GENERAL SERVICES ADMINISTRATION
Washington, DC 20405

CIO P 2165.2 CHGE 1

4/24/2021

GSA ORDER

SUBJECT: GSA Telecommunications Policy

1. Purpose. This policy establishes the policy for General Services Administration (GSA) authorized users for utilization of GSA-provided telecommunications equipment, systems, and services (hereafter, GSA telecommunications). In concert with GSA's Guide to Official Use of Telecommunications posted on GSA's Intranet "InSite", this policy serves as the official employee reference regarding telecommunications in GSA.

2. Applicability.

a. This policy applies to all GSA employees, contractors/subcontractors as specified in Memorandum of Understanding (MOUs) or other agreement vehicles, government agencies, individuals, corporations, or other organizations that process or handle any GSA-owned information, data, or IT system equipment.

b. Contracting Officers must include compliance with this guide in the Statement of Work (SOW) for contractor employees.

c. This policy applies to the Office of Inspector General (OIG) to the extent that the OIG determines this guide 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.

d. This policy 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 does not conflict with other CBCA policies or the CBCA mission.

3. Cancellation. This Order cancels and supersedes 2165.2 CIO P GSA Telecommunications Policy.

4. Background. Telecommunications technologies are evolving quickly, promising increasing variety and dramatically improved performance of communications equipment, systems and services that will help GSA users increase work productivity inside and outside Federal government offices and facilities and improve their ability to serve the public. GSA telecommunications systems are part of the GSA IT infrastructure and are subject to monitoring and other standards prescribed in the GSA Telecommunications Guide and in 2104.1B CIO CHGE 1 GSA Information Technology (IT) General Rules of Behavior.

5. Definitions. GSA telecommunications include the GSA-provided equipment, systems and services utilized by authorized users for voice, data and Internet communications, including traditional voice, voice over IP (VoIP) and unified communications (UC) systems that are accessible with a desk phone, conference phone or soft phone client on a personal computer (PC), basic cell phone, or smartphone. Additional telecommunications technologies include broadband DSL, cable modem, public Wi-Fi, and cellular 4G and 5G access networks. Personal devices, those which are not procured by GSA but used by individuals for work purposes, are included in GSA telecommunications (see Section 6.j.(6) below).

6. Guiding Principles.

a. Rules. The use of GSA telecommunications must comply with all applicable GSA policies and other Federal Government rules. The GSA Telecommunications Guide provides greater detail regarding applicable rules.

b. Authorized Use. GSA provides authorized users with all equipment, systems and services used for conducting Federal government business. Per ADM 7800.11A Personal Use of Agency Office Equipment Policy, limited personal use of GSA telecommunications must not interfere with the user's work duties. Limited personal use of GSA telecommunications is allowed as long as it does not affect work productivity or incur additional cost to GSA. When traveling outside of the US, or in areas near US borders, authorized users should seek guidance from GSA IT as to how to avoid international roaming charges. Additional information may be found here - https://insite.gsa.gov/employee-resources/information-technology/do-it-yourself-self-help/mobile-devices-phones-tablets/international-travel-with-your-gsa-smartphone.

c. Equipment Security. Users are responsible for the security of GSA telecommunications equipment assigned to them and for protecting any information regarding Federal government business that is stored on it.

(1) Users may be financially responsible for government property if it is stolen, damaged, lost, or destroyed as a result of negligence, improper use, or other willful actions.

(2) Lost or stolen equipment should be reported promptly by email to ITServiceDesk@gsa.gov or by calling 1-866-450-5250 to ensure that appropriate Agency personnel are aware of any potential data breach and to attempt to recover the GSA IT asset.

d. Information Ownership. All documents, images and messages composed, sent, received, or stored on GSA-provided equipment remain the property of the GSA.

e. Information Privacy. CIO 2180.2 GSA Rules of Behavior for Handling Personally Identifiable Information (PII) governs user behavior regarding private and confidential information.

f. Applications. Any software application determined to be a security risk cannot be installed or will be immediately removed.

g. Voice Telephony. This includes GSA-provided desk phones, softphone PC clients, basic cell phones, and smartphones. Personal usage is allowed for short-duration calls. Long-distance calls should be minimized.

h. Commercial Telephone Services. Calls using non-GSA telecommunication services such as operator-assisted, collect, and directory assistance calls should be minimized and used only for Federal government business.

i. Wireless Devices. This includes GSA-owned cell phones, smart phones, and air cards that connect to the Internet. A user whose work duties require use of a wireless device can request one through GSA's IT Service Catalog.

