colleagues can have the effect of exacerbating the problem. Containment of the information, until the legal implications of possessing it are determined, is critical. To seek advice about what to do under those circumstances, you should contact the Chief Legal Officer.

ACKNOWLEDGEMENT

All persons subject to this Policy must acknowledge their understanding of, and intent to comply with, this Policy.

Mobile Phone Policy

Policy Owner: Finance
Version: 20240227
Employee Scope: All employees

1. Purpose

This document defines the mobile device usage and reimbursement policy for Gannett employees who use either company or personal mobile devices in connection with performing their job duties. For purposes of this policy, a mobile device includes cell phones, smartphones, tablets, MiFi's and similar devices.

This policy applies to all employees of Gannett and its direct and indirect subsidiaries (the "Company"). *Please note that the Company understands and will comply with applicable law regarding collective bargaining related to this policy as it relates to employees covered by a collective bargaining agreement, represented by a union or who work for an entity that is part of a Joint Operating Agreement.*

The policy will be reviewed at a minimum annually to account for changes in carrier offerings, the ubiquity of individuals owning smartphones, and carrier plans providing unlimited talk, text, and data being widely available.

This policy is subject to change without notice.

2. Definitions

1) Employee Liable - The employee owns the device and makes full payment for plans, usage, hardware, and services. Reimbursement levels are set by the Company based on their approved use.
2) Company Liable - The Company owns and provides the device and makes full payment for approved plans, usage, hardware, and services. Effective December 3, 2021, the Company will be phasing out eligibility for individual Company Liable mobile devices.

3. Employee Liable

- Employee owns their mobile device and makes full payment for their plan, usage, hardware, and services.
- Reimbursement level set by the Company not to exceed $50 per month and may not exceed employee's cost of phone plan charges for their individual line.
    - Eligible employees may include Content staff, Sales, Distribution staff and other roles the Company determines necessarily require the business use of a personal mobile device.
- Reimbursement Standards:
    - The Company understands the importance of providing an employee with adequate devices and technology to facilitate internal and external communications and meetings, including business phones (at Company facilities) and software-based communications tools (i.e., Microsoft Teams and

Vonage) that can be used on the Company-provided desktop/laptop. Accordingly, the use of an employee's personal mobile devices for business purposes should be limited to only those circumstances where the employee is unable to use a Company-provided device or technology, for instance, during approved business travel when internet is not available to enable calls through Microsoft Teams or other Company provided programs on the employee's laptop. Therefore, the Company only reimburses employees who use personal mobile devices when doing so is actually necessary for the employee to perform his/her job responsibilities and is done at the direction/approval of the employee's supervisor. An employee who can use a Company-provided device or technology on their Company-issued desktop or laptop to make or receive business calls (or otherwise perform their job duties) who nevertheless prefers for personal reasons to use their own personal mobile devices is not eligible for reimbursement for the personal use of the employee's mobile device under this policy, as such use is not deemed necessary.

  - Accordingly, only employees who are required to use a personal mobile device for business will be eligible for expense reimbursement based on their specific approved use during the month. Department head approval is required for an employee to be eligible for expense reimbursement for use of a personal mobile device.
  - Employees who are eligible for a mobile device and usage reimbursement must submit an expense report through the Company approved expense reporting system with receipt within 35 calendar days of the expenditure. The amount is capped by the Company and represents a reasonable portion of the employee's cell phone bill for business-related use, based on the pricing of widely available plans.
  - Reimbursement level and recipient roles will be reviewed at minimum on an annual basis to assess the business use and need levels.
  - Employees who move into new roles will be reviewed to determine if their new role is eligible for reimbursement.
- Employees traveling internationally for business with an employee liable device must ensure the most cost-effective international features available to their plan are activated. Reimbursement for expenses incurred in connection with international business travel is in addition to the monthly reimbursement level noted above.

4. Company Liable

[Planned phase out of individual lines effective December 3, 2021 through 2023]

- Effective December 3, 2021, no new company liable mobile devices (including phones or lines) will be issued to individual employees. Lines no longer subject to early termination fees that are associated exclusively to an individual employee will be transferred as quickly as practicable to an employee's personally liable account or canceled. Exceptions may be approved at the discretion of the Company.
- While the use of company liable devices will continue to decline as lines are transitioned to personal plans, there will continue to be a significant presence of company liable devices for the next several years including both individual devices

still under contract as well as shared devices. It is important that company liable devices continue to be managed in the most cost-effective manner possible.

- Gannett limits carriers to Verizon Wireless (preferred), AT&T, and T-Mobile to leverage pooled data plans and optimize costs. All carrier contracts are managed by Gannett Technology.
- Company liable devices are paid for and owned by the Company. Mobile device purchase requires department head approval. Employees that leave the Company must return Company liable devices to the Company at the time of the termination of employment. Company liable device costs are allocated to the employee's cost center.
- Gannett's company data plans share a pool of data to be most cost efficient. Use of data services is for Company business with personal use of services requiring high data usage (e.g. Netflix, YouTube) prohibited. Personal use of a Company device as a Hotspot is also prohibited. Charges for data overages are allocated back to the employee's cost center.
- Employees are required to pay for smartphone and tablet application subscriptions (apps) that are not necessary in order to perform their job responsibilities. Employees may submit expense reports for reimbursement of applications that are necessary to perform job responsibilities and approved in advance.
- Employees traveling internationally with a Company liable device must complete a HelpDesk ticket in advance to make sure the international travel pass feature is activated. The travel pass costs $10/day and allows the device use of talk, text, and data from the Company's domestic plan. International travel related costs are charged to the employee's cost center.

5. Information Security:

Information security is a critical priority for Gannett. As a business, Gannett must ensure that Company data and networks are secure and free from outside threats or viruses and that Company confidential information and trade secrets remain confidential. Gannett has created the following guidelines for mobile devices to ensure the security of all Company systems.

- All mobile devices that access Company data (ex. email), regardless of whether a reimbursement is provided, are required to meet certain security standards and/or will be managed by Gannett-provided Mobile Device Management (MDM) software.
- Employees must contact the HelpDesk or their IT support contact immediately when a mobile device is lost or stolen to properly disable corporate connectivity services, and if possible, remotely erase Company data.
- Gannett reserves the right to delete Company data from mobile devices, either directly or remotely. No personal data, third party applications or operating system files stored on the device would be deleted in this process.
- Gannett reserves the right to monitor and audit its networks and systems on a periodic basis to ensure compliance with these terms and conditions per the terms of the Acceptable Use and IT Monitoring Policy.

6. Employee Exception Request:

The Company believes that the mobile reimbursement policy contained herein is adequate to ensure that employees are properly reimbursed for all reasonable business expenses that are necessarily incurred by employees in the performance of their job responsibilities. In the event, however, that an employee believes that the amounts identified do not sufficiently reimburse the employee for a particular expense the employee claims was necessarily incurred in the performance of his/her job responsibilities, or the employee incurred an expense not otherwise subject to reimbursement per this policy, the employee may submit a request for an exception or adjustment of that expense (with supporting documentation) by sending an email to expensereports@gannett.com. The Company will review the request, determine if the exception or adjustment is reasonable and necessary, and the employee will be notified of whether the request is approved or denied.

7. Mobile Program Contacts:

If you have questions regarding the mobile policy or accessing Company data with your mobile device, please reach out to your manager or contact the HelpDesk.

New Jersey Gender Equity Policy

Policy Owner: Human Resources
Version: 20231009
Employee Scope: All New Jersey employees

Overview

Right to be Free of Gender Inequity or Bias in Pay, Compensation, Benefits or Other Terms and Conditions of Employment

New Jersey and federal laws prohibit employers from discriminating against an individual with respect to his/her pay, compensation, benefits, or terms, conditions or privileges of employment because of the individual's sex.

Federal Law

Title VII of the Civil Rights Act of 1964 prohibits employment discrimination based on, among other things, an individual's sex. Title VII claims must be filed with the United States Equal Employment Opportunity Commission (EEOC) before they can be brought in court. Remedies under Title VII may include an order restraining unlawful discrimination, back pay, and compensatory and punitive damages.

The Equal Pay Act of 1963 (EPA) prohibits discrimination in compensation based on sex. EPA claims can be filed either with the EEOC or directly with the court. Remedies under the EPA may include the amount of the salary or wages due from the employer, plus an additional equal amount as liquidated damages.

Please be mindful that in order for a disparity in compensation based on sex to be actionable under the EPA, it must be for equal work on jobs the performance of which requires equal skill, effort, and responsibility, and which are performed under similar working conditions.

There are strict time limits for filing charges of employment discrimination. For further information, contact the EEOC at 800-669-4000 or at www.eeoc.gov.

New Jersey Law

The New Jersey Law Against Discrimination (LAD) prohibits employment discrimination based on, among other things, an individual's sex. LAD claims can be filed with the New Jersey Division on Civil Rights (NJDCR) or directly in court. Remedies under the LAD may include an order restraining unlawful discrimination, back pay, and compensatory and punitive damages.

Another State law, N.J.S.A. 34:11-56.1 et seq., prohibits discrimination in the rate or method of payment of wages to an employee because of his or her sex. Claims under this wage discrimination law may be filed with the New Jersey Department of Labor and Workforce Development (NJDLWD) or directly in court. Remedies under this law may

include the full amount of the salary or wages owed, plus an additional equal amount as liquidated damages.

Please be mindful that under the State wage discrimination law a differential in pay between employees based on a reasonable factor or factors other than sex shall not constitute discrimination.

There are strict time limits for filing charges of employment discrimination. For more information regarding LAD claims, contact the NJDCR at 609-292-4605 or at www.njcivilrights.gov. For information concerning N.J.S.A. 34:11-56.1 et seq., contact the Division of Wage and Hour Compliance within the NJDLWD at 609-292-2305 or at http://lwd.state.nj.us.

For Spanish translation of this guidance, visit:
https://www.nj.gov/labor/wageandhour/assets/PDFs/Employer%20Poster%20Packet/genderequityposterspanish.pdf

Non-Disclosure Agreement (US)

Policy Owner: Human Resources
Version: 20230911
Employee Scope: All new US employees except sales leaders

Confidential Information and Invention Assignment Agreement

As a condition of my employment with Gannett Co., Inc., its subsidiaries, affiliates, successors or assigns (together the "Company"), and in consideration of the mutual promises of the parties provided for herein, I agree with the Company to the following terms and conditions of this Confidential Information and Invention Assignment Agreement (the "Agreement").

1. Obligations to Prior Employers and Other Parties. I have fully disclosed to the Company any and all restrictions relating to my ability to work for the Company, including any obligations arising from any employment agreements with my former employers, and I agree to abide by any and all such valid restrictions. I also agree that I will not, during my employment with the Company, improperly use or disclose any proprietary information or trade secrets of any former or concurrent employer or other person or entity to which I may owe a duty of confidence and that I will not bring onto the premises of the Company or otherwise use during the duration of my employment with the Company any proprietary information or trade secret belonging to any such employer, person or entity unless consented to in writing by such employer, person or entity.

2. Confidential Information.
   (a) Company Information.
      (i) The Company agrees that during the course of my employment, it will provide me one or more of the following, some of which I agree that I have not received before signing this Agreement: certain Confidential Information related to my position and duties; opportunity to contact and deal with customers and prospective customers and/or to develop goodwill on behalf of the Company; and/or, specialized training related to the Company's business. In exchange, I agree at all times during the term of my employment and thereafter, to hold in strictest confidence, and not to use, except for the exclusive benefit of the Company, and not to disclose to any person, firm or corporation without authorization of the Company, any Confidential Information of the Company. I agree that upon the termination of my employment, regardless of the reason for termination, the Company shall have no obligation to provide or otherwise make available to me any of its Confidential Information.
      (ii) "Confidential Information" means any Company proprietary information, technical data, trade secrets, know-how, customer and potential customer lists and information. I further understand that Confidential Information does not include any of the foregoing items which has become publicly known and made generally available through no wrongful act or omission of mine or of others who

were under confidentiality obligations as to the item or items involved or improvements or new versions thereof.

(b) Third Party Information. I recognize that the Company has received and, in the future, will receive from third parties their confidential or proprietary information subject to a duty on the Company's part to maintain the confidentiality of such information and to use it only for certain limited purposes. I agree to hold all such confidential or proprietary information in the strictest confidence and not to disclose it to any person, firm or corporation or to use it except as necessary in carrying out my work for the Company consistent with the Company's agreement with such third party. If requested, I will sign such other agreements as may be required by a third party to confirm the foregoing.

3. Returning Company Property. I agree that, at the time of leaving the employ of the Company, I will deliver to the Company (and will not keep in my possession, recreate or deliver to anyone else) any and all devices, records, data, notes, reports, proposals, lists, correspondence, specifications, drawings blueprints, sketches, materials, equipment, other documents or property, or reproductions of any aforementioned items developed by me pursuant to my employment with the Company or otherwise belonging to the Company, its successors or assigns, including, but not limited to, those records maintained pursuant to Section 2.

4. Notification of New Employer. In the event that I leave the employ of the Company, I shall notify my new employer of the existence of this Agreement and my obligations set forth herein. I also hereby grant consent to notification by the Company to my new employer about this Agreement and my obligations set forth herein.

5. Restrictive Covenants.

(a) Solicitation of Employees. I agree that during my employment with the Company and for a period of six (6) months immediately following the termination of my employment with the Company, regardless of whether the termination is initiated by me or by the Company, and regardless of whether there is cause for or notice of my termination, I will not, either directly or indirectly, solicit, induce, recruit or encourage any of the Company's employees or independent contractors with whom I worked during my employment to terminate their relationship with the Company.

(b) Solicitation of Customers. I agree that during my employment with the Company and for a period of six (6) months immediately following the termination of my employment with the Company, regardless of whether the termination is initiated by me or by the Company, and regardless of whether there is cause for or notice of my termination, I will not, either directly or indirectly, solicit, induce, or encourage any of the Company's customers with whom I had business contact or about whom I learned confidential information during my employment to terminate or otherwise modify, to the detriment of the Company, its relationship with the Company.`

(c) Special Terms Relating to Post-Employment Restrictive Covenants.

(i) Reasonableness Stipulation. I acknowledge that I will derive significant value from the Company's agreement in Section 2(a)(i) to provide me with that Confidential Information of the Company, customer contact and goodwill

development opportunities, and/or specialized training. I further acknowledge that my fulfillment of my confidentiality obligations contained in this Agreement standing alone would be insufficient to protect the Company's legitimate business interests. Accordingly, I agree that the post-employment restrictions placed upon me in this Agreement (including my obligation not to solicit certain customers and employees, collectively the "Post-Employment Restrictive Covenants") are reasonable and necessary to protect the Company's legitimate business interests. I further acknowledge that the time, geography, and scope limitations of my obligations under the Post-Employment Restrictive Covenants are reasonable, that I will not be precluded from gainful employment if I comply with these obligations, and that I will not challenge the reasonableness or enforceability of the Post-Employment Restrictive Covenants. I acknowledge that if I violate the Post-Employment Restrictive Covenants, the duration of such obligations shall be extended by the duration of my violation of such Post-Employment Restrictive Covenants.

(ii) State Specific Exceptions.

[Georgia: For employees who reside in Georgia, and in the event that the choice of law provision contained in Section 8(a) does not control: (i) the post-employment restrictions in Section 2 shall only apply to Confidential Information that does not qualify as a trade secret for a period of three years following the termination of my employment but shall continue to apply to trade secret information for as long as the information qualifies as a trade secret, and (ii) the post-employment restrictions in Section 5(b) shall be modified to read as follows: "I agree that for a period of six (6) months following the end of my employment with Company, I will not, in any way, directly or indirectly, solicit, divert, or take away, or attempt to solicit, divert or take away, the customers of the Company which were served by me during the term of my employment with the Company for the purpose of selling to such customer any service or product which is provided by the Company at the time of execution of this Agreement; unless a duly authorized Company officer gives me written authorization to do so at the time."

Louisiana: For employees who reside in Louisiana: the enforcement of the post-employment restrictions in Section 5(b) will be limited within the state of Louisiana to the following Parishes where I have or will help the Company do business: Orleans, Caddo, Jefferson, Lafayette.]

6. Inventions.

(a) Assignment of Inventions. I agree that I will promptly make full written disclosure to the Company, will hold in trust for the sole right and benefit of the Company, and hereby assign to the Company, or its designee, all my right, title, and interest in and to any and all inventions, original works of authorship, developments, concepts, improvements, designs, discoveries, ideas, trademarks or trade secrets, whether or not patentable or registrable under copyright or similar laws, which I may solely or jointly conceive or develop or reduce to practice, or cause to be conceived or developed or reduced to practice, during the period of time I am in the employ of the Company (collectively referred to as "Inventions"). I further acknowledge that

all original works of authorship which are made by me (solely or jointly with others) within the scope of and during the period of my employment with the Company and which are protectible by copyright are "works made for hire," as that term is defined in the United States Copyright Act. I understand and agree that the decision whether or not to commercialize or market any Invention developed by me solely or jointly with others is within the Company's sole discretion and for the Company's sole benefit and that no royalty will be due to me as a result of the Company's efforts to commercialize or market any such Invention.

(b) Maintenance of Records. I agree to keep and maintain adequate and current written records of all Inventions made by me (solely or jointly with others) during the term of my employment with the Company. The records will be in the form of notes, sketches, drawings, and any other format that may be specified by the Company. The records will be available to and remain the sole property of the Company at all times.

(c) Patent and Copyright Registrations. I agree to assist the Company, or its designee, at the Company's expense, in every proper way to secure the Company's rights in the Inventions and any copyrights, patents, mask work rights or other intellectual property rights relating thereto in any and all countries, including, but not limited to, the disclosure to the Company of all pertinent information and data with respect thereto, the execution of all applications, specifications, oaths, assignments and all other instruments which the Company shall deem necessary in order to apply for and obtain such rights and in order to assign and convey to the Company, its successors, assigns, and nominees the sole and exclusive rights, title and interest in and to such Inventions, and any copyrights, patents, mask work rights or other intellectual property rights relating thereto. I further agree that my obligation to execute or cause to be executed, when it is in my power to do so, any such instrument or papers shall continue after the termination of this Agreement. If the Company is unable because of my mental or physical incapacity or for any other reason to secure my signature to apply for or to pursue any application for any United States or foreign patents or copyright registrations covering Inventions or original works of authorship assigned to the Company as above, then I hereby irrevocably designate and appoint the Company and its duly authorized officers and agents as my agent and attorney in fact, to act for and in my behalf and stead to execute and file any such applications and to do all other lawfully permitted acts to further the prosecution and issuance of letters patent or copyright registrations thereon with the same legal force and effect as if executed by me.

(d) Moral Rights. Any assignment of copyright hereunder (and any ownership of a copyright as a work made for hire) includes all rights of paternity, integrity, disclosure and withdrawal and any other rights that may be known as or referred to as "moral rights" (collectively, "Moral Rights"). To the extent such Moral Rights cannot be assigned under applicable law and to the extent the following is allowed by the laws in the various countries where Moral Rights exist, I hereby ratify and consent to any action of the Company that would violate such Moral Rights in the absence of such ratification/consent. I will confirm any such ratifications and consents from time to time as requested by the Company.

(e) Exclusions. Section 6 shall not apply to any invention that I developed entirely on my own time without using the Company's equipment, supplies, facilities, or trade secret information except for those inventions that either:
(1) Relate at the time of conception or reduction to practice of the invention to the Company's business, or actual or demonstrably anticipated research or development of the employer, or
(2) Result from any work performed by me for the Company.

7. Representations. I agree to execute any proper oath or verify any proper document required to carry out the terms of this Agreement. I represent that my performance of all the terms of this Agreement will not breach any agreement to keep in confidence proprietary information acquired by me in confidence or in trust prior to my employment by the Company. I have not entered into, and I agree I will not enter into, any oral or written agreement in conflict herewith.

