GENERAL SERVICES ADMINISTRATION
Washington, DC 20405

CIO 2104.1B CHGE 2
4/1/2022

GSA ORDER

SUBJECT: GSA Information Technology (IT) General Rules of Behavior

1. Purpose. This Order sets forth the General Services Administration's (GSA's) policy on IT General Rules of Behavior. The IT General Rules of Behavior implement the Federal policies and GSA directives provided in the "References" section of this Order.

2. Cancellation. This Order cancels and supersedes CIO 2104.1B CHGE 1, GSA Information Technology (IT) General Rules of Behavior, dated April 2, 2019.

3. Explanation of Changes.

a. Updated links and clarified terminology throughout.

b. Renumbered document to list references last.

c. Updated information in section 8 on Access, Hardware and Software, and Remote Access; and

d. Added new information to section 8 on Recordkeeping and the Use of External Sites and Social Media.

4. Objective. To communicate to users of GSA's IT resources and applications their responsibilities and expected behavior in safeguarding those assets. This pertains to government furnished equipment (GFE) and resources unless otherwise specified in Section 8 of this order.

5. Applicability.

a. This Order applies to all GSA employees and contractors using GSA IT resources and applications. This Order also applies to third parties who access GSA IT resources to conduct business on behalf of, or with, GSA or GSA-supported Government organizations.

b. This Order applies to the Office of Inspector General (OIG) only to the extent that the OIG determines it is consistent with the OIG's independent authority under the IG Act, and

it does not conflict with other OIG policies or the OIG mission.

c. This Order applies to 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 the Contract Disputes Act, and it does not conflict with other CBCA policies or the CBCA mission.

6. Roles and Responsibilities.

a. GSA supervisors must ensure their employees who access GSA IT resources and applications comply with this Order.

b. In accordance with the General Services Acquisition Regulation (GSAR) part 511.171, Contracting Officers must include compliance with this policy in the contract or task order for contractor employees.

c. GSA employees and 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.

7. Penalties for Non-Compliance. Users who do not comply with the IT General Rules of Behavior may incur disciplinary action.

8. IT General Rules of Behavior.

Category	**Rules of Behavior**
Personal Use	(1) Minimize the personal use of GSA IT resources. (2) Do not allow your personal use of GSA IT resources to interfere or prevent fulfillment of your official duties. (3) Only access GSA IT systems or information in performance of your official duties. (4) Do not use IT resources for private gain, commercial purposes (including endorsement of products), or profit-making activities.
Privacy	(1) Assume no expectations of privacy when using GSA IT resources as all activities are subject to monitoring.

	(2) Protect Personally Identifiable Information (PII) and other Controlled Unclassified Information (CUI), as described in GSA Orders CIO 2180.2 and CIO 2103.2, to include use of encryption, access controls, data extracts, and physical security.
Bring Your Own Device	These rules *only apply to personal devices* being used to conduct official business: (1) Do not download sensitive information (e.g., PII, CUI) to personal IT resources (e.g., laptop, mobile device, home computer, removable media.) (2) Keep operating system patches and antivirus software running and updated. (3) Download applications only from trusted sources.
Access	(1) Keep your passwords safe; don't share them. (2) Lock (e.g., CTRL-ALT-DELETE) your GSA laptop and remove your personal identity verification (PIV) card when stepping away from your shared work area. (3) Logoff and shutdown your GSA workstation at the end of the workday.
Hardware and Software	(1) Abide by software copyright laws and do not obtain, install, replicate, or use unlicensed software. (2) Obtain all software through the IT Service Desk unless otherwise directed by them. Do not download untrusted software from the Internet. (3) 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) Promptly respond to patching and reboot requests from GSA IT officials. (5) Protect GSA IT resources in your possession from theft, destruction, or misuse.

