Administrative Policies

Technology Devices-Acceptable Use & Security Policy

POLICY #:	*ADM-3013, Rev. 2*
EFFECTIVE:	*July 24, 2026*
SUPERSEDES:	*Technology Devices Acceptable Use & Security Policy, Rev. 1-released September 1, 2021*

PURPOSE:

This policy provides expectations and guidelines for the safe and appropriate use of WorkForce Central issued technology devices and for personal devices when used to perform WorkForce Central related business. Inappropriate use of technology devices can lead to risks including virus attacks, compromise of network systems and services, compliance concerns, and potential legal issues.

Technology devices that apply to this policy include, but are not limited to phones, laptops, tablets, notebook computers, monitors, cameras, televisions, printers, servers, switches, projectors, and copiers.

This policy was updated in its entirety to clearly define employee responsibilities and establish modern security guidelines for the use of WorkForce Central-funded devices.

The requirements for the purchasing, management, and inventory control measures specific to technology devices is addressed in WorkForce Central's Property Management & Inventory Control Policy located on WorkForce Central's Policy Library.

BACKGROUND:

This policy applies to the use of information, electronic and computing devices, and network resources to conduct WorkForce Central business or interact with internal networks and business systems, whether owned or leased by WorkForce Central, the employee, or a third party. This policy applies to employees, contractors, consultants, temporaries, and other workers at WorkForce Central, including all personnel affiliated with WorkForce Central subrecipients and other third parties.

WorkForce Central is the authorized and liable entity responsible for ensuring the security and integrity of technology devices on behalf of WorkForce Central and its employees, subrecipients, and contractors. WorkForce Central will maintain a Technology Information (IT) Department who is responsible for ensuring the security and integrity of these technology devices. WorkForce Central's IT Department can be reached at support@workforce-central.org.

POLICY:

All employees, contractors, consultants, temporaries, and other workers at WorkForce Central and its subrecipients are responsible for following the expectations and practices outlined here regarding the appropriate use of information, technology devices, and network resources in accordance with WorkForce Central policies and standards, and applicable laws and regulations.

For security and network maintenance purposes, authorized WorkForce Central staff may monitor equipment, systems, and network traffic at any time through various methods, including but not limited to remote monitoring, internal and external audits.

Any exception to this policy must first be approved by the WorkForce Central IT Department.

PROPRIETARY INFORMATION

WorkForce Central proprietary information (information collected or created as an employee or under contract with WorkForce Central) that is stored on technology devices whether owned or leased by WorkForce Central, the employee or a third party, remains the sole property of WorkForce Central. Employees are responsible for safeguarding proprietary information and must use appropriate security measures to protect it from unauthorized access, disclosure, alteration, loss, or destruction. Documents must be saved in a WorkForce Central cloud storage location, such as One Drive or SharePoint and not on the device's hard drive or desktop; only share proprietary information with authorized personnel using secure sharing features and do not share with unauthorized individuals or personal accounts; immediately report lost or stolen devices and any suspected data breaches with the WorkForce Central IT Department.

Employees may access, use, or share WorkForce Central proprietary information only to the extent it is authorized and necessary to fulfill assigned job duties. Employees must promptly report the theft, loss, or unauthorized disclosure of WorkForce Central proprietary information.

SCOPE AND SECURITY PRINCIPLES

WorkForce Central applies the principle of least privilege to all users and devices connect to internal resources. Access is limited to what is necessary to perform essential job functions.

STRICTLY PROHIBITED

The following are strictly prohibited:

- Activity that is illegal under local, state, federal or international law while using WorkForce Central resources.
- Access to WorkForce Central data/servers/accounts that is limited to authorized personnel; do not attempt access without permission.
- System and Network Misuse (strictly prohibited):
    - Installing/distributing unlicensed ("pirated") software, copying copyrighted materials without authorization.
    - Exporting software/technical information in violation of export control laws (consult WorkForce Central IT Department before any export).
    - Introducing malicious software (viruses, worms, Trojans, email bombs).
    - Making fraudulent offers originating from any WorkForce Central account.
    - Security breaches or disruptions (e.g., accessing data you are not intended to receive; logging into unauthorized servers/accounts; network sniffing, ping floods, packet spoofing, denial-of-service, forged routing).
    - Port/security scanning without prior WorkForce Central IT Department approval.
    - Executing network monitoring that intercepts data not intended for your host unless it is part of your job.
    - Bypassing or attempting to bypass login requirements, access controls, or security measures protecting systems, networks, or accounts.
    - Introducing honeypots/honeynets or similar technologies on the WorkForce Central network.
    - Interfering with or denying service to other users/devices.
    - Using scripts/programs to interfere with or disable another user's sessions/device/network access.
    - Connecting personal devices (computer/network devices/other equipment) directly-wired or wireless-to the internal corporate private network.
- Digital Communication Misuse (strictly prohibited):
    - Sending unsolicited messages (spam, junk mail) or engaging in harassment via email/phone/other digital methods.
    - Forging email headers or harvesting email addresses to harass/spam.
    - Creating/forwarding chain letters, Ponzi or pyramid schemes.
    - Posting non-business messages to large groups (spam).
    - Using WorkForce Central devices to access personal social media accounts.
    - Using WorkForce Central accounts/devices to procure or transmit material in violation of sexual harassment or hostile workplace laws.

- Using WorkForce Central trademarks/logos/IP in connection with blogging or similar activities without authorization.

WORKFORCE CENTRAL DEVICE SECURITY

Users must:

- Enable a password-protected screen saver that activates after 15 minutes or less of inactivity.
- Lock your screen or log off whenever unattended.
  - *Quick tip (Windows)*: Press Windows + L to lock instantly.
- Keep devices patched and up to date with required security updates and WorkForce Central configurations.
- Not leave WorkForce Central issued assets unattended in unsecured locations (e.g., airports, coffee shops). Acceptable secured locations include but are not limited to:
  - A locked vehicle (store assets out of sight when possible).
  - Home (secured from family/guest use).
  - Designed secure areas within WorkForce Central facilities (assigned workspaces/equipment storage).
- Report lost or stolen devices immediately to WorkForce Central's IT Department by email, phone and/or IT ticket.
- Upon termination of employment or engagement, return all WorkForce Central technology assets promptly to the WorkForce Central IT Department or other designated WorkForce Central staff.
- Follow all telecommuting policies regarding secure storage when working remotely.

PASSWORDS & AUTHENTICATION

Password Requirements

Passwords must:

- Meet current Microsoft 365 requirements in effect at the time of creation/change (e.g., length, complexity).
- Be at least 12 characters with a mix of uppercase, lowercase, numbers and special characters.
- Not be reused across multiple accounts or external services.
- Not be a previously used password.

Password Protection

Protect passwords by:

- Keeping passwords confidential; never share with anyone, including coworkers, supervisors, or WorkForce Central's IT Department.
- Not writing down or storing passwords in unsecured locations.
- Using Multi-Factor Authentication (MFA) everywhere available (required for access to company systems).
- Using password managers (e.g., Microsoft Edge Password Manager) is encouraged.

When to Change a Password

Change a password immediately if:

- A device or account is suspected to be compromised (report to support@workforce-central.org).
- Unauthorized access is suspected.
- There is evidence of a data breach.
- Directed by WorkForce Central IT Department or other authorized entity.

HANDLING REGULATED AND CONFIDENTIAL DATA

Prevent unauthorized viewing by:

- Positioning screens to reduce visibility.
- Using privacy screen protectors when appropriate.

When communicating regulated data verbally (e.g., phone calls/discussions), take the following precautions:

- Close doors, ask others to step out, use headphones, speak quietly.
- Choose a more secure method if available.
- Do not store confidential information on personal devices.

EMAIL AND PHISHING AWARENESS

- Use extreme caution with email attachments, especially from unknown senders.
- Treat emails requesting credentials or linking to sign-in portal with utmost caution.
- If in doubt, report as Phishing in Microsoft 365; do not forward suspicious emails.
    - WorkForce Central IT will investigate. Legitimate messages are released back to your inbox.
- If the "Report Phishing" button is unavailable:

- Take a screenshot (show sender, subject, content) and send via email or Teams to WorkForce Central IT Department.
- Block the sender, then delete the suspicious email from the Inbox and Trash.

- Never provide WorkForce Central credentials or identify verification codes in response to unsolicited emails, calls, or texts.