8. General Provisions.
(a) Governing Law. This Agreement will be governed by the laws of the State of Delaware without regard for any choice of law principles of said state to the contrary. In the event that the law of the State of Delaware cannot be applied, then the law of the state where I last regularly performed services for the Company shall apply and control.
(b) Entire Agreement. This Agreement sets forth the entire agreement and understanding between the Company and me relating to the subject matters contained herein and supersedes all prior discussions between us. No modification of or amendment to this Agreement, nor any waiver of any rights under this Agreement, will be effective unless in writing signed by the party to be charged. Any subsequent change or changes in my duties, salary or compensation will not affect the validity or scope of this Agreement.
(c) Severability. If, in any judicial or arbitral proceeding, a court or arbitrator refuses to enforce any provision of this Agreement (or any part thereof), then such unenforceable provision (or such part) shall be eliminated from this Agreement to the extent necessary to permit the remaining separate provisions (or portions thereof) to be enforced. In the event any of the provisions of this Agreement are deemed to exceed the time, geographic or scope limitations permitted by applicable law, then such provisions shall be reformed to the maximum time, geographic or scope limitations, as the case may be, then permitted by such law, with such modification to be limited in its application to the geographic jurisdiction of the court or arbitrator that so reforms the Agreement. The remaining provisions of this Agreement will continue in full force and effect notwithstanding the invalidity of any provision of this Agreement.
(d) Successors and Assigns. This Agreement will be binding upon my heirs, executors, administrators and other legal representatives and will be for the benefit of the Company, its successors, and its assigns without need of further action by any party. Assignment of this Agreement by the Company is expressly authorized by me. Any subsidiary, affiliate, successor or assign that subsequently employs Employee shall be treated as the Company for purposes of this Agreement.

9. Acknowledgement. I acknowledge and agree to each of the following items:
   (a) I am executing this Agreement voluntarily and without any duress or undue influence by the Company or anyone else; and
   (b) I have carefully read this Agreement. I have asked any questions needed for me to understand the terms, consequences and binding effect of this Agreement and fully understand them; and
   (c) I sought the advice of an attorney of my choice if I wanted to before signing this Agreement.

"I confirm I have reviewed and understand the guidelines."

Non-Disclosure Agreement with Non-Compete (US)

Policy Owner: Human Resources
Version: 20230911
Employee Scope: All new US sales leaders

Confidential Information and Invention Assignment Agreement

As a condition of my employment with Gannett Co., Inc., its subsidiaries, affiliates, successors or assigns (together the "Company"), and in consideration of the mutual promises of the parties provided for herein, I agree with the Company to the following terms and conditions of this Confidential Information and Invention Assignment Agreement (the "Agreement").

1. Obligations to Prior Employers and Other Parties. I have fully disclosed to the Company any and all restrictions relating to my ability to work for the Company, including any obligations arising from any employment agreements with my former employers, and I agree to abide by any and all such valid restrictions. I also agree that I will not, during my employment with the Company, improperly use or disclose any proprietary information or trade secrets of any former or concurrent employer or other person or entity to which I may owe a duty of confidence and that I will not bring onto the premises of the Company or otherwise use during the duration of my employment with the Company any proprietary information or trade secret belonging to any such employer, person or entity unless consented to in writing by such employer, person or entity.

2. Confidential Information.
   (a) Company Information.
      (i) The Company agrees that during the course of my employment, it will provide me one or more of the following, some of which I agree that I have not received before signing this Agreement: certain Confidential Information related to my position and duties; opportunity to contact and deal with customers and prospective customers and/or to develop goodwill on behalf of the Company; and/or, specialized training related to the Company's business. In exchange, I agree at all times during the term of my employment and thereafter, to hold in strictest confidence, and not to use, except for the exclusive benefit of the Company, and not to disclose to any person, firm or corporation without authorization of the Company, any Confidential Information of the Company. I agree that upon the termination of my employment, regardless of the reason for termination, the Company shall have no obligation to provide or otherwise make available to me any of its Confidential Information.

      (ii) "Confidential Information" means any Company proprietary information, technical data, trade secrets, know-how, customer and potential customer lists and information. I further understand that Confidential Information does not include any of the foregoing items which has become publicly known and made generally available through no wrongful act or omission of mine or of others who

were under confidentiality obligations as to the item or items involved or improvements or new versions thereof.

(b) Third Party Information. I recognize that the Company has received and, in the future, will receive from third parties their confidential or proprietary information subject to a duty on the Company's part to maintain the confidentiality of such information and to use it only for certain limited purposes. I agree to hold all such confidential or proprietary information in the strictest confidence and not to disclose it to any person, firm or corporation or to use it except as necessary in carrying out my work for the Company consistent with the Company's agreement with such third party. If requested, I will sign such other agreements as may be required by a third party to confirm the foregoing.

3. Returning Company Property. I agree that, at the time of leaving the employ of the Company, I will deliver to the Company (and will not keep in my possession, recreate or deliver to anyone else) any and all devices, records, data, notes, reports, proposals, lists, correspondence, specifications, drawings blueprints, sketches, materials, equipment, other documents or property, or reproductions of any aforementioned items developed by me pursuant to my employment with the Company or otherwise belonging to the Company, its successors or assigns, including, but not limited to, those records maintained pursuant to Section 2.

4. Notification of New Employer. If I leave the employ of the Company, I shall notify my new employer of the existence of this Agreement and my obligations set forth herein. I also hereby grant consent to notification by the Company to my new employer about this Agreement and my obligations set forth herein.

5. Restrictive Covenants.
   (a) Solicitation of Employees. I agree that during my employment with the Company and for a period of six (6) months immediately following the termination of my employment with the Company, regardless of whether the termination is initiated by me or by the Company, and regardless of whether there is cause for or notice of my termination, I will not, either directly or indirectly, solicit, induce, recruit or encourage any of the Company's employees or independent contractors with whom I worked during my employment to terminate their relationship with the Company.

   (b) Solicitation of Customers. I agree that during my employment with the Company and for a period of six (6) months immediately following the termination of my employment with the Company, regardless of whether the termination is initiated by me or by the Company, and regardless of whether there is cause for or notice of my termination, I will not, either directly or indirectly, solicit, induce, or encourage any of the Company's customers with whom I had business contact or about whom I learned confidential information during my employment to terminate or otherwise modify, to the detriment of the Company, its relationship with the Company.

(c) Covenant Not to Compete. I agree that during my employment with the Company and for a period of six (6) months immediately following the termination of my employment with the Company (the "Restricted Period"), I will not, without the prior written consent of the Company, work in the same or similar capacity to my role at the Company or in a management role for any person or entity (including myself) engaged in business substantially similar to the business engaged in by the Company during my employment within the Restricted Area. This covenant not to compete will not apply in the event of a position elimination. The Restricted Area shall refer to the following: (a) 50 miles of any Company office within which I was employed during the 12 months preceding my termination of employment or (b) if a manager or above, within 50 miles of any Company office for which I had responsibility during the 12 months preceding my termination of employment.

(d) Special Terms Relating to Post-Employment Restrictive Covenants.

(i) Reasonableness Stipulation. I acknowledge that I will derive significant value from the Company's agreement in Section 2(a)(i) to provide me with that Confidential Information of the Company, customer contact and goodwill development opportunities, and/or specialized training. I further acknowledge that my fulfillment of my confidentiality obligations contained in this Agreement standing alone would be insufficient to protect the Company's legitimate business interests. Accordingly, I agree that the post-employment restrictions placed upon me in this Agreement (including my obligation not to solicit certain customers and employees, and my obligation not to compete, collectively the "Post-Employment Restrictive Covenants") are reasonable and necessary to protect the Company's legitimate business interests. I further acknowledge that the time, geography, and scope limitations of my obligations under the Post-Employment Restrictive Covenants are reasonable, that I will not be precluded from gainful employment if I comply with these obligations, and that I will not challenge the reasonableness or enforceability of the Post-Employment Restrictive Covenants. I acknowledge that if I violate the Post-Employment Restrictive Covenants, the duration of such obligations shall be extended by the duration of my violation of such Post-Employment Restrictive Covenants.

(ii) State Specific Exceptions.

[Arizona: For employees who reside in Arizona, and in the event that the choice of law provision contained in Section 8(a) does not control: the restrictions in Section 5(c) shall be limited to apply only in the Restricted Area.

California: For employees who reside in California, the provisions contained in Section 5(c) shall not apply.

Georgia: For employees who reside in Georgia, and in the event that the choice of law provision contained in Section 8(a) does not control: (i) the post-employment restrictions in Section 2 shall only apply to Confidential Information that does not qualify as a trade secret for a period of three years following the termination of my employment but shall continue to apply to trade secret information for as long as the information qualifies as a trade secret, (ii) the post-employment restrictions in Section 5(c) will not apply, and (iii) the post-employment restrictions in Section 5(b) shall be modified to read as follows: "I

agree that for a period of six (6) months following the end of my employment with Company, I will not, in any way, directly or indirectly, solicit, divert, or take away, or attempt to solicit, divert or take away, the customers of the Company which were served by me during the term of my employment with the Company for the purpose of selling to such customer any service or product which is provided by the Company at the time of execution of this Agreement; unless a duly authorized Company officer gives me written authorization to do so at the time."

Louisiana: For employees who reside in Louisiana: the enforcement of the post-employment restrictions in Sections 5(b) and 5(c) will be limited within the state of Louisiana to the following Parishes where I have or will help the Company do business: Orleans, Caddo, Jefferson, Lafayette.

Massachusetts: For employees who reside in Massachusetts, the provisions contained in Section 5(c) shall not apply.]

6. Inventions.
   (a) Assignment of Inventions. I agree that I will promptly make full written disclosure to the Company, will hold in trust for the sole right and benefit of the Company, and hereby assign to the Company, or its designee, all my right, title, and interest in and to any and all inventions, original works of authorship, developments, concepts, improvements, designs, discoveries, ideas, trademarks or trade secrets, whether or not patentable or registrable under copyright or similar laws, which I may solely or jointly conceive or develop or reduce to practice, or cause to be conceived or developed or reduced to practice, during the period of time I am in the employ of the Company (collectively referred to as "Inventions"). I further acknowledge that all original works of authorship which are made by me (solely or jointly with others) within the scope of and during the period of my employment with the Company and which are protectible by copyright are "works made for hire," as that term is defined in the United States Copyright Act. I understand and agree that the decision whether or not to commercialize or market any Invention developed by me solely or jointly with others is within the Company's sole discretion and for the Company's sole benefit and that no royalty will be due to me as a result of the Company's efforts to commercialize or market any such Invention.
   (b) Maintenance of Records. I agree to keep and maintain adequate and current written records of all Inventions made by me (solely or jointly with others) during the term of my employment with the Company. The records will be in the form of notes, sketches, drawings, and any other format that may be specified by the Company. The records will be available to and remain the sole property of the Company at all times.
   (c) Patent and Copyright Registrations. I agree to assist the Company, or its designee, at the Company's expense, in every proper way to secure the Company's rights in the Inventions and any copyrights, patents, mask work rights or other intellectual property rights relating thereto in any and all countries, including, but not limited to, the disclosure to the Company of all pertinent information and data with respect thereto, the execution of all applications, specifications, oaths, assignments and all other instruments which the Company shall deem necessary in order to apply for

and obtain such rights and in order to assign and convey to the Company, its successors, assigns, and nominees the sole and exclusive rights, title and interest in and to such Inventions, and any copyrights, patents, mask work rights or other intellectual property rights relating thereto. I further agree that my obligation to execute or cause to be executed, when it is in my power to do so, any such instrument or papers shall continue after the termination of this Agreement. If the Company is unable because of my mental or physical incapacity or for any other reason to secure my signature to apply for or to pursue any application for any United States or foreign patents or copyright registrations covering Inventions or original works of authorship assigned to the Company as above, then I hereby irrevocably designate and appoint the Company and its duly authorized officers and agents as my agent and attorney in fact, to act for and in my behalf and stead to execute and file any such applications and to do all other lawfully permitted acts to further the prosecution and issuance of letters patent or copyright registrations thereon with the same legal force and effect as if executed by me.

(d) Moral Rights. Any assignment of copyright hereunder (and any ownership of a copyright as a work made for hire) includes all rights of paternity, integrity, disclosure and withdrawal and any other rights that may be known as or referred to as "moral rights" (collectively, "Moral Rights"). To the extent such Moral Rights cannot be assigned under applicable law and to the extent the following is allowed by the laws in the various countries where Moral Rights exist, I hereby ratify and consent to any action of the Company that would violate such Moral Rights in the absence of such ratification/consent. I will confirm any such ratifications and consents from time to time as requested by the Company.

(e) Exclusions. Section 6 shall not apply to any invention that I developed entirely on my own time without using the Company's equipment, supplies, facilities, or trade secret information except for those inventions that either:

(1) Relate at the time of conception or reduction to practice of the invention to the Company's business, or actual or demonstrably anticipated research or development of the employer, or

(2) Result from any work performed by me for the Company.

7. Representations. I agree to execute any proper oath or verify any proper document required to carry out the terms of this Agreement. I represent that my performance of all the terms of this Agreement will not breach any agreement to keep in confidence proprietary information acquired by me in confidence or in trust prior to my employment by the Company. I have not entered into, and I agree I will not enter into, any oral or written agreement in conflict herewith.

8. General Provisions.

(a) Governing Law. This Agreement will be governed by the laws of the State of Delaware without regard for any choice of law principles of said state to the contrary. In the event that the law of the State of Delaware cannot be applied, then the law of the state where I last regularly performed services for the Company shall apply and control.

(b) Entire Agreement. This Agreement sets forth the entire agreement and understanding between the Company and me relating to the subject matters contained herein and supersedes all prior discussions between us. No modification of or amendment to this Agreement, nor any waiver of any rights under this Agreement, will be effective unless in writing signed by the party to be charged. Any subsequent change or changes in my duties, salary or compensation will not affect the validity or scope of this Agreement.

(c) Severability. If, in any judicial or arbitral proceeding, a court or arbitrator refuses to enforce any provision of this Agreement (or any part thereof), then such unenforceable provision (or such part) shall be eliminated from this Agreement to the extent necessary to permit the remaining separate provisions (or portions thereof) to be enforced. In the event any of the provisions of this Agreement are deemed to exceed the time, geographic or scope limitations permitted by applicable law, then such provisions shall be reformed to the maximum time, geographic or scope limitations, as the case may be, then permitted by such law, with such modification to be limited in its application to the geographic jurisdiction of the court or arbitrator that so reforms the Agreement. The remaining provisions of this Agreement will continue in full force and effect notwithstanding the invalidity of any provision of this Agreement.

(d) Successors and Assigns. This Agreement will be binding upon my heirs, executors, administrators and other legal representatives and will be for the benefit of the Company, its successors, and its assigns without need of further action by any party. Assignment of this Agreement by the Company is expressly authorized by me. Any subsidiary, affiliate, successor or assign that subsequently employs Employee shall be treated as the Company for purposes of this Agreement.

9. Acknowledgement. I acknowledge and agree to each of the following items:

(a) I am executing this Agreement voluntarily and without any duress or undue influence by the Company or anyone else; and

(b) I have carefully read this Agreement. I have asked any questions needed for me to understand the terms, consequences and binding effect of this Agreement and fully understand them; and

(c) I sought the advice of an attorney of my choice if I wanted to before signing this Agreement.

“I confirm I have reviewed and understand the guidelines.”

Password Security Policy

Policy Owner: IT Security and Data Privacy
Version: 20250101
Employee Scope: All US employees who work with all passwords on any system that resides at any Gannett facility, has access to the Gannett network, or stores any Gannett information. Password Policy does not apply to external customers

Purpose

The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords, and the frequency of change.

Definitions and Acronyms

When navigating this policy, it's important to grasp the terminology. Our Glossary of Cybersecurity Terms provides concise definitions for key concepts.

Scope

Passwords are used for various purposes at Gannett. Some of the more common uses include user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Other authentications may be used to access accounts such as Biometrics; these types are not covered in this policy.

All employees, Gannett by accessing Gannett IT (Information Technology) Systems must be aware of how to select strong passwords and must follow this policy. Individual contractors and third parties providing services to Gannett by accessing Gannett IT Systems must be made aware of Gannett's password requirements. Gannett's systems are configured to require certain minimum password controls. This policy does not apply to vendor staff accessing vendor systems; however, Gannett review of vendor data security and privacy policies and practices should include review of access controls including password security.

Policy

All individuals with accounts on Gannett IT Systems are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Password Controls

- Passwords are considered proprietary and confidential Gannett information.
- Passwords are case sensitive.
- The maximum password age is defined in the chart below.
- Password length, complexity, and expiration rules are enforced based upon the risk level of the Account Type (Account Types are defined in the Account and Access Management Policy):

Account Type	Password Complexity Requirements	Maximum Password Age (Password Expiration)
User Account (employee)	8 – Character Alphanumeric	90 days
Elevated Privilege Account	14 – Character Alphanumeric with symbols	90 days
External Account	8 – Character Alphanumeric 14 – Character Alphanumeric with symbols (if elevated privilege)	90 days
Shared Account	8 – Character Alphanumeric	90 days
Mailbox Account	8 – Character Alphanumeric	90 days
Visitor Account	8 – Character Alphanumeric	90 days
Service Account	30 – Character Alphanumeric with symbols	365 days
Built-in Account	14 – Character Alphanumeric with symbols	90 days
Top Level Account	14 – Character Alphanumeric with symbols	90 days

- The password must be changed when the user is no longer in sole possession of that password.
- The previous 10 passwords must not be reused when changing passwords.
- When available, Gannett IT Systems providers will use automated methods for enforcing password history.
- When available, Gannett IT Systems must be configured to disable/lockout an account after 6 unsuccessful password attempts within a 30-minute period. The account can be re-enabled/unlocked 30 minutes after the last unsuccessful password attempt.
- The user must change any temporary and default passwords after initial login.
- Encryption must be used for the administration, presentation, storage, and transmission of all security credentials. See Acceptable Encryption Policy for appropriate method of encryption.
- Passwords must not be embedded within login scripts, macros, or executable programs.
- IT Systems must provide the capability for users to change their own password.
- Users must validate the current password when changing the password.
- When available, Gannett IT Systems shall be configured to require users to re-authenticate after a designated period to gain access to the IT System(s) after a period of inactivity, based upon the risk level of the IT System.

Top Level Account Password Management

- Top-level accounts are defined as a highly privileged account typically required for initial system configuration and/or disaster recovery purposes and is not used on a daily basis.
  - Any system that is identified for disaster recovery must have its top-level account password(s) stored in a secure location using encryption (e.g.: software / physical vault, etc.).
  - Top level accounts must leverage multi-factor authentication when possible.
  - Logging of access and usage of top-level accounts is required.

Private Key Security

- User Account Authentication Private Key Security (typically Secure Shell Administrator access)
  - User account private keys must be secured with at least a 10- character alpha-numeric passphrase.
- Service Account Authentication Private Key Security
  - Service account private keys are not required to have passphrases.
  - The holder of private keys must securely store the keys using encryption and provide access only to authorized users. See Acceptable Encryption Policy for appropriate method of encryption.

Multi-Factor Authentication

- Access control features enable validation of a user's Identity when attempting to access a Gannett Systems using one or more authentication factors based on the risk level of the Gannett Systems in a secure fashion and prevent unauthorized access to the Resource. User authentication factors are classified as:
  - Something the user has.
  - Something the user knows.
  - Something the user is.
- Multi-factor authentication must be used for all non-console administrative access.
- Multi-factor authentication must be used for remote network access.
- Multi-factor authentication must be used for all publicly accessible applications or services, examples include Software as a Service (SaaS) or any other online “as a Service” service, Third Party vendors and internally developed services.

