Technology Devices Acceptable Use & Security Policy

Policy Number: ADM-3013

Revision Date: 9-1-21

Supersedes: Previously issued Technology Devices Acceptable Use and Security Policies (no policy number or date)

PURPOSE

The purpose of this policy is to provide expectations and guidance on the safe and appropriate use of WorkForce Central issued technology devices. Inappropriate use of the 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 cell phones, laptops, tablets, notebook computers, desktop computers, monitors, smart phones, cameras, televisions, DVD players, Blu-ray players, video cameras, printers, fax machines, servers, switches, projectors, and copiers

The requirements for the purchasing, management, and inventory control measures specific to technology equipment and supplies is addressed in WorkForce Central's Property Management & Inventory Control Policy located on WorkForce Central's website at https://workforce-central.org/about/policies/.

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 sub-recipients and other third parties. This policy applies to all equipment that is owned or leased by WorkForce Central.

POLICY

All employees, contractors, consultants, temporary, and other workers at WorkForce Central and its sub-recipients are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with WorkForce Central policies and standards, and applicable laws and regulations.

General Use and Ownership

- WorkForce Central proprietary information stored on electronic and computing devices whether owned or leased by WorkForce Central, the employee or a third party, remains the sole property of WorkForce Central. Employees must ensure through legal or technical means that proprietary information is protected in accordance with the WFC Data Protection Standard as supported by the NIST Cybersecurity Framework. For example, ensure documents are saved in One Drive and not on the desktop and documents are not shared with non-authorized personnel.
- Employees must promptly report the theft, loss, or unauthorized disclosure of WorkForce Central proprietary information.

- 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 are prohibited from using WorkForce Central issued technology devices for personal use.
- For security and network maintenance purposes, authorized individuals within WorkForce Central may monitor equipment, systems, and network traffic at any time.
- WorkForce Central reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.
- It is the responsibility of WorkForce Central and its employees, sub-recipients, 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 sub-recipients 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 is the authorized and liable entity responsible for ensuring the security and integrity of technology devices on behalf of WorkForce Central and its employees, sub-recipients, and contractors. WorkForce Central will maintain a Technology Information (IT) Team who has been delegated the responsibility for ensuring the security and integrity of these technology devices. WorkForce Central's IT Team can be reached at support@workforce-central.org.
- 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 sub-recipients and contractors may result in corrective action or termination of contract.

Security and Proprietary Information

- WorkForce Central will ensure mobile and computing devices that connect to the internal network are in compliance with the Minimum Access Policy.
- System level and user level passwords must comply with the password instructions provided at the time hire or receipt of WorkForce Central issued devices. Providing password access to another individual, either deliberately or through failure to secure its access, is prohibited. Questions about passwords may be submitted to WorkForce Central's IT Team at support@workforce-central.org.
- All computing devices must be secured with a password-protected screensaver with the automatic activation feature set to 15 minutes or less. Employees must lock screens or log off when the device is unattended.
- Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of WorkForce Central authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing WorkForce Central-owned resources.

The lists below are by no means exhaustive, but an attempt to provide a framework for activities which fall into the category of unacceptable use. The following activities are strictly prohibited, with no exceptions:

- System and Network Activities:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by WorkForce Central.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which WorkForce Central or the end user does not have an active license is strictly prohibited.
- Only authorized WorkForce Central staff have access to data, servers, or accounts.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The WorkForce Central IT Team must be consulted prior to export of any material that is in question.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- Using a WorkForce Central computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.
- Making fraudulent offers of products, items, or services originating from any WorkForce Central account.
- Making statements about an items warranty, expressly or implied, unless it is a part of normal job duties.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Port scanning or security scanning is expressly prohibited unless prior notification to WorkForce Central's IT Team is made.
- Executing any form of network monitoring which will intercept data not intended for the employee's host unless this activity is a part of the employee's normal job or duty.
- Circumventing user authentication or security of any host, network, or account.
- Introducing honeypots, honeynets, or similar technology on the WorkForce Central network.
- Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

- Email and Communication Activities:
  - Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
  - Any form of harassment via email, telephone, or paging, whether through language, frequency, or size of messages.
  - Unauthorized use, or forging, of email header information.

- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters", "Ponzi", or other "pyramid" schemes of any type.
- Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).
- Employees are not authorized to use WorkForce Central technology resources to access their personal social media accounts and blogs.
- Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, WorkForce Central's trademarks, logos and any other WorkForce Central intellectual property may also not be used in connection with any blogging activity.

Policy Compliance

WorkForce Central's IT Team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits.

Any exception to the policy must be approved by the WorkForce Central's IT Team in advance.

Violation of this policy may result in disciplinary action, up to and including termination of employment or termination of contract.

ATTACHMENT

- WorkForce Central Employee Attestation for the Acceptable Use and Security of Technology Devices

APPROVED

Katie Condit (Sep 1, 2021 16:46 PDT) Sep 1, 2021

Katie Condit, WFC CEO Date

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