(1) Directory. Users should enter their cellular phone number in the GSA Credential and Identity Management System (GCIMS) located at https://gcims.gsa.gov.

(2) One Device. Users who need a wireless device for their work duties are assigned one device. If more than one device is needed, their supervisor can send a waiver request through GSA's IT Service Catalog for a second device to be provided.

(3) Wireless Security. Wireless devices must meet a number of GSA IT requirements for passwords, lockout time, encryption, and other requirements of GSA IT. Refer to 2100.1M CIO CHGE 1 GSA Information Technology (IT) Security Policy.

(4) IT Service Desk. Users requiring assistance can send an email to ITSeviceDesk@gsa.gov or call 1-866-450-5250.

(5) Wireless Services. Users normally have cellular wireless services through GSA's Cellular Wireless contract(s). These services can be used for reasonable personal use where no additional expense to GSA would be incurred such as roaming or excessive data charges.

(6) Personal Devices. Prior to using a personally owned wireless device to access GSA email or for GSA business, users must sign the "Personal Mobile Devices - Rules of Behavior with Digital Signatures" document. Then users create a ticket with the IT Service Desk by composing an email to itservicedesk@gsa.gov, attaching the digitally signed Rules of Behavior document, and requesting that the user's mobile device be provisioned with the Agency's Mobile Device Management solution. Finally, users must complete the Provisioning Certification form for their device. All documents needed for this process may be found here https://sites.google.com/a/gsa.gov/mobileinfo/rules-of-behavior-of-mobile-devices

For more information refer to the IT Security Procedural Guide: Securing Mobile Devices and Applications, CIO-IT Security-12-67.

7. Emergency Usage Reductions. During emergency situations, users should minimize use of GSA telecommunications for the duration of the emergency.

8. Waste, Fraud, and Abuse. Users are strongly encouraged to report suspected waste, fraud, and abuse of GSA telecommunications to their supervisor and to the Office of the Inspector General by emailing fraudnet@gsaig.gov. These reports will be treated confidentially.

9. Monitoring. GSA IT continuously monitors use of GSA telecommunications. GSA may audit a user's telecommunications usage at any time. The 2100.1L CIO CHGE 1 GSA Information Technology (IT) Security Policy" states:

a. Obtaining access to GSA resources must constitute acknowledgment that monitoring activities may be conducted.

b. Users have no expectation of privacy on GSA IT systems. All activity on GSA IT systems is subject to monitoring.

10. Deviation. Users who fail to comply with this policy may incur disciplinary action. Any disciplinary action within GSA shall be guided by HRM 9751.1 Maintaining Discipline.

11. Relation of this Policy to Other Policies. This policy is intended to be consistent with other GSA policies and Federal government rules and standards, which are located at https://www.gsa.gov/directives-library.

12. Clarification and GSA Contacts. For help in understanding this policy, refer to GSA's Guide to Official Use of Telecommunications. If the answer sought is not found or users wish to report a violation of this policy or request further information, please contact ITSeviceDesk@gsa.gov or call 1-866-450-5250.

13. Explanation of Changes.

a. Updated broken links throughout.

b. Updated applicability section to include information about the Civilian Board of Contract Appeals (CBCA)

c. Removed outdated references to calling cards.

d. Changed references from "GSA Order 10000 CIO G CHGE 1 GSA Telecommunications Guide", to "GSA's Guide to the Official Use of Telecommunications."

e. Changed signing official from Sonny Hashmi to current CIO, David Shive.

14. Signature.

DocuSigned by:
David Shive
A3AE4284A2754F9...

DAVID SHIVE
Chief Information Officer
Office of GSA IT