Password Protection

- Passwords are not displayed on screen when being entered unless selected by the user. Passwords are masked, suppressed, or otherwise obscured so that unauthorized individuals cannot observe or recover them.
- Users of individual User Accounts must not share their passwords with third parties (including managers, supervisors, administrative assistants, and IT support), either internally within Gannett or externally. IT Support will either ask the user to enter their password directly or trigger a password reset for support issues requiring password access to a User Account.
- User account passwords may be documented when stored in a secure location using encryption (e.g.: software / physical vault, etc.) and only accessible to authorized users only.

Enforcement and Exception

- Compliance with this policy is required under Gannett's Information Security Policies and Standards Enforcement Policy and Gannett may take actions in response to non-compliance as provided under the Enforcement Policy.
- Any exceptions to this policy must follow Gannett’s Information Security Policies and Standards Exceptions Policy.

This policy may be updated occasionally by the Company. The current version of this policy, as well as policies referenced in this document, may be viewed on MyLife@Gannett.

Pre-Print Policy for GPS Employees

Policy Owner: Human Resources
Version: 20230911
Employee Scope: All new GPS employees

Purpose

Publication content, preprints, advertising materials and commercial print products processed by Gannett Publishing Services (GPS) affiliated operations are proprietary and must remain confidential. Advertising and commercial print customers expect reasonable security and require confidentiality.

Policy

Employee compliance with the Gannett Publishing Services Product Security & Confidentiality Policy is mandatory:

- Publications and preprints must not be removed from designated production or distribution center areas without GPS management or supervisor approval.
- It is unlawful to take unauthorized photos/images of printed advertising materials. Use of cameras (including cell phones) to photograph preprints, products or publication content is strictly prohibited.
- Unauthorized disposal or distribution of surplus preprints or products is strictly prohibited.
- Employees must be aware of the potential to inadvertently share confidential information.

Enforcement

Unauthorized use or disclosure of confidential information or materials prior to the scheduled release date may result in disciplinary action up to and including termination of employment.

Principles of Ethical Conduct for Newsrooms

Policy Owner: Legal
Version: 20250101
Employee Scope: All USA TODAY journalists

Principles of Ethical Conduct for Newsrooms

This document outlines the ethical principles guiding journalists at USA TODAY Network across various platforms.

I. Seeking and Reporting the Truth in a Truthful Way

Summary: This section emphasizes honesty, accuracy, and thoroughness in news gathering and reporting.

- Be honest in gathering, reporting, and presenting news - with relevancy, persistence, context, thoroughness, balance, and fairness in mind.
- Seek to gain understanding of the communities, individuals, and issues we cover to provide an informed account of activities
- Hold editorials and opinion pieces to the same accuracy standards as news stories.
- Treat information from unofficial sources with skepticism and seek corroboration.
- Evaluate the credibility of external news content.

II. Serving the Public Interest

Summary: This section focuses on upholding democratic principles, being vigilant watchdogs, and promoting understanding and civil discourse.

- Uphold First Amendment principles.
- Act as vigilant watchdogs of government and institutions.
- Seek solutions and expose problems to effect positive change.
- Provide public forums for diverse views.
- Reflect and encourage understanding of diverse community segments.
- Promote understanding of complex issues.
- Encourage views that foster understanding and civil discourse.
- Provide free access to news during public safety emergencies when appropriate.

III. Exercising Fair Play

Summary: This section highlights the importance of respect, compassion, and transparency in journalism.

- Treat people with respect and compassion.
- Correct errors promptly.
- Include all relevant sides of a story. When news develops, and we can't include important perspectives immediately, share updates, including additional sources, when possible. Share attempts to reach sources who add value to the story.
- Explain journalistic processes to promote transparency.
- Pay attention to fairness, especially with those unaccustomed to the media.
- Use confidential sources only as a last resort and under specific procedures that best serve the public's right to know.

IV. Maintaining Independence

Summary: This section stresses the importance of remaining free from outside influences and conflicts of interest.

- Avoid outside interests, investments or business relationships that may compromise credibility.
- Ensure neutral relationships with individuals and organizations seeking to influence the news.
- Do not support political campaigns or causes publicly through the display of bumper stickers, signs, pins, public/private donations, participation in demonstrations, petitions or in social media posts.
- Individual viewpoints that might cause readers to question our impartiality in news coverage should remain private. This principle does not apply to those who are paid to write and share opinion.
- Avoid conflicts of interest and improper obligations to news sources, newsmakers and advertisers.
- Clearly distinguish between advertising and editorial content - provide appropriate disclosures, exercise transparency and avoid actual or implicit commercial endorsements by our journalists.
- Ensure sponsorships do not influence content.

V. Acting with Integrity

Summary: This section underscores the need for ethical behavior, legal compliance, and responsibility in journalism.

- Act honorably and ethically with news sources, the public, and colleagues.
- Obey the law and observe standards of decency.
- Take responsibility for decisions and consider their consequences.
- Use technological tools with skill and thoughtfulness, avoiding approaches that skew facts, distort reality, or sensationalize events.
- Do not plagiarize or fabricate information.
- Do not alter photos, video or audio to misrepresent events or mislead audiences.

Protecting the Principles

No statement of principles and procedures can envision every circumstance that may be faced while covering the news. As in the United States Constitution, fundamental principles sometimes conflict. Thus, these recommended practices cannot establish standards of performance for journalists in every situation.

Rather, they are intended as a resource to help our journalists make better decisions in accordance with our aspirational principles. These principles are not intended to be a statement of our legal obligations, nor could they be enforceable under the First Amendment.

Careful judgment and common sense should be applied to make the decisions that best serve the public interest and result in the greatest good. In such instances, journalists should not act unilaterally. The best decisions are obtained after open- minded consultations with appropriate colleagues and superiors – augmented, when necessary, by the advice of dispassionate outside parties, such as experts, lawyers, ethicists, or others whose views in confidence may provide clarity in sorting out issues.

Ensuring the Truth Principle

Summary: This section details practices for maintaining truthfulness in reporting.

- Do not lie or misstate identities or intentions.
- Accurately attribute work and thoughts of others.
- Correct or clarify information in a transparent and prompt manner.

Using Confidential Sources

Summary: This section outlines the cautious use of confidential sources in reporting.

- Use confidential sources sparingly and only when necessary.
- Corroborate information from confidential sources.
- Inform sources that their identity will be disclosed to a senior newsroom leader.
- Ensure confidentiality agreements are clear and honored.
- Use only people who are in a direct position to know.
- Attempt to corroborate information from a confidential source through another source or sources with independent knowledge of the information and/or with documents.
- Inform sources that his/her name will be disclosed to at least one senior newsroom leader.

  When content involving confidential sourcing is planned for Network coverage, the Network chief content officer/editor-in-chief and Network editor handling the story should be notified of sourcing approval.
- Hold managers who approve sourcing and the journalist working directly with the source accountable when unnamed sources are used. When a significant story to be published relies on a source who will not be named, it is the responsibility of the approving manager to confirm the identity of the source and to review the information provided. This may require arranging for the manager to meet the source. The same principles apply to the use of confidential documents. It is not enough to know and sign off on the identity of the source of the documents. The approver must be satisfied that the documents are authentic and trustworthy and that chain of custody of the documents can be traced to their originators.
- Share the source's name verbally with the approving manager. Avoid email exchanges.
- Make clear that agreements of confidentiality are between the news organization and the sources, not just between the reporter and the sources. The news organization will honor its agreements with sources. Reporters should make every effort to clear such confidentiality agreements with a senior-level manager first. Promises of confidentiality made by reporters to sources will not be overridden by the news executive; however, newsroom managers may choose not to use the material obtained in this fashion.
- Confidential treatment should be reserved for sharing facts. Weigh the value of and motive behind information before deciding to use it with an eye on fairness and accuracy. Anonymous criticism, praise and speculation should be avoided.
- In most cases, paraphrase information provided to us confidentially—unless a direct or partial quote more accurately describes that information for the reader.
- Paraphrasing is preferred because blind quotes can unfairly infuse feelings, opinions and biased interpretations. This is a judgment call that should be weighed by the manager approving sourcing.

- The number and standing of confidential sources should not be exaggerated.
- Journalists and their sources should have clear understanding of the nature of the confidentiality that is appropriate for the story. There may be multiple options and, where possible, they should be discussed with a manager before a promise of confidentiality is extended. Among the options:
  - The news organization will not name the source in the story.
  - The organization will not name the source unless compelled to do so by a court.
  - Other options, such as cases where a promise never to name a source is being considered, should be discussed with the Network's chief content officer/editor-in-chief.
- All sources should be informed that the news organization will not honor confidentiality if the sources have lied or misled the news organization.
- Make sure both sides understand the stipulations of the agreement. For example:
  - Statements may be quoted directly or indirectly and will be attributed to the source. This is sometimes referred to as "on the record."
  - The information may be used in the story but not attributed to the source. This is sometimes referred to as "not for attribution" or "for background."
  - The information will not be used in the story unless obtained elsewhere and attributed to someone else. This is sometimes referred to as "off the record."
- Describe an unnamed source's role as fully as possible (without revealing that identity) to help audience members evaluate the credibility of what the source has said or provided. When appropriate, explain to audience members why an anonymous source is being used and why the source does not want to be identified. The approving manager should agree to that description in advance.
- Do not make promises you do not intend to fulfill or may not be able to fulfill.
- Do not threaten sources.
- Anonymous sourcing from wire reports or other media we trust should be used only when necessary. Confidential treatment should align with the Network's best practices, and sourcing should be attributed to the appropriate organization.
- Wirereportsandothermediareportsthatrelyuponconfidentialsourcesshouldbe evaluated on a case-by-case basis, taking into consideration the credibility of the media source and our own best practices. It may be appropriate to refrain from running a report, or to attempt to independently verify the information if possible. It may also be appropriate to alert our audiences that the report relies upon information we have not verified.

Being Fair

Summary: This section emphasizes the importance of fairness and balance in reporting.

- Seek appropriate comments from accused persons and/or organizations before publication.
- Update information and add comments as they become available.
- Give special consideration to privacy for children and victims of sexual assault.

Being Independent

Summary: This section discusses maintaining credibility and avoiding conflicts of interest.

- Disclose potential conflicts of interest to supervisors.

- Ensure partnerships and sponsorships do not influence news coverage.
- News staff members are encouraged to be involved in worthwhile community activities, so long as this does not compromise the credibility of news coverage.
- When unavoidable personal, business, or social media interests could compromise the news organization's credibility, such potential conflicts must be disclosed to one's supervisor and, if relevant, to the audience after consulting with an editor or coach.

Conducting Investigative Reporting

Summary: This section provides guidelines for thorough and ethical investigative reporting.

- Involve multiple editors in planning and editing.
- Document information thoroughly.
- Give subjects of accusations an opportunity to respond.

Aggressive, hard-hitting reporting is honorable and often courageous in fulfilling the media's First Amendment responsibilities, and it is encouraged. Investigative reporting by its nature raises issues not ordinarily faced in routine reporting. Here are some suggested procedures to follow when undertaking investigative reporting:

- Involve more than one producer, editor, or coach at the early stages of planning and shaping coverage and in the editing of the stories, videos, and other content elements.
- Question continually the premise of the stories and revise accordingly.
- Document the information in stories to the satisfaction of the senior news executive.
- Have a "fresh edit" by an editor or coach who has not seen the material as you near publication or posting. Encourage the editor to read it skeptically, then listen carefully to and heed questions raised about clarity, accuracy, fairness and relevance.
- Make certain that care, accuracy and fairness are exercised in headlines, lead-ins, videos, photographs, interactives, presentation and overall tone.
  Whenever possible, make certain that subjects accused of wrongdoing are given an opportunity to answer those charges. Share the outcome of those efforts with our audience, regardless of whether comment was declined.
- Evaluate legal and ethical issues fully, involving appropriate colleagues, superiors, lawyers or dispassionate outside parties in the editorial process. (For example, it may be helpful to have a technical story reviewed by a scientist for accuracy, or have financial descriptions assessed by an accountant, or consult an ethicist or respected outside editor on an ethical issue.)
- Be careful about trading information with sources or authorities, particularly if it could lead to an impression that you are working in concert against an individual or entity.
- Maintain a regular practice for handling any information or notes used or unpublished related to the investigative pieces. Seek advice from a coach, and the Law Department as needed, on best practices.

Editing Skeptically

Summary: This section advises editors to scrutinize content carefully to ensure accuracy and fairness.

- Understand the facts and context of stories.
- Involve multiple editors for complex stories.
- Challenge assumptions and conventional wisdom.

In most cases editors, news directors, coaches and consumer experience directors determine what will be published or posted and what will not. Their responsibility is to question and scrutinize, even when it is uncomfortable to do so. Here are some suggested practices:

- Take special care to understand the facts and context of the story. Guard against assumptions and preconceived notions.
- Ensure time and resources for sound editing. Complex or controversial stories may require scrutiny by several editors or coaches.
- Consider involving an in-house skeptic on major stories–a contrarian who can play the role of devil's advocate. Challenge conventional wisdom.
- Consider what or who may be missing from the story. Include diverse views through a diversity of sources that reflect your community.
- Consider how others–especially antagonists or skeptical readers–may view the story. What questions would they ask? What parts would they think are unfair? Will they believe it?
- Be especially careful of stories that portray individuals purely as villains or heroes.
- Beware of stories that reach conclusions based on speculation and protect against being manipulated by advocates and special interests. (Consider these questions: "How do you know? How can you be sure? Where is the evidence? Who is the source? How does he or she know? What is the supporting documentation?")
- Don't allow deadlines, unrealistic competitive concerns, or peer pressure to force premature publication of an investigative report.

Ensuring Accuracy

Summary: This section highlights the importance of accuracy at every step of the reporting process.

- Verify information with sources or documents.
- Avoid assumptions and guesswork.
- Use reliable sources for fact-checking.

Dedication to the truth means accuracy itself is an ethical issue. Each news person has the responsibility to strive for accuracy at each step of the process.

- Consider carefully information attributed to a source and be sure the person quoted is in a direct position to know.
- Be especially careful with technical terms, statistics, mathematical computations, crowd estimates and poll results. Verify this content with the source or documents where practical or make it clear who is providing the estimate.
- Consider going over all or portions of an especially complicated story with primary sources or with outside experts. However, do not surrender editorial control.

- Don't make assumptions. Don't guess at facts or spellings. Wikipedia is not a definitive source for fact-checking or spelling.
- Consider backing up your notes digitally when ethically and legally appropriate.
- Be wary of archived content and file photos and videos, which may contain uncorrected errors or be misleading, especially if reused in the wrong context.
- Especially in the case of digital breaking news coverage, remember that you are not first if your content is not right. Also, in cases of significant news that has been broken by others, but you have yet to confirm, consider telling your audience that you are working to confirm unverified information others are reporting. When appropriate, say what you are doing to confirm the information. But do not ignore the story. Use caution when the news involves serious allegations of wrongdoing.
- When offering content produced by others or when aggregating content from multiple sources, rely on sources you know to be most reliable and eschew less reliable sources.
- Develop checklists of troublesome or frequently used names, streets, titles, etc.
- Understand the community and subject matter. Develop expertise in areas of specialized reporting.
- Use care in writing headlines, lead-ins, promotions, and summary text. Do not stretch beyond the facts of the story.

Correcting & Clarifying Errors

- Correct errors promptly and transparently.
- Ensure corrections are easy to find and understand.
- Consult with senior editors and legal counsel when necessary.

When an error occurs, the news organization has an ethical obligation to correct the error promptly and minimize any potential harm. However, *before* promising or making changes, we should acknowledge concerns and investigate the claims.

- When a concern about accuracy is received, a determination must first be made that an error was made. The reporter and the appropriate editor/platform manager/producer should confirm that a mistake was made, and the correction request should be reviewed by a senior news official not involved in the original coverage. If the error appears egregious and/or if an outside attorney has contacted the newspaper about the error, then the news organization should contact its attorney or the Law Department and the Network standards editor (contentfeedback@gannett.com).
- In instances when an error is reported in shared content from another Network newsroom, the originating outlet should determine whether a mistake was made. Information about the mistake and the proposed correction should be shared across the Network and, if appropriate, the Network standards editor and legal counsel should be consulted.
- If the facts are right but the context of information might lead users to draw the wrong conclusion, a clarification would be more appropriate rather than a correction.
- Corrections or clarifications should be worded in a manner that does not repeat the misinformation or go into detail about how the mistake occurred. At the same time, the correction should contain enough context so that audience members understand exactly what is being corrected. *Example: A Network newsroom publishes a cover story about fatherhood and says John Doe is a divorced father. He's married. Instead of: A*

cover story Tuesday about fatherhood said John Doe is divorced. He is married. (Repeats the error.) Or: A cover story Tuesday about fatherhood should have said John Doe is married. (Difficult to tell what's being corrected. Did we say John Doe is widowed or divorced? Did we imply he had a child out of wedlock by not giving his marital status?) Say: A cover story Tuesday about fatherhood misstated John Doe's marital status. He is married. (Identifies what we got wrong and what we should have said instead.)

- There are rare instances when it is appropriate to explain how an error occurred. Those would include cases in which incorrect information was provided to the news organization, or if it is necessary to protect the reputation of a reporter who was not responsible for the error.
- Corrections and clarifications should be easy to find in the paper and online. We anchor them in the paper and append to the top of stories online. Placement exceptions can be made to avoid confusing the audience.
- For online content, we label explanations "*Corrections & clarifications: Xxxxx*" when setting the record straight, and we reserve such labeling as "*Editor's note: Xxxx*" for other explanations of news coverage.
- We consider how content is shared, such as video and social media, when setting the record straight.
- Errors on social media should be corrected promptly. In some cases, it may be necessary to delete a post.
- For video, correction/clarification language should be included in the video chatter and a correction slate included at the end of the footage with that explanation. The clarification needs to be in both places because sometimes the video appears without its chatter in syndication or promotion on other sites.
- Any decision to delete a video or audio feed should be approved by a senior newsroom manager.
- In cases where a video/audio has been modified or deleted but there is no story text, we still owe readers an explanation for the change. Establishing a corrections log on the website provides a newsroom window for greater transparency when addressing standalone items.
- In the event a mistake occurs on video/audio produced by a content partner, we should alert the partner of the error before making a final decision on whether to correct the record. Errors of common knowledge can be addressed immediately but we should alert the partner.
- For online photos, the appended correction/clarification information should follow the corrected text and should be italicized and placed in parenthesis. *Example: Randy Jackson and Ryan Seacrest are American Idol holdovers. Mariah Carey, Nicki Minaj and Keith Urban are the newcomers. (An earlier version of this photo information misidentified one of the show's new judges.)*
- If the foundation of the story is erroneous, or if the inaccuracy resulted from an egregious ethical violation, it may be best to correct the error with another story admitting the error. Any such case requires consultation with the Law Department, as does any case in which a legal vulnerability appears to exist, or a lawyer's letter of complaint has been received. This should be handled working with a senior newsroom editor.

We do not remove archived material or "unpublish" content from our digital platforms, except in rare instances when simply correcting/clarifying information may not be enough. Any decision to take down a story should come only after a broader conversation with a top news leader in the newsroom. Some situations may involve consultation with the Law Department.

Social Media Guidelines for Journalists

- Be transparent about your affiliation with USA TODAY Network.
- Ensure social media content meets the same standards as published content.
- Respect confidentiality and avoid sensationalism.

Abide by the Principles of Ethical Conduct for Journalists. These Principles are centered on the following themes:

- Seeking and reporting the truth in a truthful way
- Serving the public interest
- Exercising fair play
- Maintaining independence
- Acting with integrity

When covering assignments, be transparent in social media and always make clear that you work for the USA TODAY Network or your specific newsroom property.

Consider that the content you post is public and should meet the same standards as information you publish or post on Network platforms.

If you make a mistake, acknowledge your error and correct it as quickly as possible after consulting with your manager and others as appropriate.

Avoid oversimplifying or sensationalizing issues; place your thoughts in context.

