Acceptable Use Policy, version 1.2

Status: ☐ Working Draft ☒ Approved ☒ Adopted
Document Owner: Information Security Committee
Last Review Date: January 2023

Acceptable Use Policy

Purpose

The purpose of the Washington County Acceptable Use Policy is to establish acceptable practices regarding the use of Washington County **Information Resources** in order to protect the confidentiality, integrity and availability of information created, collected, and maintained.

Audience

The Washington County Acceptable Use Policy applies to any individual, vendor, contractor, or process that interacts with any Washington County information system, computer, and network.

Contents

Policy

All computing hardware, software, electronic and telephonic media, and networks (Information Resources) provided to you by Washington County are the property of Washington County and are to be used for County business purposes only unless otherwise indicated in this policy. Communications via these Information Resources are not private. Any use of the County's Information Resources constitutes consent by the user to have such use monitored by the County at its sole discretion with or without prior notice to the user. The use of personal devices to conduct county business may be granted by management. Personal device usage for county business may subject the device to the disclosure requirements of Wisconsin's open records laws. Reference 'Bring Your Own Device' policy for further information on using personal devices for county business.

The following pages will provide guidance on the acceptable use of County information resources. If you have questions regarding any aspect of this policy, please contact the IT Help Desk at extension 6869 or email at ithelpdesk@washcowisco.gov.

- Acceptable UsePersonnel must promptly report events or policy violations involving Washington County computers, networks or information to their supervisor. Events include, but are not limited to, the following:
    - Technology incident: any potentially harmful event that may cause a failure, interruption, or loss in availability to Washington County **Information Resources**.
    - Data incident: any potential loss, theft, or compromise of Washington County information.
    - Unauthorized access incident: any potential unauthorized access to a Washington County **Information Resource**.
    - Facility security incident: any damage or potentially unauthorized access to a Washington County owned, leased, or managed facility.
- Personnel shall not purposely engage in activity that may
    - degrade the performance of Washington County computers, **networks and servers.**
    - deprive authorized Washington County personnel access to a Washington County **networks, services, and information.**
    - obtain additional permissions beyond those allowed;
    - or circumvent Washington County information security measures.
- All inventions, intellectual property, and proprietary information, including reports, drawings, blueprints, software codes, computer programs, data, writings, and technical information, developed by County personnel using Washington County **Information Resources** are the property of Washington County.
- Personnel shall cooperate with incident investigations, including any federal or state investigations.
- Personnel are expected to comply with all legal protections provided by patents, copyrights, trademarks, and intellectual property rights for any software and/or materials viewed, used, or obtained using Washington County **computers and networks.**
- Unless part of specific job duties, personnel shall not intentionally access, create, store or transmit material which Washington County may deem to be offensive, indecent, or obscene.
- Use of the system or network from Washington County facilities to access, view, store or distribute obscene or pornographic materials is prohibited and may result in disciplinary action. The only exception to this is when an employee is authorized to do so in the performance of official duties.
- Files, directories, data, and email shall be maintained in a manner consistent with the County's record/retention policy set forth at section Ch. 94, Article II of the Washington County Code.

Access Management

- Personnel are permitted to use only those network and host addresses issued to them by Washington County IT and should not attempt to access any data or programs contained on Washington County systems for which they do not have express authorization .
- All remote access made to internal Washington County networks and/or environments must be made through approved, and Washington County-provided, virtual private networks (VPNs), or remote access systems.
- Personnel should not disclose any access information to anyone not specifically authorized to receive such information, including IT support personnel.
- Personnel must not share their personal authentication information, including:
    - Account passwords,
    - Personal Identification Numbers (PINs),

  - Security Tokens (i.e. Smartcard),
  - Multi-factor authentication information
  - Access cards and/or keys,
  - Digital certificates,
  - Similar information or devices used for identification and authentication purposes.
- Access cards and/or keys that are no longer required must be returned to physical security personnel.
- Lost or stolen access cards, security tokens, and/or keys must be reported by the employee to their supervisor as soon as possible.

Authentication/Passwords

- All personnel are required to maintain the confidentiality of personal authentication information.
- Any group/shared authentication information must be maintained solely among the authorized members of the group.
- All passwords, including initial and/or temporary passwords, must be constructed, and implemented according to the following Washington County rules:
  - Must meet all requirements including minimum length, complexity, and reuse history.
  - Must not be easily tied back to the account owner by using things like username, social security number, nickname, relative's names, birth date, etc.
  - Must not be the same passwords used for non-business purposes.
  - Must be changed when required by the systems.
- Unique passwords should be used for each system, whenever possible.
- If the security of a password is in doubt, the user must contact the Information Technology Help Desk, and the password should be changed immediately.
- Security tokens (i.e. Smartcard) must be returned on demand or upon termination of the relationship with Washington County, if issued.

