GENERAL SERVICES ADMINISTRATION
Washington, DC 20405

CIO 2104.1B CHGE 1
April 2, 2019

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, GSA Information Technology (IT) General Rules of Behavior, dated January 29, 2019.

3. Explanation of Change. A change was made to the chart at paragraph 9 to clarify that GSA email may be used for occasional personal use.

4. Objectives. The objective of this IT General Rules of Behavior is to communicate to users of GSA IT resources and applications their responsibilities and expected behavior in safeguarding those resources.

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. 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 2100.1K, GSA Information Technology (IT) Security Policy

d. GSA Order CIO 1878.1, GSA Privacy Act Program

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

f. GSA Order OSC 2106.2, GSA Social Media Policy

7. 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 Acquisition Letter MV-16-01, 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 Security Rules of Behavior within 30 days of their first use of a GSA IT resource, and complete GSA's IT Security and Privacy Training annually thereafter.

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

9. IT General Rules of Behavior.

Category	**Rules of Behavior**
Personal Use	(1) Minimize the personal use of GSA IT resources. (2) Ensure that personal usage of GSA IT resources does not interfere with official system use or access. (3) Do not use IT resources for private gain, commercial purposes (including endorsement of products), or profit-making activities.
Privacy	(1) Users have no expectation of privacy on GSA IT resources as all activities are subject to monitoring.

	(2) Protect Personally Identifiable Information (PII) and sensitive data, as described in GSA Order CIO P 2180.1, 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, Controlled Unclassified Information (CUI)) to personal IT resources (e.g. laptop, mobile device) (2) Keep operating system patches and antivirus software running and updated.
Protection	Protect GSA IT resources from theft, destruction, or misuse.
Access	(1) Always keep passwords secured and private. Do not share them. (2) Only access systems or information required for official duties. (3) "Lock" GSA laptops and remove the personal identity verification (PIV) card when stepping away from the work area (4) Logoff and shutdown GSA workstations at the end of the workday.
Encryption	Use GSA provided encryption when storing, processing, or transmitting sensitive information (e.g., PII, CUI).
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. (3) Do not download software from the Internet, as downloading software from the Internet may introduce malware to the GSA network. (4) Do not acquire, possess, or use hardware or software tools that defeat software copy protection, discover passwords, identify security vulnerabilities, or decrypt encrypted files.

Remote access	Only use approved methods (e.g., VPN, Citrix, Horizon) to remotely access the GSA network.
Mobile Devices and Mobile Applications	(1) Secure GSA-issued mobile devices at all times to prevent theft. (2) Download applications only from trusted sources. (3) Obtain prior approval from IT Security for mobile applications that require: a) The use of GSA network credentials to operate; or b) Applications that download, store, or transmit GSA data on mobile devices.
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 web sites. (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.
Email	(1) Use @gsa.gov email accounts for official business; occasional personal use is authorized. (2) Never automatically forward GSA email to a non-Federal email account.
Reporting	Promptly report suspected or confirmed breaches of security or PII/CUI to the IT Service Desk.

10. 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 the GSA Chief Information Security Officer (CISO).

11. Signature.

e-Signed by David Shive
on 2019-04-02

DAVID SHIVE
Chief Information Officer
Office of GSA IT