- Remember that social network platforms are forms of public expression and should be used for strategic reasons to enhance your journalism, engage your community of followers, enlighten your news outlet's audience, and promote your news organization's brand in a positive way. Like other forms of public expression – attending political demonstrations, voicing opinions on a talk show, making political campaign contributions – they are subject to the limitations that are placed on newsroom employees through the Principles of Ethical Conduct.
- These are designed to maintain credibility with the audience.
- Properly attribute your content and link to the original source if possible. Respect others' copyrights.
- Ensure that your public conduct – on and off the job – does not undermine your credibility with the public or the Network's standing as a fair, impartial source of news.
- Although news staffers are encouraged to develop a public personality, that personality cannot cast doubt on the individual's or the organization's impartiality. We provide leeway for greater expression to those who cover opinion.

- Be sure to respect confidentiality of colleagues and sources. It may be appropriate to consider asking permission to publish or report on conversations that are meant to be private or internal.

Reinforcing the Principles

- Communicate principles to colleagues and the public.
- Conduct staff training on ethical conduct.
- Address problems promptly and appropriately.

Every Network journalist has a responsibility to communicate these principles to colleagues and to the public, and communication from newsroom leaders will include the following guidance:

- We ensure that sound hiring practices are followed to build a staff of ethical and responsible journalists. Such practices include making reference checks, conducting sufficient interviewing and drawing reasonable conclusions about the individual's personal standards.
- We provide prospective hires, interns, contract employees and free-lancers with a copy of these principles.
- We conduct staff training as often as needed surrounding the Principles of Ethical Conduct.
- We share these principles with new hires and seek to revisit the guidelines annually to acknowledge an understanding of our standards and to raise any questions about them.
- Raise questions or concerns with the Network standards editor and ethics advisory team by emailing contentfeedback@gannett.com.

Addressing problems

There may be times when coverage or conduct falls short of the principles outlined. When that happens, newsroom leaders will promptly weigh the nature and severity of circumstances to determine next steps. Most cases can and should be settled at the local level. In more egregious situations Network newsrooms will be guided as follows:

- When problems resulting in lapses with standards require heightened alert within the Network, local properties will work with their designated regional editor for help with are solution.
- USA TODAY's executive editor will be the first line of contact for addressing national coverage issues.
- Claims of egregious errors, such as plagiarism and fabrication, or actions that may cause serious harm to individuals or groups of individuals, should be shared as soon as possible, but no later than within 24 hours with their designated regional editor (network) or USAT executive editor (national) for review and next steps. This includes content situations that prompt public backlash or unwanted media attention.
- The VP/Group News Editor or USAT executive editor (national) will work with the newsroom team editor on proposed next steps, recommendations or a resolution. This information will be shared with the USA TODAY editor-in-chief (national), Network standards editor and Network chief content officer for final input and approval.

- Some situations may involve input from human resources, legal and communications teams.

Router Security Policy

Policy Owner: IT Security and Data Privacy
Version: 20250101
Employee Scope: All US employees who work with all routers owned and/or controlled by Gannett.

Purpose

This policy outlines how network routing must be secured within Gannett.
An improperly secured router exposes Gannett to risks including malicious software attacks (viruses, worms, etc.), compromise of network and host computer systems and services, loss of data, reputational harm, and legal action.

Definitions and Acronyms

When navigating this policy, it's important to grasp the terminology. Our Glossary of Cybersecurity Terms provides concise definitions for key concepts.

Policy

Operational Responsibilities

- An operational group must be designated by the appropriate networking manager in the applicable technology tower to manage a Gannett router.
- The operational group responsible for the configuration of the router must have a documented process for maintaining configuration files.
- The operational group that manages routers must ensure that they are configured according to an approved security configuration standard as approved by the Technology Compliance leadership team.
  - The configuration standard must be kept up to date.
- Changes to the configuration must include review and approval by the appropriate networking manager in the applicable technology tower. Any changes that deviate from the approved configuration standard must be approved by the Technology Compliance leadership team.

General Router Security Configuration Policy

- All router configuration files must be secured from unauthorized access.
- Router functions and processes that will not be used must be disabled where possible.
- No one may make copies of router configuration files other than as expressly authorized for Gannett business.
- There must be at least two previous revisions of a working configuration file retained for each router.
- All router software upgrades must be tested prior to being installed, where possible.
  - Upgrades should only be completed to correct a network operational issue, to remediate a reported vulnerability, when an additional feature is required or when otherwise authorized by the networking manager in the applicable technology tower.
- Security patches must be installed on the system in accordance with the Vulnerability Management Policy.

- A secure method for system administration must be used when available (e.g., SSH, IPSec, SSL).
- Network diagrams including all and their topology (describing the location and purpose of each router) must be maintained and updated with any changes in the applicable network.

Physical Access

- Routers should be physically secured based on the Information Technology Physical Security Policy.
- Access to the router console must be restricted to staff approved by the appropriate networking manager in the applicable technology tower.

Monitoring

- All security logs must be kept available for at least 30 days or as dictated by the applicable configuration standard.
- Logging detail level will be dictated by the appropriate configuration standard. In the absence of a configuration standard, the minimum logging should include the following when the option is possible:
  - All logon attempts.
  - Configuration changes.
- Security-related incidents must be reported according to the Cybersecurity Incident Reporting Policy.

Access Privileges

- Account access to a router is considered an elevated privilege and must be documented in accordance with the Account and Access Management Policy.
- Account access to a router may only be provided as necessary to accomplish assigned tasks in accordance with that user's job function.

Routers That Are In-scope for PCI (Payment Card Industry)

- Routers in-scope for PCI must have their rule sets reviewed at least every six months to verify that they accurately represent approved and consistent configurations as required by the PCI-DSS standard.

Enforcement and Exception

- Compliance with this policy is required under Gannett's Information Security Policies and Standards Enforcement Policy and Gannett may take actions in response to non-compliance as provided under the Enforcement Policy.
- Any exceptions to this policy must follow Gannett's Information Security Policies and Standards Exceptions Policy.

This policy may be updated occasionally by the Company. The current version of this policy, as well as policies referenced in this document, may be viewed on MyLife@Gannett.

Sales Compliance Certification

Policy Owner: Legal
Version: 20240105
Employee Scope: All new sales employees

Sales Compliance Certification

I agree that during my employment with Gannett or its affiliates ("Gannett"), I will abide by these guidelines and I will not deviate from them without advanced written authorization (email, tickets, etc.)—that I will retain—from Support, the Finance Department or the Legal Department, as applicable:

1. I understand that LOCALiQ's media products are bundled solutions. A portion of each client's campaign budget is used to purchase media, which varies by client due to a number of factors. In addition to the media spend, a client's campaign budget also pays for use of LOCALiQ's technology platform, and costs for campaign management, support personnel, operations and certain third-party services, all of which are required to deliver excellent results. I have received regular training and I will comply with it in all regards, including but not limited to with respect to how I describe LOCALiQ's pricing and services to prospective and current clients. I understand that I should never make any misrepresentations to a client and should answer any questions about our pricing honestly.
2. I will not add to or modify Order Forms (also known as the Insertion Order, IO, Electronic Agreement, or Paper Contract) or Terms and Conditions other than completing the applicable required information.
3. I will not agree, in writing (including via email) or verbally, to a credit, refund or reduction of any amount owed.
4. I will only apply credits to clients for whom the credits were intended, and I will not transfer credits from one client to another client.
5. I will not offer or agree, in writing (including via email) or verbally, to provide any services to any client in exchange for compensation of any kind other than those covered by a LOCALiQ Order Form.
6. If I provide my client with additional financial analysis or billing information, it will not alter the amounts owed or the due dates, as set forth either in the Platform or otherwise indicated by the finance department.
7. During the regular course of business while employed at Gannett, with the exception of utilizing a service offered to the general public such as teeth cleaning, plumbing services, or the like, I will not conduct personal business with a Gannett client or vendor outside of the standard Gannett sales process, whether the business is of a competitive nature or otherwise.
8. I will not sell or refer to another provider any service that is offered either in whole or in part by LOCALiQ. The only two exceptions to this rule are: a. Website design referrals, for which I have obtained the advanced written (or emailed) approval of my RSM, because the website requires a different functionality than that offered by LOCALiQ website; and b. Display creative requiring a different functionality than that offered by LOCALiQ.

9. For products and services that are not offered by LOCALiQ, I will not accept a commission, fee or kickback of any kind in exchange for my referral of such businesses to a vender or other business.
10. I will not have any involvement in any business other than Gannett, or if I am involved in some other sort of business. I have fully disclosed this to the Human Resources department.
11. I will not use personal funds to pay for client campaigns.
12. I will not distribute promotional materials or gifts to clients from any business or organization other than Gannett, including from other Gannett clients.
13. I will not personally profit from any interaction with a client, other than to occasionally accept gifts that comply with the Gannett Code of Business Conduct and Ethics Policy (a copy of which I have reviewed).
14. I will not give gifts to any client that would constitute a violation of the Gannett Code of Business Conduct and Ethics Policy.
15. I will not recruit Gannett employees for any other type of business.
16. I will follow financial approval process to get any custom rate (off rate card) approved by all approving parties before presenting to the customer.
17. I will retain an approved form of authorization for advertising and marketing services buys from clients before ordering and billing.

If there are any exceptions to the above, I have fully disclosed them to Human Resources or the Legal Department. I understand that any violations of this policy will subject me to disciplinary action, up to and including termination.

Server Time Policy

Policy Owner: IT Security and Data Privacy
Version: 20250101
Employee Scope: All US employees who work with all internal premise-based systems that are Gannett- owned and/or controlled by Gannett including, but not limited to, domain controllers, desktops, servers (including iSeries), and network equipment ("Gannett Internal Systems").

Purpose

- This policy ensures time synchronization technology is implemented for accurate and consistent synchronization of all critical Gannett system clocks.
- This policy will cover the requirements to acquire, distribute and store the accurate time on Gannett systems.

Definitions and Acronyms

When navigating this policy, it's important to grasp the terminology. Our Glossary of Cybersecurity Terms provides concise definitions for key concepts.

Policy

- Gannett Internal Systems must synchronize their clocks to an accurate Network Time Protocol (NTP) system.
  - The NTP source for Gannett must be based on International Atomic Time or Coordinated Universal Time (UTC).
  - The Gannett NTP Infrastructure configuration must adhere to the Payment Card Industry Data Security Standards (PCI DSS).
  - The Gannett Technology team must have processes to verify synchronization and monitor the NTP Infrastructure.
- The configuration standard must be updated based on the latest vulnerabilities.
- Configuration changes must follow the Gannett Change Management Policy.
- Access to Gannett's NTP Infrastructure must be restricted to approved personnel that require access as necessary to accomplish assigned tasks in accordance with that user's job function.

Enforcement and Exception

- Compliance with this policy is required under Gannett's Information Security Policies and Standards Enforcement Policy and Gannett may take actions in response to non-compliance as provided under the Enforcement Policy.
- Any exceptions to this policy must follow Gannett's Information Security Policies and Standards Exceptions Policy.

This policy may be updated occasionally by the Company. The current version of this policy, as well as policies referenced in this document, may be viewed on MyLife@Gannett.

Signature Authorization Policy

Policy Owner: Finance
Version: 20250515
Employee Scope: All employees

Purpose

The purpose of this Policy is to promote the efficient operation of the Company and establish sound internal controls where only individuals with properly delegated signature authority are able to commit the Company to binding obligations and execute Contracts, as defined below, on behalf of the Company.

This Policy establishes guidelines, procedures, and requirements for:

(a) Designating the persons who are authorized to commit the Company to binding obligations and execute Contracts on behalf of the Company ("**Authorized Signatory**" or "**Authorized Signatories**"); and

(b) Defining the limits, if any, on such authority.

Except as otherwise stated herein, this Policy supersedes all signature authorization practices and policies adopted by the Company, including any prior delegations of authority.

This Policy applies to all Contracts entered into on behalf of the Company. Contracts include, without limitation, all agreements, licenses, leases, promissory notes, instruments, assignments, powers of attorney, terms and conditions, memoranda of understanding, letters of intent, settlements, releases, waivers, renewals, amendments, or modifications to existing contracts, claims, disputes, representations, and other similar documents and commitments (collectively, "**Contracts**"). Contracts also include any online web services and/or agreements, including, but not limited to software licenses, terms of service, and privacy policies (collectively, "**Online Agreement**"). Authorized Signatories must obtain legal approval before clicking "Accept" or otherwise indicating acceptance, via "click-to-sign", "click-wrap", "click-through" or "checkbox" methods, of any Online Agreement.

Policy

(a) All Contracts must be in writing.

(b) **ORAL CONTRACTS ARE <u>NEVER AUTHORIZED</u> REGARDLESS OF WHETHER THERE IS A MONETARY EXCHANGE.**

Anyone found to be out of compliance with this policy, including sales representatives who sign contracts on anything other than standard paper are subject to disciplinary action up to and including termination.

Application of Policy

1. Signature Authorization

The Board of Directors may authorize, or provide for the authorization of, officers, employees or agents to enter into any Contract or execute and deliver any instrument in the name and on behalf of the Company. Any such authorization may be general or limited to specific Contracts or instruments.

2. Authorized Signatories

(a) An individual is designated an Authorized Signatory pursuant to one of the following:
  (i) Company By-Laws; and
  (ii) the Board's authorization via a written resolution. The Company's Authorized Signatories are the Executive Committee Members and the Designated Signatories identified on Schedule A, attached hereto.

(b) Only Authorized Signatories have authority to execute Contracts, subject to:
  (i) any limitations, if any, set forth in Schedule A; and
  (ii) Subsection 4(c) below.

(c) AUTHORIZED SIGNATORIES CAN ONLY EXECUTE A CONTRACT AFTER RECEIVING PROPER DOCUMENTATION/EVIDENCE THAT SUCH CONTRACT HAS BEEN REVIEWED AND APPROVED BY THE CORPORATE LEGAL DEPARTMENT AND THE CORPORATE FINANCE DEPARTMENT IF REQUIRED PER THE COMPANY'S TECHNICAL ACCOUNTING CONSULTATION GUIDELINES defined in Schedule B of this policy.

(d) With respect to any approvals required under this Policy, including without limitations Subsection 4(c), approval:
  (i) will be in the form of emails from the Corporate Legal Department and the Corporate Finance Department; and
  (ii) with respect to the Corporate Finance Department, approval will be from the applicable FP&A Partner per the Company's Technical Accounting Consultation Guidelines, attached hereto as Schedule B.

(e) Authority to sign includes physical signatures and electronic signatures.

3. Responsibilities of Authorized Signatory

Each Authorized Signatory is responsible for:

(a) Ensuring that he or she has the appropriate authority to execute and approve a Contract.

(b) Exercising his or her authority with care and diligence. The Authorized Signatory should undertake appropriate investigation and inquiry to confirm that the Contract and any commitments made on behalf of the Company are:
  (i) based on accurate information;
  (ii) being made for a proper purpose, in the best interest of the Company, and in furtherance of its mission;
  (iii) capable of being lawfully undertaken by the Company;

(iv) in compliance with other Company policies; and
(v) not in conflict with existing Company agreements.

(c) Confirming that all other reviews and approvals required by applicable Company policies, including the requirements under Subsection 4 under this Policy, have been obtained prior to Contract execution, including:
(i) subject matter approvals, such as by the risk management (data privacy and security) and tax departments, and other relevant specialized personnel within the Company;
(ii) funding approvals; and
(iii) the approval of any other business department affected by the Contract.

(d) This Policy is not exhaustive. The Company expects all Authorized Signatories to exercise common sense and judgment in carrying out the decision-making process, such as when deciding the precise consultation and approval route for a particular Contract. If any Contract is of an unusual nature or outside the normal course of Company activities and practices, the Authorized Signatory should elevate such Contract to a higher organizational level for review and decision, even if the Contract is within the Authorized Signatory's scope of authority.

4. Compliance with Other Policies

Signature and approval authority does not override other safeguards in the contracting process. Any approval and execution of a Contract must comply with all relevant policies, internal controls, and guidelines of the Company, including those procedures and forms specific to the nature of the activity. This includes, without limitation:

(a) Conflicts of interest. All Company employees are responsible for ensuring that the Company does not enter into a Contract that presents a real or perceived conflict of interest. All Company employees shall comply with the Company's Code of Business Conduct and Ethics Policy when reviewing, approving, or otherwise exercising their authority with respect to such Contract. If a real or perceived conflict of interest does arise, the issue must be resolved prior to entering into such Contract, as required by the Company's Code of Business Conduct and Ethics Policy. Questions about possible conflicts of interest should be directed to the Corporate Legal Department. A copy of the Company's Code of Business Conduct and Ethics Policy is available at Code of Business Conduct and Ethics Policy.

(b) Other Company policies. The review, approval, and exercise of authority under this Policy must comply with other Company policies and procedures.

5. Signature Requirements

Each Authorized Signatory approving a Contract must affix his or her own signature (physical or electronic, as permitted) to any Contracts that are required to be signed. Signing or fixing someone else's name is strictly prohibited, except in special circumstances where permission is granted in writing for an express purpose by the person whose name is being affixed.

6. Violation of this Policy

(a) Only Authorized Signatories may sign Contracts on behalf of the Company. Any other individual who enters into a Contract that purports to bind the Company is

acting without authority and may be subject to discipline, up to and including termination of employment.

(b) Conduct that violates this Policy is always considered outside the scope of employment of any employee acting on behalf of the Company.

(c) Any employee, regardless of position or title, who violates any provision of this Policy (including individuals who enter unauthorized Contracts) will be subject to discipline, up to and including termination of employment.

Administration of Policy

1. The Company expressly reserves the right to change, modify, or delete the provisions of this Policy without notice.
2. The Corporate Legal Department is responsible for the administration of this Policy. All employees are responsible for consulting and complying with the most current version of this Policy. If you have any questions regarding this Policy, please contact Sheryl Costa in the Corporate Legal Department at scosta@gannett.com.
3. If a Contract's dollar threshold is greater than the established "Threshold", such Contract must be sent to the Chief Financial Officer or the Chief Legal Officer for review.
4. Third party distribution agreements include, without limitation, carrier agreements, freelancer agreements, stringer agreements, photojournalist agreements, B2B Commercial Distribution agreements and large-scale commercial distribution agreements.
5. Only the Chief Executive Officer, Chief Financial Officer or Chief Legal Officer can change the individual and/or aggregate dollar amounts.

[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK]

Schedule A

Authorized Signatories

Threshold (per agreement)	Title
$500K	**Sales Representatives** – For revenue based standard advertising contracts only, including without limitation advertising commitments and insertion orders, up to the threshold. Any changes to the standard Gannett Terms and Conditions and standard contract language must be pre-approved through the Custom Finance Approval (FA) process and all changes to legal terms and conditions must be pre-approved by Gannett Legal. All third-party paper must be pre-approved by Gannett Legal prior to making any commitments to the client and any changes to Gannett's standard rates on third-party paper must also be pre-approved through the Custom Finance Approval (FA) process.
$500K	**Sr Director Real Estate** – For real estate and purchase contracts only, including lease contracts with annual leasing payments up to the threshold.
$500K	**Chief Privacy Officer** - For privacy-related contracts only, including data processing agreements and privacy services agreements, with annual payments up to the threshold.
<$1.5M	* See chart below
<$2.5M	SVP Publishing Operations, Steve Wagenlander
	SVP Corporate Development, Jay Fogarty
	SVP Finance, Chief Tax Officer, Walt Nagel
≤ $5M	Executive Committee, GM DMS
$5M +	Chief Legal Officer, Chief Financial Officer, Chief Executive Officer
$50K	Jeremy Billy, VP Corporate Development
Insurance Policies	SVP Corporate Development, Jay Fogarty
Varies	Signing authority for third-party distribution agreements are limited as follows: **(a)** Carrier Agreements will be executed on the "one over one" basis (i.e., executed by both the District Manager and his/her direct Supervisor) with annual revenues or expenditures not to exceed the Threshold set forth in the chart below; **(b)** Commercial

	Distribution Agreements (i.e., Gannett delivers third-party product or third-party delivers Gannett product) will be executed by SVP Publishing Operations or VP Publishing Operations up to their respective Threshold set forth in the chart below; and **(c)** Large Scale Commercial Distribution Agreements (e.g. PCF and ANS) will be executed by SVP Publishing Operations or VP Publishing Operations up to their respective Threshold set forth in the chart below.