CONNECTIVITY SERVICES & NETWORK USE

Microsoft 365 (web access)

Emergency Access Only: Employees with Exchange accounts may use Microsoft 365 web page access from internet-connected browser only in emergency circumstances. Whenever possible, remote access to email, calendar, and Teams must be conducted using work-issued devices or approved applications on authorized personal mobile devices.

PERSONALLY OWNED TECHNOLOGY/DEVICES

General

Use of personal devices for WorkForce Central business requires WorkForce Central IT Department authorization.

Allowed personal device and usage:

- Personal smartphones
  - Permitted apps: Microsoft Teams and Outlook only.
  - Use cases: messaging, meetings, calendar, basic communication.
- Personal tablets
  - Teams (web version only); users must log in manually every time (no auto-login).

Prohibited personal device and usage:

- Personal laptops/PCs for any work access.
- Accessing internal systems, file shares.
- Downloading, storing, forwarding, or processing personally identifiable information (PII)/sensitive/confidential data
- Syncing work data to personal cloud services (e.g., iCloud, Google Drive).
- Downloading work materials/files to personal devices.
- Any high-risk telework activity

Personal device security and access controls

Personal devices must:

- Have screen lock and strong password/PIN (biometric allowed).
- Not be jailbroken/rooted; no auto-login for any WorkForce Central service.
- Use only WorkForce Central IT-authorized apps.
- Use private/incognito mode when accessing approved resources.
- Access may be denied if insecure configurations are detected (e.g. jailbroken/rooted, no passcode).

Wi-Fi Rules for Personal Devices

- **Allowed:** Home networks using WPA2/WPA3
- **Restricted:** Public Wi-Fi and only if necessary and only for Teams/Outlook (MFA required); no PII viewing.
- **Prohibited:** Open/unsecured Wi-Fi (no password).

Outlook on Personal Devices

- **Allowed:**
  - Outlook Mobile App or Outlook Web (private/incognito mode).
  - Viewing/responding to non-sensitive emails, calendar/meeting links.
- **Required:**
  - Device passcode/biometric.
  - Device note jailbroken/rooted.
  - Logout after each browser session; do not save passwords.
- **Prohibited:**
  - Saving attachments to the device.
  - Forwarding work email to personal accounts.
  - Using native mail apps (Apple Mail, Samsung Mail, Gmail app, etc.)
  - Storing, screenshotting, or copying sensitive/confidential email content.
  - Syncing calendar/contacts to personal clouds.

Work Photos on Personal Devices

Work-related photos are permitted on personal devices only when:

- No work device is available, and
- The content supports an authorized business purpose.

Required Handling

Work-related content such as images/photos/videos on personal devices must be transferred to OneDrive/SharePoint as soon as possible; verification of upload is required. Upon successful transfer:

- Immediately delete the content from the personal device and delete from the Recently Deleted/Trash.
- Ensure media does not auto-back up to personal cloud accounts.
- Do not share via personal messaging/email/AirDrop/personal social platforms.

Personal Devices-Public Records Reminder

Any work-related emails, images/photos/videos on a personal device are public records. Only the work content is subject to disclosure. Personal data on the device is not subject to disclosure.

PERSONAL HOTSPOT USAGE

General Requirements

- Use personal hotspots only when WorkForce Central Wi-Fi or approved wired network connections are unavailable.
- Hotspots must use encryption and strong passwords; change regularly.
- Disable automatic connections and turn hotspots off when not in use.
- Ensure hotspot use does not expose WorkForce Central data or systems to risk.

Prohibited Hotspot Usage

- Do not access, transmit, or process PII over personal hotspots or public Wi-Fi.
- Do not share personal hot spots with unauthorized individuals or devices.
- Do not use hotspots to bypass WorkForce Central network security controls/monitoring.

Best Hotspot Practices

- Use the strongest available encryption (WPA2/WPA3).
    - iPhone: WPA2 by default; WPA3 supported on iOS 15+ where available; keep iOS updated.
    - Android: Settings > Network/Hotspot> WPA3-Personal if available, otherwise WPA2-Pesonal. Never use Open (no password).
    - Alternatively, check the Wi-Fi security type on a connected device (e.g., WPA2/WPA3).
- Keep SSID non-identifiable (avoid personal/WorkForce Central details).
- Review connected devices regularly; disconnect any unauthorized device.
- Limit hotspot usage to essential business functions only.