Remote access	Use approved methods (e.g., Multi-Factor Authentication (MFA), Citrix (via anywhere.gsa.gov), or Virtual Private Network (VPN) to remotely access the GSA network.
Mobile Security	(1) Do not use mobile applications that request GSA network credentials unless pre-approved by IT Security. (2) Carry or store your GSA-issued mobile device(s) in a way that prevents theft. (3) When traveling, turn off your phone's unused radios (i.e., Bluetooth, WiFi, Cellular).
Prohibited Usage	(1) Never convey classified data or information over the GSA network. (2) Never convey any material that is sexually explicit, offensive, abusive, discriminatory, or objectionable. Never browse sexually explicit or hate-based websites. (3) Never transmit non-business-related large attachments, chain letters, unauthorized mass mailings, or malware. (4) Never use copyrighted or otherwise legally protected material without permission. (5) 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) Never transmit any material that is libelous or defamatory.

Social Media	(1) Any GSA social media account must be approved by Office of Strategic Communication (OSC) and must abide by the requirements contained in GSA Order OSC 2106.2, GSA Social Media Policy. Any GSA social media account discovered to be noncompliant with GSA policy, standards, or guidelines will be frozen or terminated. (2) Personal social media account usage also is also governed by GSA' Social Media Policy, including but not limited to not disseminating non-public information, not using official GSA branding, and adhering to the Hatch Act and the Standards of Ethical Conduct for Employees of the Executive Branch. (3) GSA employees are encouraged to use a disclaimer clarifying that their social media communications reflect only their personal views and do not necessarily represent the views of GSA or the United States.
Use of External Sites	(1) Do not re-use GSA identifiers (e.g., email addresses, usernames) or authentication secrets (e.g., passwords, token codes, PINs) for creating accounts on external sites/applications.
Email	(1) Use guidance found in GSA Order CIO 2160.2B CHGE 3, GSA Electronic Messaging and Related Services. (2) Use @gsa.gov email accounts for official business; occasional personal use is authorized. (3) When non-agency email addresses are used for agency business, the email must be copied/forwarded to an agency account within 20 business days per the Federal Records Act (44 U.S.C. 2911 as amended by Pub. L. 113-187). (4) Never automatically forward GSA email to a non-Federal email account. (5) Use GSA-mandated encryption procedures when transmitting sensitive information (e.g., CUI, PII) to non-GSA email addresses.
Security Training	Complete the required GSA IT Security and Awareness Training each year.

Reporting	Promptly report suspected or confirmed breaches of security or PII/CUI to the IT Service Desk (or contact via +1-866-450-5250 or email ITServiceDesk@gsa.gov.)
Recordkeeping	GSA's directive CIO 1820.2, GSA Records Management Program, provides direction on implementing recordkeeping requirements as both the development and the use of technology may create agency records.

9. Deviations. All deviation requests must be submitted to the appropriate Information Systems Security Officer (ISSO) or Authorizing Official (AO), who will coordinate as necessary with GSA's Chief Information Security Officer (CISO).

10. References.

a. Appendix III, Office of Management and Budget (OMB) Circular A-130 – Security of Federal Automated Information Resources

b. Federal Information Security Modernization Act (FISMA) of 2014 (Public Law 113-283)

c. GSA Order CIO 2103.2, Controlled Unclassified Information (CUI) Policy

d. GSA Order CIO 2100.1M, GSA Information Technology (IT) Security Policy

e. GSA Order CIO 2160.2B CHGE 3, GSA Electronic Messaging and Related Services

f. GSA Order ADM 7800.11A, Personal Use of Agency Office Equipment

g. GSA Order CIO 2180.2, GSA Rules of Behavior for Handling Personally Identifiable Information (PII)

h. GSA Order OSC 2106.2, GSA Social Media Policy

i. General Services Acquisition Regulation (GSAR) part 511.171

j. The Federal Records Act of 1950, as amended

k. The Hatch Act

l. Standards of Ethical Conduct for Employees of the Executive Branch

11. Signature.

DocuSigned by:
David Shive
A3AE4284A2754F9...

DAVID SHIVE
Chief Information Officer
Office of GSA IT