***Signature Authority Up To $1.5M**	
Name	**Title**
Alex Hunsucker	SVP, Chief Product Officer, DMS
Allen Jones	SVP Sales
Caroline Harris	VP, Content Monetization
Cher Tate	Sr Deputy General Counsel
Cindy Gallagher	Chief Accounting Officer and Controller
Ed Larkin	Chief Litigation Officer
Garrett Cummings	Deputy General Counsel
Jennifer Thomas	General Counsel, ReachLocal
Jonathan Camerata	SVP Chief Sales Officer
Michelle Ngo	SVP, Consumer Success
Rajendra Sudra	SVP Engineering
Renn Turiano	SVP Product Gannett Media
Sheryl Costa	Legal Operations Director
Terri Snider	SVP People Operations
Thomas Curley	Associate General Counsel
Tony Simmons	VP Publishing Operations

Schedule B

Technical Accounting Consultation Guidelines

Background

As business leaders negotiate agreements in the normal course of business, specific contract terms or conditions may be identified in contracts that require additional accounting policy consultation prior to execution. The primary purpose for the consultation is to ensure timely communication to accounting to ensure complete and accurate financial statements and compliance with existing lender requirements.

Policy

The following transaction types require technical accounting policy consultation prior to execution:

Contract/Contract Term/Activity	Threshold
Joint Venture Agreement	No threshold
Partnership Agreement	No threshold
Gannett investment in third party	No threshold
Contract granting GCI Equity or Ownership	No threshold
Contract granting GCI Board Representation	No threshold
Agreements with related parties	No threshold
Contracts with EY or Grant Thornton	$500,000
Agreements between entities with minority interests	No threshold
Company-wide restructuring plans	No threshold
Executive compensation agreements that include stock compensation and/or other non- standard terms (ex. special bonus, non-standard change of control)	No threshold
All side letters / agreements documenting terms apart from a base agreement	No threshold
Initial revenue recognition determination for all new products that are expected to generate more than $5 million in revenue (if new product doesn't initially qualify but subsequently crosses this threshold the revenue recognition determination should be submitted for evaluation when the threshold is crossed)	$5,000,000
All collaborative agreements	No threshold
Sale of Tradename, Patent, etc.	No threshold
Business Divestitures	No threshold
Business Acquisitions	No threshold

Contract/Contract Term/Activity	Threshold
Loan Contracts	No threshold
Debt Contracts	No threshold
Line of Credit Contracts	No threshold
Non-Real Estate or Vehicle Leases	$100,000
Contracts containing a derivative or hedge	No threshold
Contracts with Material Purchase Commitments*	$1,000,000 total commitment
Contracts with Minimum Spend Commitments*	$1,000,000 total commitment
Material Outsourcing Agreements	$1,000,000 total commitment
Contracts containing terms that are not directly correlated to the underlying purpose of the contract (ex. Software License contract granting GCI stock awards)	No threshold

**Excludes newspaper purchase commitments*

Note: The transaction types requiring consultation above exclude required normal course consultations with accounting leaders such as lease agreements, real estate sales, pension plan modifications, etc.

Timing
The team will work as quickly as possible to respond to time sensitive requests associated with contract negotiations that are in progress. The nature of the request drives our required response time. We ask for a minimum of one day for time sensitive requests.

Where to go for help

Please contact AccountingPolicyConsultation@gannett.com with any questions or concerns.

Social Media Guidance for Newsrooms

Policy Owner: Legal
Version: 20230911
Employee Scope: All News Division employees

Overview

This guidance includes concepts and language developed by Gannett journalists and The Associated Press, NPR and Scripps.

Gannett's expectations for journalists in the social media environment are found in the Principles of Ethical Conduct and the Gannett Social Media Policy. The guidance below applies these long-tested principles to the ever-changing social media arena. The following questions and answers are designed to help journalists best operate in the world of social networks as to advance both our brands and their own identities. This guidance will be updated and revised as developments warrant.

Nothing in this document prohibits or interferes with employees' rights to communicate with work colleagues about terms and conditions of employment. Social media accounts should not be used to comment inappropriately on the work of others or about Gannett.

Accounts

Q: Should Gannett journalists have social media accounts?
A: All Gannett journalists are strongly encouraged to have accounts on social networking sites. These sites are now an integral part of everyday life for millions of people around the world. They have become a way to deeply engage with people, to better understand and engage with the communities we serve, a tool to improve news gathering, a method for further distribution, and a catalyst to improve our news products on all platforms.

Q: Should Gannett journalists have separate accounts for personal and professional, or one account used for everything?
A: Gannett journalists are encouraged, but not required, to establish separate social media accounts for personal and professional use. Separate accounts enable journalists to maintain a modicum of personal privacy and are a recommended best practice from digital security experts.
All social media activity, regardless of whether personal or professional, is held to the Principles of Ethical Conduct and the Gannett Social Media Policy. This guidance is shared as a supplement to those policy documents.
Whether on your personal or professional account, Gannett newsroom employees should be mindful that any opinions or personal information they disclose about themselves, or colleagues may be linked to Gannett's name, and may impact Gannett's position as a trusted source of news and information. That's true even if staffers restrict their personal pages to viewing only by friends.
Employees should also be aware that records relating to both personal and professional accounts could potentially be discoverable in litigation involving the company and/or the individual.

Gannett employees may also manage branded accounts as part of their responsibilities. These accounts are official accounts tied to the property's brand.
Examples of branded accounts include @USATODAY, the Arizona Republic Facebook page, and @Humankind. Access to the branded account belongs to the company and the name and contents are the property of Gannett. Gannett reserves the right to edit, monitor, promote or cancel the branded account.

For example:
Jane Smith writes a column called "Ms. Bargain."
The Twitter account is @msbargain. If Jane Smith left the company, she would not take @msbargain with her, and it will continue to be maintained by Gannett.
Accounts that incorporate a Gannett brand in any way shall be considered branded accounts. An example of a branded individual Twitter account would be @JohnSmithAZRepublic or Susan Smith's Austin American-Statesman Facebook page.

For example:
John Smith is a columnist at the Arizona Republic. His professional Twitter account is @JohnSmithAZRepublic.
If John Smith leaves the company, he would not take @JohnSmithAZRepublic with him. Access to the branded account remains with Gannett.

Q: What if a Gannett employee who manages a branded account leaves the company?
A: Access to branded accounts remains with the company. When an employee leaves, the company retains the account and responsibility is transferred to another Gannett employee.

PRIVACY

Q: If my personal social network account settings are set as private, can I say whatever I want?
A: All social media accounts are held to the standards of the Principles of Ethical Conduct and the Gannett Social Media Policy. Employees should be mindful that any opinions or personal information they disclose about themselves, or colleagues may be linked to Gannett's name. That's true even if staffers restrict their pages to viewing only by friends.
Posting on a social network is not just like uttering a comment to your friends in person. It's accessible to many more people and it is all too easy for someone to copy material out of restricted pages and redirect it elsewhere for wider viewing.
We do still recommend customizing your privacy settings on social media platforms to determine what you share and with whom. However, as multitudes of people have learned all too well, virtually nothing is truly private on the Internet.

GUIDELINES FOR APPROPRIATE POSTS

Q: Is it OK for Gannett news staff members to express opinions when posting on social media accounts?
A: All content posted on a social media site should be considered "public," even if you have set privacy settings to restrict access to limited numbers of persons. As such the

expression of opinions in a social media environment is subject to the same limitations that are placed on newsroom employees through the Principles of Ethical Conduct. These are designed to maintain the credibility of the journalist and the company brand with the audience.

There may be times when expressing an opinion is a good thing. For example, posts about hometown teams and community pride are areas where opinion is well received. Here are some additional recommendations and considerations when posting content on social media platforms:

- Post reported content or links to verified reporting.
- Avoid sharing your opinion on events in the news when your primary role does not involve opinion journalism. Beware of quick reactions to unfolding situations.
- Pause before you post or share information; consider how the information will affect perceptions of you as a Gannett employee. If in doubt, ask a supervisor.
- Consider posting: Factual, personal experiences; recommend books or resources for individuals who have questions.
- Post factual, verified information.
- Never paint any group with a broad brush. Step back from your own personal experience to view your post as others might.
- If you are concerned about making knee-jerk reactions in the moment, remove social media apps from your phone or take other steps to give yourself time and space. If you are ever unsure, please consult your manager.

RETWEETING

Q: Are there issues with retweeting or sharing posts?

A: Retweets, like tweets, should not be written in a way that looks like you're expressing an opinion on the news issues of the day. Similarly, a retweet should not endorse the accuracy of the reposting if the original tweet relates to a developing story that your newsroom hasn't confirmed. In addition, a retweet with no comment of your own can easily be seen as a sign of approval of what you're relaying.

Examples:

7. RT @jonescampaign: smith's policies would destroy our schools 2. RT @dailyeuropean: at last, a euro plan that works bit.ly/xxxxx 3. RT @TMZ: Michael Jackson has died.

These kinds of retweets must be avoided. Similarly, you shouldn't simply hit Twitter's "retweet" button on tweets like these.

However, you can cautiously retweet opinionated material if you make clear you're simply reporting it, much as you would quote it in a story. Introductory words, colons and quote marks help make the distinction:

Examples:

1. Jones campaign now denouncing Smith on education: RT @jonescampaign: smith's policies would destroy our schools
2. Big European paper praises euro plan: RT @dailyeuropean: "at last, a euro plan that works" bit.ly/xxxxx.
3. TMZ reporting Michael Jackson died moments ago: RT @TMZ: Michael Jackson has died

These cautions apply even if you say on your Twitter profile that retweets do not constitute endorsements.

BLOGS

Q: Are there any rules or restrictions for journalists maintaining personal blogs?
A: A journalist's personal blog/Web site should not address issues typically covered by the journalist in his or her professional role. However, even on a personal blog, journalists are held to the standards of the Principles of Ethical Conduct and the Gannett Social Media Policy.

FRIENDING/FOLLOWING

Q: Are there any issues with friending or following sources or politicians?
A: It is acceptable to friend or follow parties or groups so long as you follow those on the other side of the issues as well.
In addition, there are technically ways to follow people without following or friending them. Using Facebook's Interests Lists and Twitter Lists you can receive postings without joining the person's official list of followers.
For further information on sources, please see the sourcing section of this document. Additional caution is necessary so as not to inadvertently disclose the identity of a source by friending that person.

Q: Is it okay to follow competitors?
A: Yes, you can and are encouraged to follow competitors on social media. This can help you not only keep track of what your competitors are working on; it can also help you create reciprocal relationships with others who may cover the same beat. In social media, audiences like when you share items of interest, even if you didn't write/produce them yourself. That said, caution as noted above should be exercised when retweeting a developing news story which your news organization has not verified. And if the competitor's post is based on an anonymous source, a manager's approval is necessary before you retweet.

PUBLISHING

Q: How should I handle breaking news and social media?
A: Social media should be an important part of your breaking news strategy. When breaking news on social platforms, you should use the same standards and treatments (attribution) as on every other platform we currently use. You may break news on social media if you have thoroughly verified its accuracy. As rumors begin to spread on social media, the public looks to traditional media for the facts.
You should be transparent in your reporting of breaking news and give a window into the process. Social media audiences look for real time updates and will appreciate the efforts we take to obtain the truth.
Sometimes giving the facts to debunk a rumor is the story you can own. We should check out tips. Ignoring rumors is as irresponsible as reporting them.
As soon as you are able, you should provide links to Gannett content.

You can also link to content from other media organizations unless the material spreads rumors based on anonymous sources or unconfirmed information not fit for Gannett publications. Be mindful of competitive and corporate issues as you post links.

Q: May I post information on social media that wasn't in my story?
A: If material you have gathered meets our standards for quality and accuracy, but wasn't included in the story, it is acceptable to share it on social networks. This includes material sometimes referred to as "cutting room floor" content -- material that doesn't make it into our products because of space and time limits. You must consult with your manager before posting.
In addition, behind-the-scenes glimpses of newsroom activity are very well received on social media sites.
Of course, material that hasn't been verified or that you promised to keep confidential should not be posted.

CORRECTIONS/DELETIONS

Q: What should I do if I post something I later realize is incorrect?
A: Erroneous tweets or other social media posts need to be corrected as quickly and transparently as errors in any other Gannett product. This applies to any of your social media accounts.
You should tweet or post that you made a mistake and explain exactly what was wrong.
For example:
Correction: U.S. Embassy in Nigeria says bombings could happen this week at luxury hotels in Abuja (previously we incorrectly said Lagos): apne.ws/uxr9ph
Serious errors need to be brought to the attention of a manager and the appropriate desk.

Q: If I post something I later realize is incorrect or inappropriate, can I just delete it?
A: In most cases, deleting a message is not the best response. However, if the further spreading of the message is detrimental to public safety or could seriously damage our brand reputation; deleting a post may be the best course of action. You need to get approval before deleting a post.
Deleting a post does not necessarily remove it from all social media sites. Posts that have been retweeted or reposted elsewhere will remain publicly visible. If you are deleting a post because of incorrect information, see previous question.
If you do delete a post, the next post with the correct information should note that a previous post had incorrect information and was deleted.

Q: What are the differences with social platforms that I should keep in mind?
A: Some general guidance:
Facebook – FB posts are editable, so edit the post depending on severity, and put a note in comments noting the correction. If the error was also repeated in a story that's part of the post, be sure to correct it there and "refresh share attachment" so the latest information is available to FB readers.
Twitter – You can't edit a tweet, so if it's circulating bad information, take it down and issue a correction tweet.

Instagram - You can edit the captions, so start there. If the incorrect information is in the image or graphic, remove it and put the new image and note the correction in the comments.

SOURCING

Q: Are there any considerations I need to be aware of when finding story sources via social media?

A: It can be difficult to verify the identity of sources found on social networks. Sources discovered there should be vetted in the same way as a source found by any other means. If a source you encounter on a social network claims to be an official from a company, organization or government agency, call the place of business to confirm the identity, just as you would if a source called on the phone.

Special note: Use of social media to locate sources should be restricted to first communication (exchanging contact information). To protect the confidentiality of your newsgathering, avoid exchanging information with your sources via social media. Since social media sites routinely turn over user posts in response to subpoenas, you should conduct your interviews outside the social network -- over the phone or in person.

Q: Are there any special steps I need to take to verify information I see on social networks?

A: Verify information obtained from social networks just as you would for everything else. You should assume that most of the posts you are seeing are unverified rumors. Only once it's proven to be fully accurate should you feel comfortable sharing. To verify a tweet, look at the account: How many followers does it have; how many is it following? What is the link in the bio? Is it an official Twitter verified account?

Investigate the creator of the content just as you would for any other source. You can always ask a manager for help when trying to verify information or an account.

Q: Are there issues with using tweets, photos or other media shared via social networks?

A: To include photos, videos, or other multimedia content from social networks in your news report, we must determine who controls the copyright to the material and get permission from that person or organization to use it. You should never simply lift quotes, photos or video from social networking sites and attribute them to the name on the profile or feed where you found the material. Most social media sites offer a way to send a message to a user; use this to establish direct contact, over email or by phone, so you can explain what you're working on and get more detailed information about the source.

Any exceptions must be discussed with a manager and Legal. See the Gannett Re-Usage guidance.

Q: I'm always careful about checking for sources and permissions with photos I use in Presto. Social media is different though, right?

A: No. Copyright is copyright. If you don't have permission to use something in Presto, you can't use it on FB, Twitter, IG, etc., - unless you're using an embed function or are re-sharing.

INTERACTING WITH USERS

Q: Is it okay for me to engage with readers and viewers on social media?

A: Gannett is strongly in favor of engaging with those who consume our content. Engaging with our communities adds value to the relationships our consumers have with our brands. It is important the audience sees us as more than just their local news source. They need to think of us as fellow members of their community.

Q: How should I respond to audience feedback?

A: Feedback comes in many forms: story chat and comments, corrections, and clarifications and audience complaints.

REACTING TO AUDIENCE COMMENTS

Journalists, editors, and other staff members should consider responding to comments especially when doing so will clarify a point or correct a misstatement.

Don't rise to the bait. It goes without saying that staffers should not offer personal opinions or betray emotions that would raise questions about impartiality or professionalism. That said, all staffers should comment in a voice consistent with their role.

Audiences should be treated with respect. In addressing comments, staffers should be fact-based and respectful.

If you have questions about the best way to handle a comment, contact your manager.

CORRECTIONS AND CLARIFICATIONS

A thoughtful note from a reader or viewer that leads to a correction by us deserves an email or tweet of thanks (try to avoid repeating the original error). If a correction or clarification is needed, it should be changed as soon as possible (news managers should be familiar with our guidelines for handling corrections.)

If someone offers a businesslike criticism of a story or image but has their facts wrong, it's good to reply to clarify the facts.

However, abusive, bigoted, obscene and/or racist comments posted to a Gannett-managed platform or directed at you personally should be flagged to a manager immediately.

AUDIENCE COMPLIANTS, ABUSIVE COMMENTS, AND THREATS

If someone posts a complaint which is not about the accuracy of the story, but about your skills, or you personally, respectfully acknowledge that you have received their complaint. However, you should not get into protracted back-and-forth exchanges with angry people that become less constructive with each new round. While the vast majority should receive a respectful acknowledgment, sometimes silence is the best policy. Insulting or abusive comments directed to you, or any individual staffer should be reported immediately to a manager. If such comments are posted online, contact a manager. Of course, any comments that are truly threatening to individuals should be brought to the immediate attention of your manager.

Any response you make to a reader or viewer could go public. Email and direct Facebook and Twitter messages may feel like private communications but may easily find their way to blogs and political pressure groups, attorneys, and others. In the case of a story or image that stirs significant controversy, the news manager is likely the best person to reply,

rather than the person who created the content. News managers can also reply, saying they investigated the complaint and here's what they found. This is particularly true if the response requires an explanation of Gannett policies or otherwise goes beyond the immediate content in question.

Q: How should I respond to an incoming message that threatens legal action?
A: Any incoming message that threatens legal action against the Company or you should be reviewed by a Gannett attorney before a response is made.

CREDENTIALED NEWS EVENTS

Q: I'm credentialed to cover an event and I'd like to cover it on our social pages too. Do I need to do anything special?
A: Yes. In addition to touching base with your social team colleagues to see what works for them, review your media credentials closely – some organizations may not permit live streaming or other types of social sharing.

Social Media Policy

Policy Owner: Legal
Version: 20230912
Employee Scope: All employees

Overview

All references to the "Company" shall mean Gannett Co., Inc. and its subsidiaries and all references to "we", "us" or "our" will collectively mean the Company and its employees.

Social media is an important part of how we communicate with the public, our consumers, and with both current and prospective advertisers. Social media is also an important part of an employees' life because it provides an environment where they can interact with family, friends and personal communities. Social Media also provides a mechanism that allows us to better understand and serve our local communities and to enhance and improve our journalism. However, employees' use of social media can: (a) pose risks to the Company's confidential and proprietary information, reputation, and brands; (b) expose the Company to discrimination and harassment claims; and (c) jeopardize the Company's compliance with business rules and laws (collectively, "Business Risks"). This Social Media Policy (this "Policy") provides guidance for employees' use of social media, which should be broadly understood for purposes of this Policy to include a variety of internet-based communication tools, including without limitation, Facebook, Twitter, LinkedIn, Instagram, Pinterest, Tumblr, blogs, wikis, microblogs, message boards, chat rooms, electronic newsletters, online forums, social networking sites, and other sites and services that permit users to share information with others in a contemporaneous manner. A violation of this Policy is a serious matter and may result in disciplinary action up to and including dismissal.