- Keep device OS/security patches up-to-date.

MIFI DEVICE USAGE

- A MiFi device is available for business use and should only be used when WorkForce Central Wi-Fi or other approved network connections are unavailable or unsuitable for business needs.
- Prior WorkForce Central IT Department approval is required.
- Users are responsible for safeguarding the device, using it in accordance with this policy, and ensuring WorkForce Central data remains protected while connected.
- The device must be returned promptly to the WorkForce Central IT Department upon completion of use or when requested to do so.
- Unauthorized sharing, transfer, modification, or use of the device for personal, illegal, or non-business purposes is prohibited.

LIMITED PERSONAL USE OF WORKFORCE CENTRAL ISSUED DEVICES

Limited personal use of Workforce Central issued devices is authorized only if:

- The use does not interfere with job responsibilities or WorkForce Central operations.
- It does not result in additional cost to WorkForce Central (i.e., excess token usage for our AI users).
- Does not violate WorkForce Central policies; federal, state, or local laws or regulations.
- The use does not include accessing personal social media which is prohibited.

ATTESTATION AND CONSEQUENCES FOR NON-COMPLIANCE

It is the responsibility of WorkForce Central and its employees, subrecipients and contractors to safeguard the integrity of publicly funded purchases, including technology devices. WorkForce Central employees are required to attest that they have read and understand WorkForce Central's Technology Devices Acceptable Use and Security Policy. Copies of signed attestations will be placed in WorkForce Central employees' personnel files. WorkForce Central subrecipients and contractor attestations will be captured at the time of contract execution through the contract terms and conditions. Attestations may be made available upon request for monitoring and/or auditing purposes.

WorkForce Central staff who violate any part of this policy may be subject to employee disciplinary action. Violation of any part of this policy on behalf of WorkForce Central subrecipients and contractors may result in corrective action or termination of contract.

DEFINITIONS

AirDrop: A feature on Apple devices that allows users to wirelessly share files, photos, and other content with nearby Apple devices.

Denial-of-Service (DoS): An attack that attempts to make a system, application, or network unavailable by overwhelming it with excessive traffic or requests.

Forged Routing: The unauthorized manipulation of network routing information to redirect, intercept, or disrupt network traffic.

Harvesting Email: The collection of email addresses from websites, directories, messages, or other sources, often for spam, phishing, or marketing purposes.

Honeypot/Honeynet: A decoy system or network intentionally created to attract and study cyberattacks while helping detect malicious activity.

Jailbroken/Rooted Device: A mobile device that has been modified to remove manufacturer or operating system security restrictions, allowing unauthorized access to system functions.

MiFi Device: A portable wireless hotspot device that uses a cellular data connection to provide internet access to other devices.

Multi-Factor Authentication (MFA): A security method that requires users to provide two or more forms of verification, such as a password and a code sent to a mobile device

Network Monitoring: The observation and analysis of network activity to ensure performance, detect issues, and identify security threats.

Network Sniffing: The monitoring or capturing of data traveling across a network to view information being transmitted between devices.

OS (Operating System): The core software that manages a device's hardware, applications, and system functions, such as Windows, macOS, iOS, Android, or Linux.

Packet Spoofing: The creation and transmission of network data that contains a false or misleading source address to disguise its origin.

Password Manager: A software application that securely stores, generates, and manages passwords for user accounts.

Phishing: A fraudulent attempt to obtain sensitive information, such as passwords, financial information, or personal data, by pretending to be a trusted person or organization.

Ping Floods: A type of cyberattack that overwhelms a device or network by sending a large number of ping requests to disrupt normal operations.

Port/Security Scanning: The process of examining devices, systems, or networks to identify open ports, services, vulnerabilities, or security weaknesses.

SSID: The name of a Wi-Fi network that users see when searching for available wireless connections.

WPA2/WPA3: Wireless security standards used to protect Wi-Fi networks through encryption and authentication. WPA3 is the newer and more secure version.

AI-Assisted Content Notice: Portions of this policy were developed with the assistance of Artificial Intelligence (AI) tools. All content has been reviewed, validated, and approved by the organization to ensure accuracy, relevance, and alignment with organizational requirements.

WorkForce Central is an equal opportunity employer/program. Auxiliary aids and services are available upon request for individuals with disabilities. Washington Relay Service – 711.