Clear Screen

- Personnel should log off from applications or network services when they are no longer in use.
- Personnel should log off or lock their workstations and laptops when their workspace is unattended.
- Physical and/or electronic keys used to access **confidential information** should not be left on an unattended desk or in an unattended workspace if the workspace itself is not physically secured.
- Laptops should be either locked with a locking cable or locked away in a drawer or cabinet when the work area is unattended or at the end of the workday if the laptop is not encrypted.
- Passwords must not be posted on or under a computer or in any other physically accessible location.
- Remote users must take all necessary precautions off-site to minimize any inadvertent disclosure of information, including but not limited to keeping the computer screen out of sight of others, logging off the computer when tasks are completed, and logging off and securing the computer when it is not being used.

Data Security

- Personnel should use approved encrypted communication methods whenever sending **confidential information** over public computer networks (Internet). This includes encrypting email, using HTTPS (Secure) websites, and other secure protocols or portals.
- Only authorized **cloud computing applications** may be used for sharing, storing, and transferring **confidential** or **internal information**.
- Information must be appropriately shared, handled, transferred, saved, and destroyed, based on the information sensitivity.
- All electronic media containing confidential information must be securely disposed when no longer in service. Please contact IT for guidance or assistance.
- Users are prohibited from maliciously changing data information, eavesdropping and tapping of telecommunications lines. Employees are put on notice that a violation of this rule is considered of the utmost gravity and may result in termination for first offense.

Email and Electronic Communication

- The electronic mail (email) system hardware, software, and data are County property. All messages composed, sent or received on the electronic mail system are and remain the property of the County. Email messages are not the private property of any user. All communications may be public records subject to disclosure under Wisconsin's Public Records law.
- The County reserves the right to access, monitor and disclose the contents of all messages created, sent or received using its email system without the consent of the user. Users are expected to communicate in a professional manner reflecting positively on them and Washington County.
- Auto-forwarding electronic messages outside the Washington County internal systems is prohibited.
- Electronic communications should not misrepresent the originator or Washington County.
- Individual accounts must not be shared without prior authorization from Washington County IT, with the exception of calendars and related calendaring functions.
- Any personal use of Washington County provided email shall not:
    - Involve solicitation.
    - Be associated with any political entity.
    - Forward chain emails.
    - Contain or promote unethical behavior.
    - Violate local, state, federal, or international laws or regulations.
    - Result in unauthorized disclosure of Washington County **confidential information**.
    - Or otherwise violate any other Washington County policies.
    - Be considered offensive or disruptive. Offensive or disruptive content includes, but is not limited to images or language that may reasonably be considered to be obscene, harassing, illegal, or otherwise inappropriate for the workplace.
- Personnel should use caution when responding to, clicking on links within, or opening attachments included in electronic communications.
- Personnel should not disclose **confidential information** in Out of Office or other automated responses.

Hardware and Software

- All hardware must be formally approved by IT Management before being connected to Washington County networks.
- Software installed on Washington County equipment must be approved by IT Management and installed by Washington County IT personnel.
- All Washington County computers and networking equipment taken off-site should be physically secured at all times.
- Employees should not allow family members or other non-employees to access Washington County **Information Resources**.
- No user-owned or non-County purchased/owned software is to be installed on County owned computer equipment. Demonstration software needs prior approval from the Information Technology department.
- Violation of software licensing agreements is a serious action and will subject the violator to appropriate discipline. Unauthorized software will be deleted upon discovery with or without prior notice from the Information Technology department.

Internet

- Personal use of the Internet service furnished by or through the County shall be extremely limited, tempered by good judgement at all times, shall not interfere with work responsibilities or impact network performance.
- Unapproved Internet activities include, but are not limited to:
    - Recreational games,
    - Streaming media,
    - Personal social media,
    - Accessing or distributing pornographic or sexually oriented materials,
    - Attempting or making unauthorized entry to any network or computer accessible from the Internet.
    - Or otherwise violate any other Washington County policies.
- Access to the Internet from outside the Washington County network using a Washington County owned computer must adhere to all of the same policies that apply to use from within Washington County facilities.
- The County has the right to monitor internet websites visited by all users while using County computers and the County network.
- Use of copyrighted materials shall be done with the express written permission of the owner.
- The Internet is an unsecured network. Confidential or privileged information shall be protected and secured at all times, by using encryption and/or secure methods of transfer such as SecureFTP, or HTTPS sites.
- All use of the Internet shall be in conformity with local, state, and federal laws as well as Washington County policies and procedures.
- Installation and use Social Media application TikTok, is prohibited from use on Washington County devices, and Washington County's networks and systems.

