U.S. General Services Administration (GSA)

GSA Order: GSA Telecommunications Policy
CIO 2165.2C
GSA IT
ITSeviceDesk@gsa.gov

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.

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 2104.1C CIO GSA Information Technology (IT) General Rules of Behavior.

Applicability:

1. 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.

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

3. 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.

4. 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.

Cancellation:

This Order supersedes CIO P 2165.2B, GSA Telecommunications Policy

Summary of Changes:

1. Updated document to conform with OAS 1832.1C.
2. Added paragraph to align with requirements in OMB memo M-25-21.

Signature

____/S/______________________
David Shive
Chief Information Officer
Office of GSA IT

__12/19/2025________
Date

1. 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 broadband telecommunications technologies include DSL, cable modem, public Wi-Fi hotspots, and cellular data networks. Personal devices, those which are not procured by GSA but used by individuals for work purposes, are included in GSA telecommunications (see Section 2.10 below).

2. Guiding Principles

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.

2.1. Authorized Use

GSA provides authorized users with all equipment, systems and services used to conduct official Federal government business. As outlined in, ADM 7800.11A Personal Use of Agency Office Equipment Policy limited personal use of GSA telecommunications is permitted, provided it does not interfere with work duties, negatively impact productivity, or incur additional costs to GSA. When traveling outside the United States, users must comply with OMA guidance for submitting Foreign Travel Notifications to obtain required approvals.

2.2. 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.

- 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.

- Users are responsible for the security and proper management of all government property issued to them by

GSA. This includes, when necessary, transporting the property between their home and workplace and securing it overnight in a personal or office locker if using an unassigned or hoteling workstation.

- 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.

2.3. Information Ownership

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

2.4. Information Privacy

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

2.5. Applications

Any software application determined to be a security risk cannot be installed or will be immediately removed. The GSA IT Standards Program is governed by CIO 2160.1 CIO GSA Information Technology (IT) Standards Policy.

2.6. Artificial Intelligence (AI)

The use of AI tools and applications accessed through GSA resources must be for authorized purposes only and in accordance with CIO 2185.1B Use of Artificial Intelligence at GSA. Users are prohibited from using AI for personal gain, illegal activities, or any purpose that violates agency policy or federal law.

2.7. 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.

2.8. 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.

2.9. Wireless Devices

This includes GSA-provided cell phones and smart phones. A user whose work duties require use of a wireless device can request one through GSA's IT Service Catalog.

- 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.
- 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 Securing Mobile Applications and Devices [CIO-IT Security-12-67 Rev. 8].
- 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.

2.10. Personal Devices

Cannot access the GSA internal Wired or Wireless Networks in Regional and Central Office Buildings. They can connect only to the GSA Guest Network to access the Internet and GSA resources available to the public (www.gsa.gov).

- Guest Wireless Accounts. Are not GSA enterprise accounts.
- Guest Wireless Traffic. Is subject to the same content filtering as traffic on the GSA network.

2.11. Peripheral Devices

External hardware components (ex., docking stations, keyboards, mice, microphones, monitors, webcams, etc.) that do not possess storage and network (WiFi/Ethernet) capabilities. Devices of this type do not require IT Security review or approval for usage with GSA-provided equipment.

- They must use generic drivers.
- They must not require the installation of software or firmware for usage.

3. IT Service Desk

Users requiring assistance can connect with the Help Desk by email: ITSeviceDesk@gsa.gov, by phone: 1-866-450-5250, or URL: Self Service Portal.

4. Emergency Usage Reductions

During emergency situations, users should minimize use of GSA telecommunications for the duration of the emergency.

5. 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.

6. Monitoring

GSA IT continuously monitors use of GSA telecommunications. GSA may audit a user's telecommunications usage at any time. GSA Order 2100.1Q CIO P GSA Information Technology (IT) Security Policy states:

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

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

7. Deviation

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

8. 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.

9. Clarification and GSA Contacts

For help in understanding this policy, refer to GSA's Guide to Official Use of Telecommunications. If further assistance is required, contact ITSeviceDesk@gsa.gov or call 1-866-450-5250.