GSA Order: GSA IT General Rules of Behavior
CIO 2104.1C
Office of the Chief Information Officer
ispcompliance@gsa.gov

Purpose:

This Order sets forth the General Services Administration's (GSA's) Information Technology (IT) General Rules of Behavior and lists the responsibilities and expected behavior of users of GSA's IT resources and applications to safeguard GSA's assets and data.

Background:

Office of Management and Budget (OMB) Circular A-130, "Managing Information as a Strategic Resource" requires Federal agencies to establish rules of behavior for employees and contractors that have access to Federal information, including Personally Identifiable Information (PII) and Controlled Unclassified Information (CUI), and information systems. This Order addresses these requirements. The IT General Rules of Behavior implement the Federal policies and GSA directives provided in the References section of this Order.

Applicability:

This Order applies to:

1. All GSA employees and contractors using GSA IT resources and applications as they perform their duties;
2. Third parties with a gsa.gov account who access GSA IT resources to conduct business on behalf of, or with, GSA or GSA-supported Government organizations;
3. The Office of Inspector General (OIG) only to the extent that the OIG determines it is consistent with the OIG's independent authority under Public Law 110-409, "Inspector General Reform Act of 2008," and it does not conflict with other OIG policies or the OIG mission; and
4. The Civilian Board of Contract Appeals (CBCA) only to the extent that the CBCA determines it is consistent with the CBCA's independent authority under Public Law 95-563, "Contract Disputes Act of 1978," and it does not conflict with other CBCA policies or the CBCA mission.

Cancellation:

This Order cancels and supersedes CIO 2104.1B CHGE 2, GSA Information

Technology (IT) General Rules of Behavior, dated April 1, 2022.

Summary of Changes:

1. Updated document to conform with OAS 1832.1C.
2. Added rules regarding Artificial Intelligence.
3. Edited and updated all rules to reflect current user behavior requirements.

Roles and Responsibilities:

GSA Supervisors - Must ensure compliance with this order for their employees who access GSA IT resources and applications.

Contracting Officers - Must insert a clause into the contract or task order, ensuring compliance of contractor employees with this order in accordance with the General Services Acquisition Manual (GSAM) part 511.171.

Employees/Contractors - Must acknowledge these IT General Rules of Behavior within 30 calendar days of their first use of a GSA IT resource and annually thereafter.

Signature:

/S/_____ 11/5/2024_____

DAVID SHIVE
Chief Information Officer
Office of GSA IT

Date

1. IT General Rules of Behavior

Category	Rules of Behavior
Artificial Intelligence (AI)	(1) **Usage Authorization**: Do not use generative AI unless explicitly authorized, as per CIO 2185.1A, "Use of Artificial Intelligence at GSA." (2) **Data Guidelines**: Only use generalized, non-sensitive data with online providers of generative AI (e.g., ChatGPT, Google Gemini).
Personal Use	(1) **Minimization**: Limit personal use of IT resources (e.g., mobile devices, laptops, printers, copiers). (2) **Work Priority**: Ensure personal use does not interfere with or prevent the fulfillment of official duties. (3) **Prohibited Activities**: Do not use IT resources for private gain, commercial purposes (including endorsements), or profit-making activities.
Privacy	(1) **Monitoring**: All activities are subject to monitoring; there is no expectation of privacy. (2) **Data Protection**: Use encryption, access controls, data extracts, and physical security measures to protect Personally Identifiable Information (PII) and other Controlled Unclassified Information (CUI) as outlined in GSA orders CIO 2180.2, "GSA Records Management Program," and CIO 2103.2, "Controlled Unclassified Information (CUI) Policy."

Category	Rules of Behavior
Access	(1) **Password Safety**: Keep your passwords secure; do not share them. (2) **Workstation Security**: Lock your GSA laptop (e.g., CTRL-ALT-DELETE) and remove your authentication tokens (e.g., PIV card) when leaving your shared workspace. (3) **Regular Restarts**: Restart your GSA workstation weekly, or sooner if requested by GSA Help Desk to help protect against malicious apps, phishing, and other attacks. (4) **Re-authentication**: GSA users authenticate to the GSA network via single sign-on daily in the performance of GSA work. At a minimum, re-authenticate using your Enterprise account every 30 days or sooner if requested by the GSA Help Desk or Security. (5) **Logoff**: Logoff your GSA workstation at the end of the workday.
Remote Access	**Approved Methods**: Use approved methods to remotely access the GSA network.
Hardware and Software	(1) **Licensing**: Abide by software copyright laws; do not obtain, install, replicate, or use unlicensed software. (2) **Obtaining Software**: Obtain all software through the IT Service Desk unless otherwise directed. Do not download untrusted software from the Internet. (3) **Prohibited Tools**: Do not acquire, possess, or use hardware or software tools that defeat software copy protection, discover passwords, identify security vulnerabilities, or decrypt encrypted files. (4) **Patching and Rebooting**: Promptly respond to patching and reboot requests from GSA IT officials. (5) **Resource Protection**: Protect GSA IT resources in your possession from theft, destruction, or misuse.