Responsibilities

To minimize the Company's Business Risks, to avoid loss of productivity and distraction from employees' job performance, and to ensure that the Company's IT resources and communications systems are used appropriately, the Company requires its employees to adhere to the following guidelines and rules regarding social media use:

- Any use of social media and the content posted may affect various aspects of the Company's business. As such, employees need to know and adhere to the Company's other policies and guidelines that might apply when using social media. The policies and guidelines that employees should keep in mind when using social media include, but are not limited to:
  - Code of Business Conduct and Ethics Policy
  - Anti-Discrimination Harassment and Retaliation Policy
  - Acceptable Use and IT Monitoring Policy
  - Principles of Ethical Conduct for Newsrooms (as applicable)
  - Insider Trading Policy
  - Confidential Information Guidelines
  - Employee Conduct Guidelines
  - Social Media Guidance for Newsrooms (as applicable)

- Employees should refrain from writing or posting anything that could compromise the Company's reputation as a trusted news source.
- Employees should assume that all their activities on a social media site are public, regardless of the privacy tools used, and exercise discretion in sharing personal information, as well as political, cultural or religious views.
- Employees should not represent themselves as spokespersons for the Company unless authorized to do so. If the Company, its products or its people are the subject of content being posted, employees must be transparent about the fact that they are an employee the Company and make it clear that their views do not represent the views of the Company or its employees.
- Employees must not publish, post or release the Company's confidential and proprietary information. Confidential and proprietary information includes, without limitation information regarding projects being worked on, news content that has not been published or made public, products, financial information, know-how and technology, internal reports, internal business-related communications, or communications known to be protected by an attorney-client privilege. If employees have questions or seek more information about what information is deemed confidential and proprietary, please contact the Company's Corporate Legal Department.
- Employees should not post comments that include discriminatory remarks, harassment, threats of violence or similar content.
- Employees should not engage in conduct, whether in the social media environment or otherwise, that adversely affects their job performance, the job performance of their work colleagues, or the interests of our customers.
- Employees should abide by the terms of use of the social networking platforms they use.
- Employees are prohibited from using intellectual property of others (including text, images, audio, photography and video) without the proper license/permission. If employees have any questions regarding the use of intellectual property or are unsure whether they have the right to use certain intellectual property, please reach out to the Company's Corporate Legal Department for guidance. Unauthorized use of a third-party's intellectual property may expose employees and the Company to liability.
- Employees whose position or responsibilities involve regular interaction with the public, government or business officials, or others in the community in such a way that they may be seen as speaking for or on behalf of the Company should be careful when posting, sharing, making or endorsing statements on social media that might be viewed as controversial or political in nature. Employees should also exercise discretion when following, friending or liking other individuals or groups to avoid any actual or perceived conflicts.
- Employees should never post or share anything that they would not be willing to publish.

Journalists

- In addition to the general policies and guidelines for all employees, Journalists should:
  - be transparent in social media and always make clear that they work for the Company or for their respective news organization when working on behalf of the Company.
  - consider that the content they post, and share is public and should meet the same standards as information they publish and share on the Company's news media platforms.
  - properly attribute their content and link to the original source if possible (respect others' copyrights).
  - ensure that their public conduct – on and off the job – does not undermine their credibility with the public or the Company's standing as a fair and impartial source of news[1].
  - be sure to respect confidentiality of colleagues and sources. It may be appropriate to consider asking permission to publish or report on conversations that are meant to be private or internal.
  - review the following policies and guidelines: (a) *Social Media Guidance for Newsrooms*; and (b) *Principles of Ethical Conduct for Newsrooms*.

LEGAL DISCLAIMER: Nothing in this Policy shall be construed as creating any contract (express or implied), duty or obligation on the part of the Company to take any actions beyond those required of an employer by existing law. The Company reserves the right to amend, modify or cancel this Policy at any time and at the Company's sole discretion. Nothing in this Policy shall apply to conduct that is protected under applicable federal, state, or local laws or regulations, including without limitation the *National Labor Relations Act* (collectively, "Applicable Law"). To the extent that any provision in this Policy is inconsistent with Applicable Law, then the Applicable Law will govern. Adherence to this Policy is required by all employees. With respect to those employees coming under a Collective Bargaining Agreement (the "CBA"), this Policy is not intended to replace, amend or supplement any terms or conditions of the CBA. In the event the terms in this Policy differ from the terms expressed in the applicable CBA, the terms of the CBA will govern.

Telecommuting Guidelines for Personnel Who Handle Credit Card Data

Policy Owner: IT Security and Data Privacy
Version: 20250101
Employee Scope: All employees who handle credit card data on behalf of Gannett or Gannett customers

Purpose

The purpose of these guidelines is to outline the required practices that Gannett Co., Inc., and its affiliates (collectively "Gannett") requires of its employees in accordance with the Payment Card Industry Data Security Standard ("PCI DSS") as it relates to telecommuting/working from home ("WFH") and support the Credit Card Environment and Processing.

Ensure Gannett personnel who handle credit card data are aware of the risks related to telecommuting and WFH and what should be required to maintain the security of systems, processes, and equipment supporting processing payments.

Definitions and Acronyms

When navigating this policy, it's important to grasp the terminology. Our Glossary of Cybersecurity Terms provides concise definitions for key concepts.

General Guidelines

- Use equipment and systems provided by Gannett to perform the functions of your job. These items shall remain the property of Gannett and must be returned to Gannett including but not be limited to, cases of extended illness, upon the employee's resignation or termination, or if the telecommuting ends or otherwise upon Gannett's request. Please refer to the Technology Teleworking Guidance provided by the People Division.
- All Gannett files (including those on BYOD devices) must be returned to Gannett including but not limited to cases of extended illness, upon the employee's resignation or termination, or if the telecommuting ends or otherwise upon Gannett's request.
- If account data relating to Gannett or Gannett customers is written down, it must be immediately transferred to the applicable Gannett system and securely discarded thereafter by crosscut shredding.
- The work area/room used by the employee for telecommuting should be a space set aside for work purposes.
- Any materials taken home or sent to an employee's home shall be kept secure, confidentially, and not accessible by non- Gannett personnel.
- All information about Gannett customers including all credit card data, must be kept in strict confidence and protected against unauthorized access including viewing, copying or scanning by others residing or visiting the household.
- Personnel handling credit card data from their home must not connect Gannett provided systems to personal devices such as printers.
- Unauthorized, sharing or storing of payment data is prohibited.

Physical Security Guidelines

- Only authorized Gannett personnel are allowed in the area/room while you are handling credit card data relating to Gannett or Gannett customers (e.g., family members and friends are not sitting may not be sitting in the same area/room).
- System(s) used to process credit card data, and any account data to which personnel have access, must be securely maintained, and not accessible to unauthorized individuals (e.g., keep computer screen locked when not in use).
- Only Gannett approved hardware devices shall be utilized in connection with credit card data relating to Gannett or Gannett customers.
- Telecommuting personnel must take reasonable precautions to protect the Gannett equipment from theft, damage, or misuse (e.g. do not leave a Gannett laptop in a locked or unlocked car).
- The physical environment where Gannett credit card data is handled needs to be effectively monitored and access controlled.

System Security Guidelines

- Utilize multi-factor authentication when accessing Gannett or customer credit card data on Gannett systems.
- Utilize a VPN (Virtual Private Network) connection when accessing Gannett or customer credit card data.
- The latest version of virus protection software shall be implemented (Version updates are applied by the Technology Department).
- Latest approved security patches must be installed (Patches are applied by the Technology Department).
- Do not disable any security controls on Gannett devices.
- Personal firewalls must be installed and operational (Firewalls are maintained by the Technology Department).
- Telecommuting personnel must timely accept all updates and patches pushed to Gannett devices.
- Personnel must notify the Help Desk if their Gannett computer is not working properly (e.g., extremely slow, will not start, does not accept password(s), or will not load software).
- Other individuals in the household shall not have access to Gannett log-in information and Gannett equipment.

If you have any questions or concerns related to the above guidelines, please contact your manager directly.

Enforcement and Exception

- Compliance with this policy is required under Gannett's Information Security Policies and Standards Enforcement Policy and Gannett may take actions in response to non-compliance as provided under the Enforcement Policy.
- Any exceptions to this policy must follow Gannett's Information Security Policies and Standards Exceptions Policy.

This policy may be updated occasionally by the Company. The current version of this policy, as well as policies referenced in this document, may be viewed on MyLife@Gannett.

Travel and Business Expense Reimbursement Policy

Policy Owner: Finance
Version: 20250601
Employee Scope: All employees

Purpose

This document defines and establishes the principles, responsibilities and practices required to reimburse employees for reasonable business expenses that are within the requirements and limitations set within this policy, and are compliant with federal, state and local regulations as applicable. Employees are required to comply with this policy and the related procedures. Failure to comply may result in disciplinary action up to and including termination of employment.

Scope

This policy applies to all employees of Gannett and its direct and indirect subsidiaries (collectively, the "Company") except as noted below. Any exceptions to this policy must be approved by the CFO. The Company understands and will comply with applicable law regarding collective bargaining related to this policy as it relates to employees covered by a collective bargaining agreement, represented by a union.

Policy

The Company assumes no obligation to reimburse employees for expenses that are not incurred in compliance with this policy and the Code of Business Conduct and Ethics policy and, for journalists, the Principles of Ethical Conduct for Newsrooms. The policy may change at any time without notice. Any changes will be applied prospectively.

How to ensure you get paid

1. Always treat work related expenses with the same rigor you would your own. We don't believe in "company money".
2. If you aren't sure if you should incur/claim an expense, you probably shouldn't. When in doubt, ask.
3. All travel must be booked and expenses processed through Concur
4. Use approved travel partners for air, lodging, auto and rail, as designated in Concur as "Preferred". Exceptions must be approved by the Travel Program Administrators ("TPA") at travel@gannett.com.
5. Receipts must accompany your expense claim (see Appendix A for examples)
   a. All cash reimbursement requests, except tips of less than or equal to $5, require a receipt
   b. All expenses incurred on the company card over $75 require a receipt
   c. Some vendors will automatically submit e-receipts in Concur. If you enable this functionality, no further documentation will be required for these specific vendors.
   d. When submitting receipts, full credit card numbers should not be included
   e. Credit card or bank statements are not considered valid receipts
6. Avoid travel except when a business need justifies the expense. Consider the use of video or audio conferencing as an alternative. Essential travel is defined as:

   a. News gathering
   b. Client facing meetings and events
   c. Events, meetings and conferences sponsored or otherwise pre-approved by management
7. Use Gannett's company credit card if submitting four or more expense reports per year (not including mileage and cellphone reimbursements). The application for a card can be found here: Card Application Form. **Please ensure you are behind Gannett's firewall, using VPN, to access this application.**
8. Ensure the business purpose is documented for each expense
9. Submit your claim within 35 calendar days of completion of a trip or incurrence of the expense. Notify the Shared Services Finance personnel (expensereports@gannett.com) in cases where the 35-day deadline falls after a quarter-end or if the reimbursement request is for expenses > $25,000. Expenses not submitted timely will result in notification to the Executive Committee and Human Resources.
10. While some travel websites may appear to offer lower rates in certain situations, they come with restrictions such as no change of date or cancellation refunds or credits. If you consistently find a lower rate for the exact same travel situation, please contact the TPA by emailing travel@gannett.com.
11. Gannett will not be responsible or liable for any costs incurred not in compliance with this policy
12. We reserve the right to withhold reimbursement while we investigate reimbursement requests
13. Submitting fraudulent receipts, falsifying expense reports, or using the company card for personal expenses will result in disciplinary action, up to and including termination of employment and possible legal action.

Your responsibilities as a manager

1. Ensure employee awareness and compliance with this policy
2. Reject any non-reimbursable or inappropriate expenses
3. Managers will be held accountable for inappropriately approving expense reports that are not in compliance with this policy

About your company card

1. Company cards must be used for business travel, meals, and entertainment expenses if the employee submits at least four expense reports per year.
2. Company cards may not be used for personal expenses. If a card is accidentally used for a personal expense, please alert expensereports@gannett.com immediately for reimbursement instructions.
3. Company card transactions may take up to a week from the date of purchase to become visible in the corporate expense management tool. Please allow time for the card transactions to appear in the expense management tool before submitting a corresponding expense report. Company card transactions should not be submitted with a payment type of "CASH".

Allowable Expenses

Allowable expenses by category are set forth in the attached following exhibits:

1. Exhibit A: Travel Related Expenses
2. Exhibit B: Entertainment and Other Expenses
3. Exhibit C: ReachLocal Supplemental Guidelines

Employee Questions

Please email expense reimbursement policy questions to expensereports@gannett.com.

Exhibit A
Work Related Travel Expenses

Where you are required to travel for work, we expect you will incur work-related travel expenses. The below outlines the types of allowable expenses incurred by an employee traveling for business purposes. Personal travel or other personal expenses during a business trip, including but not limited to a family member's expenses if accompanying a Company employee on a trip, are not reimbursable. Personal property theft or loss while on a Company business trip is not reimbursable.

1. Lodging
   a. Lodging is an allowable expense when an employee is required to be away from home overnight. Employees are encouraged to secure reasonably priced accommodation to minimize the cost to the Company. Costs associated with upgrades will not be reimbursed unless standard accommodation is not available.
   b. In-room movies, mini-bar, and spa services are not reimbursable expense.
   c. Laundry services and valet parking are generally considered non-reimbursable expenses.
   d. Hotel cancellations must be made in a manner to minimize costs.

2. Meals
   a. Employees' daily meal expenses should not exceed $65.
   b. For tax purposes employees must note in their expense report whether the meal was on (on the business premises) or off-site and include a list of those in attendance.
   c. Meals for special events, leadership meetings, or group travel that are anticipated to exceed the daily limit should be pre-approved by the employee's direct manager. Pre-approval in writing must be included with the receipt when the expense report is filed.
   d. The most senior level employee present must pay for the meal or event expenses.

3. Transportation
   a. Air Travel
      i. Airfare must be booked at least 14 days in advance of travel to ensure the lowest cost. Exceptions may be made for last minute travel in areas such as breaking news or other exigent business needs.
      ii. The lowest reasonable coach fare available for all domestic flights must be selected.
      iii. Business class for international flights with a single leg exceeding seven hours is permitted if the CEO or an Executive Committee ("EC") member has approved such prior to booking.
      iv. Travel to/from airports and airport parking should be managed cost effectively
      v. TSA PreCheck charges are reimbursable under the following conditions:
         1. Employees by nature of their role, and considering current travel patterns, are expected to travel for business purposes more than 12 times per year.
         2. Department head approval email or other documentation must be attached when employee requests reimbursement.

3. Reimbursement only applies to TSA PreCheck and not to Clear or Global Entry.

b. Car Rental
   i. Intermediate models or smaller vehicles must be rented unless more than two people are traveling together. Rental of larger vehicles is permitted if transporting materials and cargo space is a factor or if local weather dictates another vehicle for additional safety. Incremental costs of vehicle upgrades are not reimbursable.
   ii. Employees should refill the vehicle before returning it and decline the refueling option when picking up a rental car (unless the rental car agency is offering a refueling price that is comparable with the rates in the area, as verified by the employee, or there are safety or health concerns). Rental cars should be returned to the original rental location whenever possible to avoid costly drop-off charges.
   iii. Insurance should be declined for domestic car rentals, although all available coverage should be accepted for international car rentals.
   iv. Reimbursement for toll pass rental is permissible where reasonable and applicable, e.g. travel route requires highway and/or bridge tolls.

c. Rail
   i. Acela service is recommended for travel between New York City and Washington D.C.

d. Personal Vehicles / Mileage
   i. Mileage is not reimbursable while using Company-provided vehicles.
   ii. All mileage reimbursement requests are required to use the Concur Drive App or Concur Mileage Calculator. More information on the Concur Drive App can be found in these three locations:
      i. Concur Drive Getting Started Guide
      ii. Concur Drive Online Course
      iii. Concur Drive FAQs
   iii. For employees assigned to work exclusively from their home office, all business mileage is reimbursable.
   iv. For employees assigned to a Company office, the commuting mileage to and from home is not reimbursable and should be deducted from mileage reimbursement requests (i.e., if an employee's normal commuting mileage is 10 miles and the business trip requires a 15-mile drive, the reimbursement mileage is 5 miles).
   v. Parking at the employee's assigned home office or co-work location is not reimbursable.
   vi. Parking costs and tolls incurred during non-commuting business travel is reimbursable.
   vii. Mileage reimbursement is intended to cover the costs of the use of an employee's vehicle. Costs such as maintenance, fuel, oil and insurance are not reimbursable.

viii. Parking tickets, fines and any other motor vehicle violations are not reimbursable as employees are expected to comply with all legal requirements.

e. Taxi / Rideshare / Shuttle / Public Transportation
   i. Employees should evaluate their individual circumstances and select the safest, most economical alternative when traveling to and from all destinations.

f. Cellular Expenses during Travel
   i. See Mobile Policy.

Exhibit B
Entertainment and Other Expenses

1. Entertainment Expenses
   a. Expenses incurred while entertaining business associates/clients are allowable to the extent that the expense is reasonable and necessary, occurs infrequently, and complies with the provisions of the Company Code of Business Conduct and Ethics policy.
   b. Expense details must include the name of the person or persons who are being entertained, as well as the purpose of the entertainment.
   c. Personal expenses and entertainment are not reimbursable.

2. Employee Gifts & Awards
   a. Managers and employees may give personal gifts to fellow employees if the gifts are in good taste, reasonable and appropriate. These gifts must be paid for by the employee and not expensed to Gannett, including during the holidays.
   b. Gifts of flowers or food are acceptable for one time life events such as birth, adoption, bereavement or hospitalization subject to business unit approval and are limited to $100.
   c. Gift cards used as incentives, onetime bonus, or as part of a team building program must be preapproved by the CFO. The recipient(s) of the gift card should be notated in the expense submission.
   d. All gift cards or cash equivalent awards are considered taxable to employees. A list of employees receiving gift cards or cash equivalent awards and the amounts must be provided to Payroll at DayforcePayroll@Gannett.com immediately following distribution (refer to Section F for procedures) to ensure proper tax withholding and reporting on the employees W2. Gift cards or cash equivalent awards will not be grossed up for tax purposes.
   e. Eligible employees who have earned the Sales award travel are required to comply with the expense and reimbursement terms as outlined by the travel award event. Per IRS regulations, award travel is considered taxable income and reported on Form W-2. The value of the award travel will be reported in the pay period as income following the award travel and the employee will be responsible for the payroll taxes. The value of award travel is not grossed up to cover the payroll taxes due. In the event the eligible employee is not able to attend the award travel event, the value will not be included in the employee's income and no payroll taxes will be due on such value however, the value of any alternate award given to the employee will be reported as income and reported on Form W-2, and subject to payroll taxes.
   f. Managers are required to follow the procedure below to report a taxable award to Payroll:
      i. Populate the template with the employee recipient information and value amounts Gift Card Reporting Form Send the completed template back to Payroll using the email: DayforcePayroll@Gannett.com.
      ii. Information supporting the business reason and approvals for the distribution of gift/prize/award must be included.

iii. For gifts/prizes issued near the end of year, if receipt of final information is not received in time for the final biweekly pay period, taxable amounts will be included in a future pay cycle in the next calendar year.