Physical Security

- Personnel must badge in to access-controlled areas.
- Visitors accessing card-controlled areas of facilities must be accompanied by authorized personnel at all times.
- Eating or drinking are not allowed in data center or network closets.

Privacy

- Systems Administrators, Washington County IT, and other authorized Washington County personnel may have privileges that extend beyond those granted to standard business personnel. Personnel with extended privileges shall not access files and/or other information that is not specifically required to carry out an employment related task.
- All information received by the user that is confidential in nature shall be protected and secured at all times in accordance with applicable federal, state and local laws and regulation, and departmental policies. Confidential information shall not be disclosed or re-disclosed by the user except as allowable or required by law.

Removable Media

- The use of **removable media** for storage of Washington County information must be supported by a reasonable business case.
- All **removable media** use must be approved by Washington County IT prior to use.
- **Personally owned removable media** use is not permitted for storage of Washington County information.
- Personnel are not permitted to connect **removable media** from an unknown origin without prior approval from the Washington County IT.
- Confidential and internal Washington County information should not be stored on **removable media** without the use of encryption.
- All removable media must be stored in a safe and secure environment.
- Employees must report the loss or theft of a **removable media** device that may have contained any Washington County information. Loss or theft must be reported to the Washington County IT and the employees supervisor immediately.

Security Training and Awareness

- All new personnel must complete an approved **security awareness** training class prior to, or at least within 30 days of, being granted access to any Washington County **Information Resources**.
- All personnel must complete the annual security awareness training.

Voicemail

- Personnel should not disclose **confidential** in voicemail greetings.
- Personnel should not access another user's voicemail account unless it has been expressly authorized.

Incidental Use

- As a convenience to Washington County personnel, incidental use of **Information Resources** is permitted. The following restrictions apply:

    - Incidental personal use of electronic communications, Internet access, fax machines, printers, copiers, and so on, is restricted to Washington County approved personnel; it does not extend to family members or other acquaintances.
    - Incidental use should not result in direct costs to Washington County.
    - Incidental use should not interfere with the normal performance of an employee's work duties.
    - No files or documents may be sent or received that may cause legal action against, or embarrassment to, Washington County or its customers.
- Storage of personal email messages, voice messages, files and documents within Washington County **Information Resources** must be nominal.
- All information located on Washington County **Information Resources** are owned by Washington County, may be subject to open records requests, and may be accessed in accordance with this policy.

Wireless Network (WIFI)

- Washington County will make available wireless access to the Internet for employees and guests, at certain enabled location which have been equipped with wireless access points.
- Washington County may grant access to this resource as a privilege.
- All users are expected to use this wireless access in a legal and responsible manner.
- Any user activity which violates local, state or federal law is strictly prohibited.
- The use of wireless access to the Internet and Information Resources is at the sole discretion of Washington County.
- Washington County may cancel access or discontinue offering wireless at any time without notice for any reason.
- Anyone who use wireless access to the Internet does so at their own risk.
- Any information transmitted over the network may be viewed by others.
- Washington County does not guarantee the privacy of any network communication.
- Washington County reserves the right to monitor activity and to disconnect the user at any time without notice for any reason.
- Washington County will not provide any technical support or assistance whatsoever unless it is on Washington County issued equipment and related to the conduct of official County business.
- Users should be aware that there is security, privacy and confidentiality risk inherent in wireless communications and associated technology and Washington County does not make any assurances or warranties related to such risks.
- Washington County reserves the right to deny or restrict access to any user who abuses the network, such as by excessive bandwidth consumption or acts that deliberately waste computer resources or unfairly monopolize resources to the exclusion of others.
- Washington County reserves the right to deny or restrict any type of activity or purpose deemed by Washington County to be unlawful, harassing, abusive, criminal or fraudulent.

Enforcement

Personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment, and related civil or criminal penalties.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

Version History

Version	Modified Date	Approved Date	Approved By	Reason/Comments
1.0	June 2021		Joel Woppert	Document Origination
1.1	April 2022		J. Woppert	Use of personal device may be granted by management.
1.2	January 2023		J. Woppert	Added verbiage on blocking TikTok.