Category	Rules of Behavior
Government Furnished Equipment	(1) **International Travel**: Request and use a GSA Loaner Laptop when working internationally. (2) **Mobile Applications**: Do not use mobile applications that request GSA network credentials unless pre-approved by IT Security (reference GEAR's IT Standards List). (3) **Prevent Theft**: Carry or store your GSA-issued device(s) in a manner that prevents theft. (4) **Secure Usage**: Turn off unused communications capabilities (e.g., Cellular, Bluetooth, WiFi) when not in use or when traveling.
Use Your Own Device	When a personally-owned device is approved for conducting official business, the following rules apply: (1) **Connection Restrictions**: Personal devices may only connect to GSA systems with explicit authorization. (2) **Sensitive Data**: Do not download sensitive information (e.g., PII, CUI) to personal IT devices. (3) **Updates**: Apply software updates promptly.

Category	Rules of Behavior
Prohibited Usage	(1) **Classified Information**: Never convey classified information over the GSA network. (2) **Inappropriate Content**: Never convey any material that is sexually explicit, offensive, abusive, discriminatory, or objectionable. Do not browse sexually explicit or hate-based websites. (3) **Large Attachments and Chain Letters**: Never transmit non-business-related large attachments, chain letters, unauthorized mass mailings, or malware. (4) **Copyright Compliance**: Never use copyrighted or otherwise legally protected material without permission. (5) **Privacy and Security**: Never use GSA IT resources to "snoop" on or invade another person's privacy or break into any computer, whether belonging to GSA or another organization. (6) **Defamatory Material**: Never transmit any material that is libelous or defamatory. (7) **Hatch Act/Ethics**: Adhere to the requirements in the Hatch Act and the Standards of Ethical Conduct for Employees of the Executive Branch.
Use of External Sites	**Unique Identifiers**: Do not reuse GSA identifiers (e.g., email addresses, usernames) or authentication information (e.g., passwords, token codes, PINs) to create accounts on external sites or applications.
Security Training	**Mandatory Training:** Complete the mandatory GSA IT Security and Privacy Awareness Training each year.
Recordkeeping	**Recordkeeping Compliance**: Follow GSA order CIO 1820.2A, "GSA Records Management Program," which provides guidance on implementing recordkeeping requirements.

Category	Rules of Behavior
Social Media	(1) **Approval and Compliance**: Any GSA social media account must be approved by the Office of Strategic Communication (OSC) and must comply with the requirements in GSA Order OSC 2106.2A, GSA Social Media Policy. Noncompliant GSA social media accounts will be frozen or terminated. (2) **Personal Account Guidelines**: Personal social media accounts must also adhere to GSA's Social Media Policy. This includes but is not limited to: ● Not disseminating non-public information. ● Not using official GSA branding. ● Adhering to the Hatch Act and the Standards of Ethical Conduct for Employees of the Executive Branch. (3) **Personal Views Disclaimer**: GSA employees are encouraged to use a disclaimer stating that their social media communications reflect only their personal views and do not necessarily represent the views of GSA or the United States.

Category	Rules of Behavior
Email	Use guidance found in GSA Order CIO 2160.2B CHGE 4, GSA Electronic Messaging and Related Services: (1) **Official Business**: Use @gsa.gov email accounts for official business. Occasional personal use is authorized. (2) **Non-Agency Email**: When using non-agency email addresses for agency business, ensure the email is copied or forwarded to an agency account within 20 business days, as required by the Federal Records Act (44 U.S.C. 2911 as amended by Pub. L. 113-187). (3) **Automatic Forwarding Prohibited:** You must not automatically forward emails from your government account to any other account unless IT Security gives prior authorization. Manual forwarding is permitted. Reach out to the GSA Help Desk to request IT Security's approval. (4) **Emailing Sensitive Information**: Use GSA-mandated encryption procedures when transmitting sensitive information (e.g., CUI, PII) to non-GSA email addresses.
Reporting	**Report Security Incidents**: Promptly report any suspected or confirmed security breaches or PII/CUI incidents to the IT Service Desk.
Contact the IT Service Desk	Connect with the Help Desk via email, phone, or the Self-Service Portal. Number: 1-866-450-5250 Email: ITServiceDesk@gsa.gov URL: Self Service Portal

2. Deviations

Any deviations from this policy must be approved by GSA's Chief Information Security Officer (CISO).

3. Penalties for Non-Compliance

Users who do not comply with the IT General Rules of Behavior may incur disciplinary action.

4. References

a. Federal Records Act of 1950, as amended
b. Public Law 95-563, The Hatch Act
c. Public Law 110-409, Inspector General Reform Act of 2008 (5 U.S.C. §§ 401-424)
d. Public Law 113-283, Federal Information Security Modernization Act of 2014
e. OMB Circular A-130, Appendix I, Security of Federal Automated Information Resources.
f. Standards of Ethical Conduct for Employees of the Executive Branch
g. General Services Acquisition Manual (GSAM) part 511.171
h. GSA Order CIO 1820.2A, GSA Records Management Program
i. GSA Order CIO 2100.1P, GSA Information Technology (IT) Security Policy
j. GSA Order CIO 2103.2, Controlled Unclassified Information (CUI) Policy
k. GSA Order OSC 2106.2A, GSA Social Media Policy
l. GSA Order CIO 2160.2B CHGE 4, GSA Electronic Messaging and Related Services
m. GSA Order CIO 2180.2, GSA Rules of Behavior for Handling Personally Identifiable Information (PII)
n. GSA Order CIO 2185.1A, Use of Artificial Intelligence at GSA