3. Other Expenses
   a. Membership Dues: With pre-approval from an employee's manager to ensure both appropriateness and budget capacity, membership dues for professional organizations and associations are reimbursable expenses in cases where they support professional certifications, etc. that contribute to/complement the employee's job duties and related skill set at the Company.
   b. Staff Events: Certain staff events are reimbursable within the limitation of departmental budgets and based on management approval (e.g., department luncheons, employee exit luncheon, holiday luncheon, and overtime meals). These must be pre-approved and paid for by the most senior leader/department head to ensure the expense is appropriate and reimbursable.
   c. Home Office Equipment:
      i. Home office technology equipment requests should be submitted to the Service Desk and are not eligible for reimbursement (e.g., monitor, printer, etc.).
      ii. Business calls should be made using the Company's soft client telephone services (e.g. Microsoft Teams, Vonage, etc.).
      iii. Employees should contact expensereports@gannett.com to request the use of office furniture and supplies that are available and can be obtained from a company office.
      iv. Home office supply requests should be made through Coupa. Instructions found here.
      v. For any questions or requests about home office equipment, please contact your manager or expensereports@gannett.com.
   d. Home Internet:
      i. Employees who are assigned to work exclusively from their home office, and live in California, Illinois, Montana, North Dakota or South Dakota, may be eligible for a $10 per month home internet reimbursement. To ensure proper reimbursement, a copy of the home internet bill must be submitted in Concur. Employees should work with their manager and expensereports@gannett.com to determine eligibility.

4. Other Non-Reimbursable Expenses
   a. Only reasonable expenses directly related to Company business are reimbursable. The following is a brief list of expenses that are not reimbursable. This is not an all-inclusive list.
      i. Childcare & Pet care
      ii. Personal toiletries, hair salon expense, clothing, luggage, medicines, personal side trips, personal trip insurance, bed linens, pillows, earphones
      iii. Personal entertainment such as movies, mini bar, internet downloads
      iv. Fees connected with the use of recreational, health, and gym facilities
      v. Adult entertainment establishments e.g. Casinos, Strip Clubs

vi. ATM fees, personal credit card late fees, annual credit card fees or interest charges
vii. Passport, passport photos, driver's license fees (Visas required to support business travel and any special handling fees for passports will be reimbursed)
viii. U.S. Customs & Border Protection Traveler Programs (e.g. Global Entry, Nexus, Sentri, FAST, etc.)
ix. Travel incentive awards (frequent flyer miles, points, free flight coupons or travel vouchers) used to pay for business travel are not reimbursable to the employee
x. Employee convenience fees such as Early Boarding Fee or Airline Club fees
xi. No show charges for hotel or rental car, unless extenuating circumstances (i.e. health, death in family, etc.)
xii. Political or charitable contributions
xiii. Loss or theft of cash, travel tickets or credit cards
xiv. Loss, theft, or damage to personal property (e.g., luggage, auto, clothing)
xv. Personal legal charges
xvi. Accident-related costs when an employee uses his own personal auto for Company business unless otherwise authorized by applicable law
xvii. Invoices that could be paid through regular accounts payable process.
xviii. Expenses for technology software, online web services, and cloud computing providers are prohibited and NOT eligible for reimbursement to the employee. Only authorized individuals may expense approved technology software or services. Please use Approved Applications and Tools to request software or web services.
xix. Software and AI services are prohibited
xx. Gift cards for independent contractors. Extraordinary situations that may warrant out of policy gift card purchases will need approval from Division leadership and CFO.

Exhibit C
ReachLocal Supplemental Guidelines

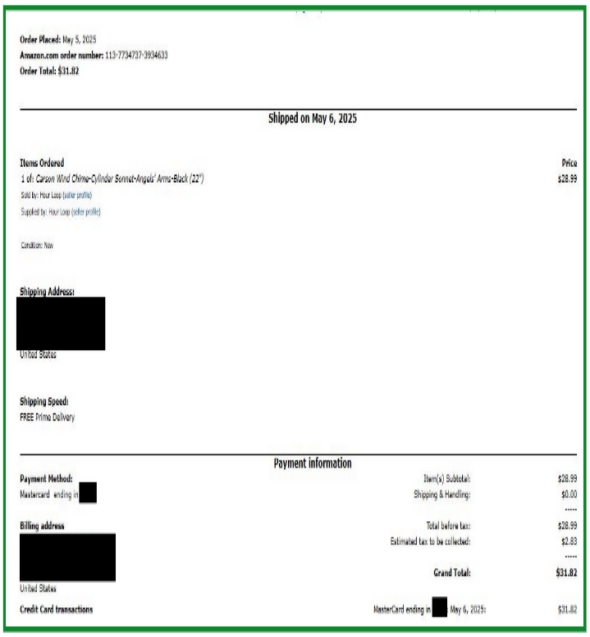
1. Canada
   a. To be reimbursed for a reasonable business expense, employees must submit receipts for all business expenses incurred using personal funds or credit cards.
   b. Employees should comply with this policy. For business kilometric reimbursement, employees are entitled to claim the allowable per kilometer reimbursement rate as specified by Canadian law.
      i. Kilometric reimbursement information can be found on the official website of the Government of Canada at CRA Kilometric Rates.

2. Australia
   a. Australia policy linked here.
   b. The employee is entitled to claim the allowable per kilometer reimbursement rate as specified by the applicable local procedure. https://www.ato.gov.au/Business/Income-and-deductions-for-business/Deductions/Deductions-for-motor-vehicle-expenses/Cents-per-kilometre-method/

Appendix A
Receipt Examples

ONLINE PURCHASES – All online purchases must be supported by a detailed receipt

Reimbursable Receipt



Order Placed: May 5, 2025
Amazon.com order number: 113-7734737-3934633
Order Total: $31.82

Shipped on May 6, 2025

Items Ordered — Price
1 of: Carson Wind Chime-Cylinder Sonnet-Angels' Arms-Black (22") — $28.99
Sold by: Hour Loop (seller profile)
Supplied by: Hour Loop (seller profile)
Condition: New

Shipping Address:
[redacted]
United States

Shipping Speed:
FREE Prime Delivery

Payment information

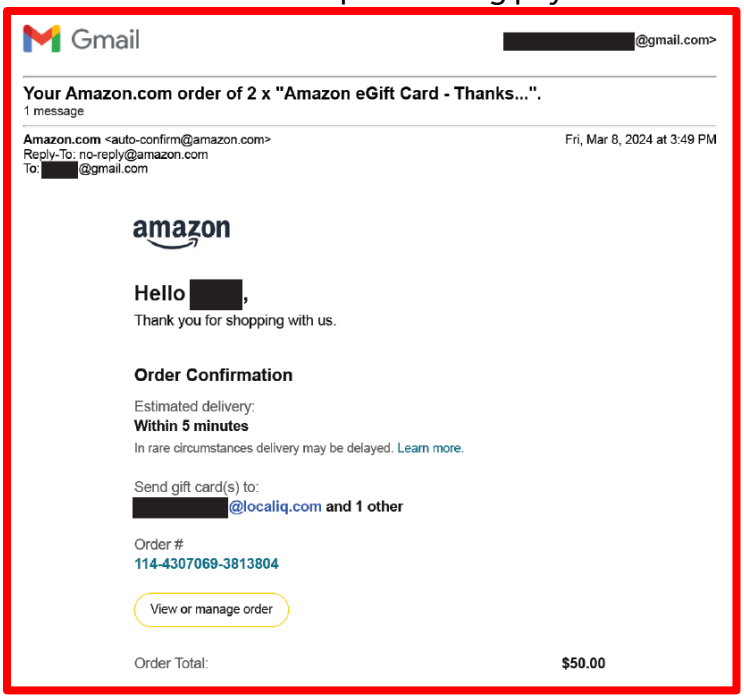
Payment Method:
Mastercard ending in [redacted]

Billing address
[redacted]
United States

Credit Card transactions

Item(s) Subtotal: $28.99
Shipping & Handling: $0.00
Total before tax: $28.99
Estimated tax to be collected: $2.83
Grand Total: $31.82
MasterCard ending in [redacted] May 6, 2025: $31.82

Non-reimbursable Receipt – Missing payment information.



Gmail [redacted]@gmail.com>

Your Amazon.com order of 2 x "Amazon eGift Card - Thanks...".
1 message

Amazon.com <auto-confirm@amazon.com> Fri, Mar 8, 2024 at 3:49 PM
Reply-To: no-reply@amazon.com
To: [redacted]@gmail.com

amazon

Hello [redacted],
Thank you for shopping with us.

Order Confirmation

Estimated delivery:
Within 5 minutes
In rare circumstances delivery may be delayed. Learn more.

Send gift card(s) to:
[redacted]@localiq.com **and 1 other**

Order #
114-4307069-3813804

View or manage order

Order Total: **$50.00**

RAIL EXPENSES

Reimbursable Receipt

SALES RECEIPT

Purchased: 02/28/2024 10:35 AM PTThank you for your purchase.

1. Retain this receipt for your records.
2. Show the QR code on the attached eTicket to the conductor or use the Amtrak app.

Merchant ID 009461 Massachusetts Ave NWWashington, DC 2C001800-USA-RAILAmtrak.com

Reservation Number - [redacted]Washington, DC - Union Station to New York, NY - Moynihan Train Hall at Penn Sta. (Round-Trip)FEBRUARY 28, 2024

Billing Information

Mastercard ending in [redacted] (Purchase)Authorization Code [redacted] **Total $2**

Purchase Summary - Ticket Number 0590946561461

TRAIN 2166: Washington, DC - Union Station to New York, NY - Moynihan Train Hall at Penn Sta. (Round-Trip) Depart 1:00 PM, Tuesday, March 12, 2024
1 ACELA BUSINESS CLASS SEAT **$71.99**

Car 5 - Seat 6D

Ticket Terms & ConditionsVLD DATE/TRAIN TICKETED. NO SHOW: FORFEIT VALUE.ACELA BUSINESS/FIRST: CHANGES CANCELS PERMITTED, NO FEE.ADULT FULL FARE ID REQUIRED **Subtotal $71.99**

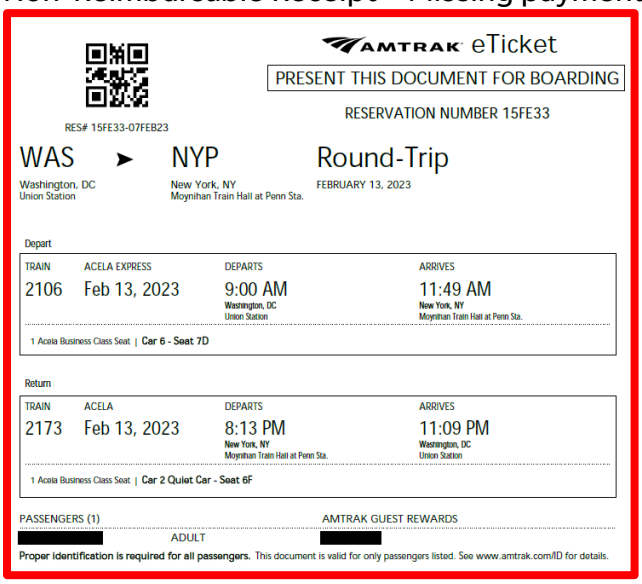
TRAIN 2163: New York, NY - Moynihan Train Hall at Penn Sta. to Washington, DC - Union Station (Round-Trip) Depart 3:00 PM, Thursday, March 14, 2024
1 ACELA BUSINESS CLASS SEAT **$138.60**

Car 6 - Seat 10D

Ticket Terms & ConditionsVLD DATE/TRAIN TICKETED. NO SHOW: FORFEIT VALUE.ACELA BUSINESS/FIRST: CHANGES CANCELS PERMITTED, NO FEE.ADULT FULL FARE ID REQUIRED **Subtotal $138.60**

Total Charged by Amtrak $210.59

Non-Reimbursable Receipt – Missing payment information



AMTRAK eTicket

PRESENT THIS DOCUMENT FOR BOARDING

RESERVATION NUMBER 15FE33

RES# 15FE33-07FEB23

WAS ➤ NYP Round-Trip

Washington, DC Union Station — New York, NY Moynihan Train Hall at Penn Sta. — FEBRUARY 13, 2023

Depart

TRAIN	ACELA EXPRESS	DEPARTS	ARRIVES
2106	Feb 13, 2023	9:00 AM Washington, DC Union Station	11:49 AM New York, NY Moynihan Train Hall at Penn Sta.

1 Acela Business Class Seat | Car 6 - Seat 7D

Return

TRAIN	ACELA	DEPARTS	ARRIVES
2173	Feb 13, 2023	8:13 PM New York, NY Moynihan Train Hall at Penn Sta.	11:09 PM Washington, DC Union Station

1 Acela Business Class Seat | Car 2 Quiet Car - Seat 6F

PASSENGERS (1) AMTRAK GUEST REWARDS

[redacted] ADULT [redacted]

Proper identification is required for all passengers. This document is valid for only passengers listed. See www.amtrak.com/ID for details.

RESTAURANT EXPENSES

Itemized receipt and payment receipt should both be included if not combined on one copy.

Reimbursable Receipts

Dos Amigos Restaurant
New York, NY

SALE

12-12-2014 10:32 AM

Batch #:04A2A
APPR CODE:3A6CE
Trace: 9
VISA ****[redacted]

1 Tacos Del Mal Shrimp	14.98
1 Especial Salad Chicken	12.50
1 Fountain Beverage	1.99
Sub-total:	29.47
Sales Tax:	2.50
Total:	31.97

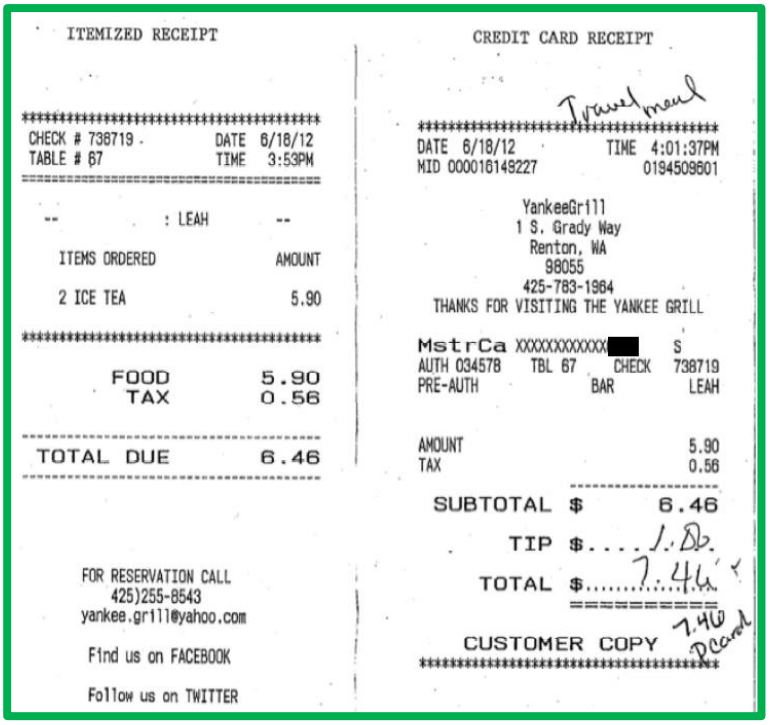
TIP: _____

TOTAL: _____

APPROVED

THANK YOU

CUSTOMER COPY



ITEMIZED RECEIPT

CHECK # 738719 DATE 6/18/12
TABLE # 67 TIME 3:53PM

-- : LEAH --

ITEMS ORDERED	AMOUNT
2 ICE TEA	5.90
FOOD	5.90
TAX	0.56
TOTAL DUE	6.46

FOR RESERVATION CALL
425)255-8543
yankee.grill@yahoo.com

Find us on FACEBOOK

Follow us on TWITTER

CREDIT CARD RECEIPT

Travel meal

DATE 6/18/12 TIME 4:01:37PM
MID 000016148227 0194509601

YankeeGrill
1 S. Grady Way
Renton, WA
98055
425-783-1964
THANKS FOR VISITING THE YANKEE GRILL

MstrCa XXXXXXXXXXXX[redacted] S
AUTH 034578 TBL 67 CHECK 738719
PRE-AUTH BAR LEAH

AMOUNT	5.90
TAX	0.56
SUBTOTAL $	6.46
TIP $	1.00
TOTAL $	7.46

CUSTOMER COPY 7.46 Pcard

Non-Reimbursable Receipt – Missing either itemization or payment information.

Harvest Moon
12125 N Oracle Rd D5
Tucson, AZ 85739
TEL:520-825-5351
www.harvestmoontucson.com

CARD TYPE : MC
CARD HOLDER : [redacted]
CARD NUMBER : ********** [redacted]
EXPIRATION DATE : XXXX

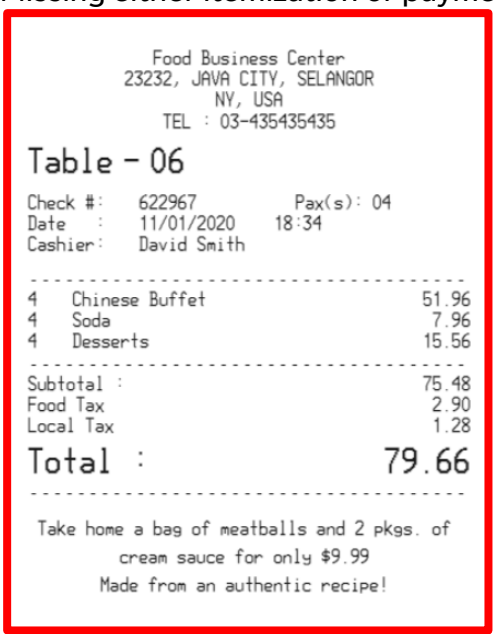
DATE : 2013-11-11 TIME : 1:57:34 PM

Invoice# : 00301111
Table# : B05
Server Name : CYNTHIA_LOPEZ

Charge Amt$: 19.46

TIP AMOUNT$_____

FINAL AMT$_____



Food Business Center
23232, JAVA CITY, SELANGOR
NY, USA
TEL : 03-435435435

Table - 06

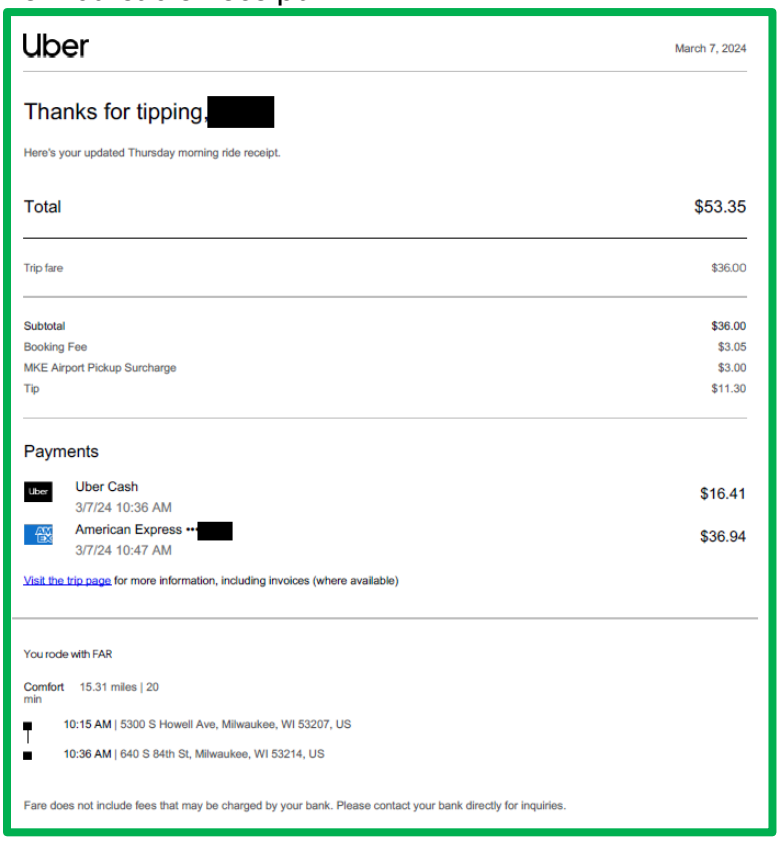
Check # : 622967 Pax(s) : 04
Date : 11/01/2020 18:34
Cashier : David Smith

4	Chinese Buffet	51.96
4	Soda	7.96
4	Desserts	15.56
Subtotal :		75.48
Food Tax		2.90
Local Tax		1.28
Total :		79.66

Take home a bag of meatballs and 2 pkgs. of cream sauce for only $9.99
Made from an authentic recipe!

RIDE SHARE SERVICES

Reimbursable Receipt



Uber

March 7, 2024

Thanks for tipping, [redacted]

Here's your updated Thursday morning ride receipt.

Total	$53.35
Trip fare	$36.00
Subtotal	$36.00
Booking Fee	$3.05
MKE Airport Pickup Surcharge	$3.00
Tip	$11.30

Payments

Uber Cash 3/7/24 10:36 AM	$16.41
American Express ••[redacted] 3/7/24 10:47 AM	$36.94

Visit the trip page for more information, including invoices (where available)

You rode with FAR

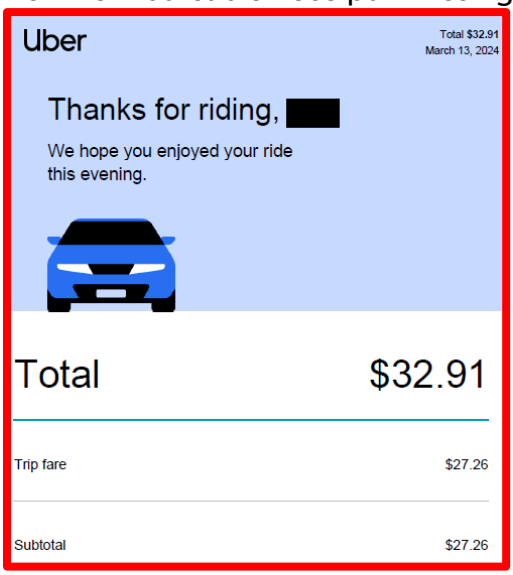
Comfort 15.31 miles | 20 min

10:15 AM | 5300 S Howell Ave, Milwaukee, WI 53207, US

10:36 AM | 640 S 84th St, Milwaukee, WI 53214, US

Fare does not include fees that may be charged by your bank. Please contact your bank directly for inquiries.

Non-Reimbursable Receipt – Missing payment information



Uber

Total $32.91
March 13, 2024

Thanks for riding, [redacted]

We hope you enjoyed your ride this evening.

Total	$32.91
Trip fare	$27.26
Subtotal	$27.26

OTHER

Non-Reimbursable Receipts – Credit Card Statements


Mar
13
CHICA LAS VEGAS
Dining
[redacted]
$84.67
LAS VEGAS, NV 89109 USA
Purchased: Mon, Mar 11, 2024
Posted: Wed, Mar 13, 2024
Purchased By: [redacted]
Appears on statement as: CHICA LAS VEGAS LAS VEGAS NV 89109 USA
Report a problem

Vulnerability Management Policy

Policy Owner: IT Security and Data Privacy
Version: 20250101
Employee Scope: All employees who work with all Gannett resources that can be affected by vulnerabilities, including but not limited to, servers, workstations, network devices, operating systems, software, and applications

Purpose

This policy outlines the processes for vulnerability scanning, vulnerability management workflow, risk classification and remediation processes to secure vulnerabilities in Gannett managed technology resources, both on-premises and cloud ("Gannett Resources").

Any exploit of vulnerabilities can expose Gannett to risks including malicious software attacks (viruses, worms, etc.), compromise of network and host computer systems and services, loss of data, reputational harm, and legal action.

Definitions and Acronyms

When navigating this policy, it's important to grasp the terminology. Our Glossary of Cybersecurity Terms provides concise definitions for key concepts.

Roles and Responsibilities

Gannett Cybersecurity Team

- Review new industry-reported cybersecurity vulnerabilities and their associated risk ratings at least monthly, using reputable outside sources.
- Determine prioritization by assigning a severity rating to identified vulnerabilities.

Gannett Resource Owner(s)

- Gannett Resource Owner(s) who are responsible for managing the systems, services, or applications covered by this policy must have vulnerability identification and remediation processes in place to address the vulnerability based on the vulnerability severity rating.

Policy

Vulnerability Identification

1. Using approved scanning tools and industry threat intelligence, the Gannett Cybersecurity Team must conduct regular scans of Gannett resources to identify new and existing vulnerabilities.
2. Scanning must be conducted on at least a monthly basis, or when a significant change occurs.
3. Any vulnerability identified as a result of the scans must be provided to Gannett Resource Owners.

Vulnerability Prioritization

1. When a vulnerability is found affecting a Gannett Resource, the Gannett Cybersecurity team must provide prioritization by classifying the vulnerability with a severity rating of critical, high, medium, or low.
2. The process for how a vulnerability is classified must be documented and approved.

Vulnerability Remediation

1. Vulnerability remediation must be in accordance with the Gannett Vulnerability Management Standard.
2. Gannett Resource Owners must have an established process for remediating identified vulnerabilities. This process must include verification that the vulnerability has been resolved via a re-scan after remediation.
   a. Vulnerabilities that cannot be remediated due to business reasons must be submitted through the vulnerability remediation exception process - Information Security Policies and Standards Exceptions Policy.
3. Operating systems must be configured to automatically update.
4. Applications must be configured to automatically update.

PCI Compliance

This section of the policy is applicable only to PCI in-scope environments and applications.

External Scanning

1. External facing Gannett Resources must be scanned at least a quarterly or when a significant change occurs, by qualified personnel using a PCI Approved Scanning Vendor as determined by Gannett's Information Security organization.
   a. All vulnerabilities must be corrected quarterly or approved as an exception by the PCI Approved Scanning Vendor.

Penetration Testing

1. Penetration tests must be performed annually or after a significant internal infrastructure or application upgrade or modification.
2. High severity findings must be remediated within 30 days, and a remediation verification must be performed.

Enforcement and Exception

- Compliance with this policy is required under Gannett's Information Security Policies and Standards Enforcement Policy and Gannett may take actions in response to non-compliance as provided under the Enforcement Policy.
- Any exceptions to this policy must follow Gannett's Information Security Policies and Standards Exceptions Policy.

This policy may be updated occasionally by the Company. The current version of this policy, as well as policies referenced in this document, may be viewed on MyLife@Gannett.

Whistleblower Procedure of Gannett Co., Inc.

Policy Owner: Corporate Governance
Version: 20210301
Employee Scope: All employees

A. Responsibilities of the Audit Committee With Respect to Specified Complaints

1. The Audit Committee (the "Audit Committee") of Gannett Co., Inc. (the "Company") adopted these Whistleblower Procedures to establish procedures for (i) the receipt, retention and treatment of complaints concerning accounting, financial reporting, internal accounting controls and auditing matters relating to the Company and (ii) the confidential anonymous submission of complaints by Concerned Persons (as defined below) of alleged questionable accounting or auditing matters. The Company's Audit Committee is responsible for overseeing the receipt, retention and treatment of all such complaints. The Company is committed to complying with all applicable securities laws and regulations and accounting standards and practices applicable to accounting or auditing matters.

2. The Audit Committee has adopted these Whistleblower Procedures in order to:
   a. Facilitate the disclosure of any questionable accounting or auditing matters before they can disrupt the business or operations of the Company or result in injury to stockholders;
   b. Promote a climate of individual accountability among the employees, officers, directors and stockholders of the Company (collectively, the "Concerned Persons") who perform various functions for the Company with respect to the Company's accounting, financial reporting, internal accounting controls and auditing matters; and
   c. Ensure that Concerned Persons feel secure in making, and have open and effective channels through which to make, reports to the Audit Committee concerning any questionable accounting matters, auditing matters or related legal or regulatory matters.

   Nothing in these Whistleblower Procedures or in any agreement between any employee and the Company shall in any way (i) restrict or prohibit any employee from lawfully making reports to, or communicating with, any government agency or law enforcement entity regarding possible violations of federal law or regulation in accordance with the provisions and rules promulgated under Section 21F of the Securities and Exchange Act of 1934, as amended, or Section 806 of the Sarbanes-Oxley Act of 2002, or of any other express whistleblower protection provisions of state or federal law or regulation, or (ii) require notification or prior approval by the Company of any reporting described in clause (i) hereof.

3. The Audit Committee shall receive, retain, investigate and act on reports, complaints and concerns of Concerned Persons ("Reports") in accordance with these Whistleblower Procedures regarding:

a. questionable accounting, internal accounting controls and auditing matters (an "Accounting Allegation");
   i. The phrase questionable accounting, internal accounting controls and auditing matters includes, but is not necessarily limited to, suspected or known acts of:
      a) fraud or deliberate error in the preparation, evaluation, review or audit of any financial statement of the Company;
      b) fraud or deliberate error in the recording and maintenance of financial records of the Company;
      c) deficiencies in, noncompliance with or the circumvention or attempted circumvention of the Company's internal accounting controls;
      d) misrepresentation or false statement to or by a senior officer or accountant of the Company regarding any matters contained in the financial records or any financial reports or audit reports of the Company;
      e) misappropriation of Company funds; or
      f) deviation from full and fair reporting of the Company's results of operations, cash flows and financial condition.
b. retaliation against employees who make Accounting Allegations (a "Retaliatory Act").

4. In the discretion of the Audit Committee, responsibilities of the Audit Committee created by these procedures may be delegated to the Chair of the Audit Committee or to a subcommittee of the Audit Committee.

B. Confidentiality of Concerned Persons Making Reports

1. Reports may be made anonymously (outside of the United States, only to the extent permitted by local law), however, if Concerned Persons provide their contact information, it may facilitate investigation and follow-up.

2. If the identity of any Concerned Persons making a Report ("Reporting Person") is known, unless such Reporting Person has authorized the Company to disclose his or her identity, the Company will exercise reasonable care to keep the identity of such person confidential unless: (i) such confidentiality is incompatible with a fair investigation of the complaint; (ii) there is an overriding reason for identifying or otherwise disclosing the identity of such person; or (iii) such disclosure is required by applicable law or regulation.

3. Furthermore, the identity of any such Reporting Person may be disclosed if it is reasonably determined that such person made a complaint maliciously or recklessly, or if disciplinary proceedings are invoked against such person in connection with the malicious or reckless complaint. In all cases, the Audit Committee, the Company's General Counsel (the "General Counsel"), the Director of Internal Audit, and the Chief Financial Officer will have access to all information contained in the complaint, unless otherwise determined by the Chair of the Audit Committee.

C. Procedures for Receiving Reports

1. Any Report that is made directly to management, whether openly, confidentially or anonymously, shall be promptly reviewed by a team composed of the General Counsel and at least one member of the Company's Disclosure Committee (the "Review Team"). Reports that are not related to Accounting Allegations will be sent to the Legal Department or Human Resources Department, as appropriate.
2. Unless the investigation shall be conducted by the Audit Committee, as described below, the Review Team shall designate persons to conduct a reasonable investigation of all Accounting Allegations and Retaliatory Acts that are reported with sufficient information (the "Investigation Team").
3. Unless clearly erroneous, the Review Team shall promptly send the following types of Accounting Allegations or Retaliatory Acts (the "Critical Allegations") to the Chair of the Audit Committee:

    a. Any allegation of intentional violation of the federal securities laws or regulations or allegation of other fraud associated with accounting, auditing or internal controls;

    b. Any allegation of a significant deficiency or material weakness (as defined by the Public Company Accounting Oversight Board) in the design or operation of the Company's internal controls;

    c. Any allegation raising material issues with respect to the accuracy or completeness of the Company's financial statements or records;

    d. Any allegation of misconduct involving an executive officer of the Company or an employee who has a significant role in internal control over financial reporting; and

    e. Any other compliance allegation that, in the judgment of the Review Team, poses substantial financial or reputational risk to the Company.

    The Chair of the Audit Committee or the Audit Committee may determine that the Audit Committee should investigate any Critical Allegation, and will provide notice to the Review Team if such determination is made, if necessary.

4. Any Report that is made directly to the Audit Committee, the Chair of the Audit Committee or the Board directly shall be forwarded by the Chair of the Audit Committee to the Review Team, unless the Chair of the Audit Committee or the Audit Committee determines that the Audit Committee will conduct the investigation. The Review Team may direct any such Reports that are not Accounting Allegations to the Legal Department or Human Resources Department, as appropriate.

5. If the Review Team conducts an investigation, the Review Team may retain employees, third-party consultants or advisors, as appropriate, to conduct or

support the investigation. The Investigation Team shall periodically report to the Review Team regarding the status of any investigation. The Company shall provide the Investigation Team with funding adequate to take all steps reasonably necessary for the investigation.

6. If the Audit Committee determines to conduct an investigation, the Audit Committee shall promptly determine what professional assistance, if any, it needs in order to conduct the investigation. The Audit Committee shall be free in its discretion to engage the Review Team, outside third-party consultants or advisors, as appropriate to assist in the investigation and in the analysis of results. Any Investigation Team engaged by the Review Team pursuant to this subsection shall periodically report to the Review Team regarding the status of any investigation, and the Review Team shall report the results of the investigation as promptly as practicable to the Audit Committee. The Company shall provide the Review Team or the Investigation Team with funding adequate to take all steps reasonably necessary for the investigation.
7. At each regularly scheduled Audit Committee meeting, the General Counsel and/or Director of Internal Audit, or his or her respective designee, shall report on all Accounting Allegations and Retaliatory Acts received since the previous meeting and describe the status of any investigations undertaken. Such reports shall include the date, a description of the Accounting Allegation or Retaliatory Acts, the steps taken in the investigation and its status, and, if available, management's response. Regular reports shall continue at each subsequent Audit Committee meeting until the final resolution of a matter.

D. Considerations Relative to Whether the Audit Committee or Management Should Investigate a Report

In determining whether the Audit Committee should investigate a Report or a Critical Allegation, the Audit Committee shall consider, among any other factors that are appropriate under the circumstances, the following:

1. Who is the alleged wrongdoer? If an executive officer, senior financial officer, such as a chief financial officer or chief accounting officer, or other high management official is alleged to have engaged in wrongdoing, that factor alone may weigh in favor of the Audit Committee conducting the investigation.
2. How serious is the alleged wrongdoing? The more serious the alleged wrongdoing, the more appropriate that the Audit Committee should undertake the investigation. If the alleged wrongdoing would constitute a crime involving the integrity of the financial statements of the Company, that factor alone may weigh in favor of the Audit Committee conducting the investigation.
3. Would there be significant reputational risk? The more likely it is that there could be reputational risk based on the allegation, the more appropriate that the Audit Committee should undertake the investigation. In assessing reputational risk, the Audit Committee should consider all facts surrounding the allegation, including but not limited to whether similar allegations have been made in the press or by analysts.

4. Will delegation to management reveal the identity of the person who made the Report? If the person who made the Report requested that his or her identity be kept confidential, the Audit Committee must consider whether passing on the Report to management would enable management to identify the person who made the Report.

E. Protection of Whistleblowers

Consistent with the policies of the Company, the Audit Committee shall not retaliate, and shall not tolerate any retaliation by management or any other person or group, directly or indirectly, against anyone who, in good faith, makes an Accounting Allegation, reports a Retaliatory Act or provides assistance to the Audit Committee, management or any other person or group, including any governmental, regulatory or law enforcement body, investigating a Report. The Audit Committee shall not, unless compelled by judicial or other legal process, reveal the identity of any person who makes an Accounting Allegation or reports a Retaliatory Act and who asks that his or her identity as the person who made such Report remain confidential and shall not make any effort, or tolerate any effort made by any other person or group, to ascertain the identity of any person who makes a Report anonymously.

F. Records

Subject to compliance with applicable data protection laws, the Audit Committee shall retain all records relating to any Accounting Allegation or report of a Retaliatory Act and to the investigation of any such Report in accordance with applicable document retention laws.

G. Procedures for Making Complaints

In addition to any other avenue available to a Concerned Person, any Reporting Person may report openly, confidentially or anonymously any Accounting Allegation or report of a Retaliatory Act orally or in writing to management by contacting Polly Grunfeld Sack, General Counsel, at 175 Sully's Trail, 3rd Floor, Pittsford, New York 14534 or by calling the Ethics Hotline at 1-866-553-4734 at any time. Reports may also be made on an anonymous basis via a website established for this purpose (http://www.whistleblowerservices.com/gannett/). The toll-free line and website are managed by an outside, independent service provider and allows anyone to make a Report without divulging his or her name. The hotline service provider is required to share the information provided in the Report to management or, if requested by the individual making the Report, the Audit Committee as promptly as practicable.

Workstations & Mobile Devices Policy

Policy Owner: IT Security and Data Privacy
Version: 20250101
Employee Scope: All US employees who work with all workstations and mobile devices that have access to Gannett networks or store any Gannett information or are used as a single sign-on second factor

Purpose

- This policy covers all end user computing devices running the Windows or macOS operating systems.
  These devices will be known as "workstations" for the purpose of this document.
- This policy also covers end user computing device running the iOS, Android, or Chrome OS operating systems. These devices will be known as "mobile devices" for the purpose of this document.
- The policy outlines additional security measures to protect easily transportable devices (e.g., laptops, smartphones, tablets, etc.) from loss or unauthorized access.

Definitions and Acronyms

When navigating this policy, it's important to grasp the terminology. Our Glossary of Cybersecurity Terms provides concise definitions for key concepts.

Policy

General – Workstations

- Non-company-owned workstations are prohibited from accessing the Gannett network.
- Workstations must adhere to the Password Security Policy. Operating systems that cannot provide secure password authentication to the Gannett computing domain should not be used.
- Workstations must have the latest security patches and updates applied as required to address vulnerabilities, as set forth in the Vulnerability Management Policy.
- Workstations must be protected with a current endpoint protection product, as set forth in the Endpoint Protection Policy.
- Workstations must be protected with firewall software. Firewall software may be integrated into the operating system or a third-party product but must be current and updated with the latest patches.
- Data on workstations must be encrypted in adherence to the Data Protection Policy and the Acceptable Encryption Policy.

General – Mobile Devices

- While mobile devices may access sections of the wireless Gannett network, mobile devices may NOT access any section of the network included in the PCI (Payment Card Industry) scope.
- Mobile devices will have the following standards established by the SRC (Security Review Council) and Technology Lifecycle Team.
  - Pin, password, or biometric protected screen lock

- Disallow “rooted” devices
- Ability to wipe company data

User Responsibilities for Easily Transportable Devices (users must take additional steps to secure easily transportable workstations and mobile devices)

- Restrict viewing of sensitive information in public places.
- Secure devices while in-transit. Laptops and mobile devices should never be checked with luggage when traveling; they should instead be included as a carry-on bag in the passenger compartment.
- If a laptop, mobile device, or other devices that can store and process or help grant access to Gannett data is lost or stolen, you must immediately contact the Gannett Help Desk so that the lost or stolen device procedures may be implemented.
- To re-enable the user account(s), the Account Policy must be followed.

Network Connections

- Corporate Virtual Private Network (VPN) access. See the appropriate section of the Remote Access Security Standard.
- Wireless networking access. See the appropriate section of the Remote Access Security Standard.
- Laptops and mobile devices accessing company e-mail via Outlook Web Access (OWA). See the appropriate section of the Remote Access Security Policy.

Physical Security

- See the Information Technology Physical Security Policy.

Enforcement and Exception

- Compliance with this policy is required under Gannett's Information Security Policies and Standards Enforcement Policy and Gannett may take actions in response to non-compliance as provided under the Enforcement Policy.
- Any exceptions to this policy must follow Gannett’s Information Security Policies and Standards Exceptions Policy.

This policy may be updated occasionally by the Company. The current version of this policy, as well as policies referenced in this document, may be viewed on MyLife@Gannett.