Policy on Use of Communications and Computer Systems

Jeffcom 911 Communications

Adopted February 26, 2026, replacing undated two-page document entitled "Use of Communications and Computer Systems"

Overview

This policy establishes the rules of behavior for using Jeffcom communications, computer systems, and information resources. It applies to all Jeffcom employees, contractors, volunteers, and any other personnel who are granted access to Jeffcom information technology (IT) systems or data.

Before accessing Jeffcom systems or information, users must read, acknowledge, and comply with these rules. These requirements are not exhaustive. Users are expected to exercise sound judgment, act responsibly, and uphold the highest ethical standards at all times.

Penalties for Violations

Jeffcom may take corrective or disciplinary action against any user who violates Jeffcom policies or any applicable Washington State Patrol (WSP) or FBI system security requirements. Actions may include one or more of the following, as permitted by law:

- Discipline up to and including termination in accordance with Jeffcom policy and labor agreements;
- Suspension or revocation of system access or privileges; and
- Referral for criminal investigation or prosecution, when appropriate.

Prohibited Activities

The following activities are prohibited on any Jeffcom-owned or Jeffcom-managed information system, including Jeffcom-issued computers, phones, tablets, and other devices:

- Gambling;
- Knowingly accessing or viewing pornographic material;
- Political campaigning or political activity;
- Activities related to outside employment or personal business ventures; and
- Endorsement or promotion of non-Jeffcom products, services, or organizations.

Ethical Use Guidelines

Users must conduct themselves ethically and responsibly when using Jeffcom systems. Eight basic and generally accepted ethical guidelines should govern your actions.

- Do not use Jeffcom systems or devices to cause harm.
- Do not interfere with the work of others.
- Do not pry or meddle in other's files.
- Do not use Jeffcom systems to commit or facilitate criminal activity.
- Do not install, copy, or use unlicensed or unauthorized software.
- Do not steal or misuse intellectual property.
- Do not impersonate another individual.
- Do not access, review, or modify Jeffcom computing resources without authorization.

Accountability and User Responsibilities

Users are accountable for all actions taken using Jeffcom information resources assigned or made available to them.

Users shall:

- Act in an ethical, informed, and trustworthy manner;
- Remain alert to cybersecurity threats, including malware and phishing;
- Complete required IT security awareness and training programs;
- Install only software approved by Jeffcom IT;
- Comply with all software licensing terms and applicable copyright laws;
- Understand that Jeffcom systems may be monitored and that there is no expectation of privacy when using Jeffcom IT resources; and
- Report all cybersecurity, privacy, or data-handling incidents immediately.

Users shall also safeguard their accounts by:

- Locking or logging out of devices when unattended;
- Using strong, complex passwords on all Jeffcom systems, in accordance with Jeffcom password requirements;
- Assisting with the remediation of security incidents, regardless of fault;

- Notifying Jeffcom IT promptly of changes in role, assignment, or employment status;
- Complying with rules of behavior when accessing external systems; and
- Reading and understanding system banners and end-user license agreements.

Information Integrity

Users must protect the accuracy, completeness, and reliability of Jeffcom information.

This includes:

- Ensuring data is accurate, complete, and current;
- Completing required training before entering or modifying data;
- Properly handling confidential and sensitive information, including personally identifiable information (PII) and criminal justice information (CJI), which must be encrypted and shared only on a need-to-know basis;
- Protecting systems from malicious code by applying required updates and discontinuing system use at the first sign of compromise; and
- Never knowingly entering false, misleading, or unauthorized information into any system.

System Access

Users shall access Jeffcom systems only as required to perform their assigned job duties and shall protect their access credentials from misuse.

Users shall:

- Be responsible for all activity conducted under their user ID;
- Never share passwords or authentication credentials;
- Follow approved procedures for system access and information sharing; and
- Access only systems, files, and applications for which authorization has been granted.

Users shall not:

- Provide information to individuals who lack proper authorization;
- Store sensitive or confidential information without appropriate access controls;
- Use their trusted position and system access for personal benefit or for any reason other than the performance of their official duties;

- Browse or access other users' files without authorization; or
- Use peer-to-peer (P2P) filesharing technologies.

Software Use

Users may not install or use unauthorized software, including freeware or shareware, on Jeffcom-owned devices without approval from Jeffcom IT or management.

Users shall not:

- Use Jeffcom-licensed software on personal or non-Jeffcom systems without authorization;
- Modify system configurations, including installing or removing hardware or software, without approval; or
- Run security or diagnostic tools that could expose system vulnerabilities unless expressly authorized.

Jeffcom-issued Equipment

Jeffcom-issued equipment is for official Jeffcom business only. Users must take reasonable precautions to protect equipment from loss, theft, or damage.

Users shall:

- Protect equipment from theft, damage, and misuse;
- Report lost or stolen equipment immediately to Jeffcom IT; and
- Return all Jeffcom-issued equipment upon separation or reassignment.

Users shall not:

- Connect unauthorized hardware or media to Jeffcom devices;
- Leave devices unattended or unsecured;
- Deface or alter Jeffcom equipment; or
- Take Jeffcom-owned devices outside the United States without authorization from management, IT oversight, and appropriate service-plan coordination.
- Remove Jeffcom-owned devices that store or provide access to PII or CJI from Jeffcom premises unless encryption has been applied and approved by Jeffcom IT;

Mobile Devices

Additional safeguards are required when using Jeffcom-issued mobile devices.

Users shall:

- Maintain required security software and updates;
- Use passwords or PINs and automatic lock timeouts;
- Install only approved applications;
- Protect data stored on mobile devices; and
- Report lost or stolen devices immediately.

Users shall not:

- Download Jeffcom data to personal devices;
- Leave devices in unsecured locations;
- Use Jeffcom mobile devices for personal calls, messaging, streaming, or web browsing unrelated to official duties;
- Connect to unsecured Wi-Fi networks without IT approval; or
- Access or store PII or CJI on Jeffcom-issued mobile devices outside Jeffcom facilities unless approved encryption is in place.

Teleworking

Remote work increases security risks. Users must take additional precautions when accessing Jeffcom systems outside Jeffcom facilities.

Users shall:

- Secure home or remote networks using strong passwords and basic security controls; and
- Prevent unauthorized viewing of Jeffcom information in public or shared spaces.

Users shall not:

- Use unapproved hardware or storage devices;
- Leave devices unsecured; or
- Allow any other person to use Jeffcom-issued equipment.

Email Use

Jeffcom email systems are monitored and are intended primarily for official business. All email created or stored on Jeffcom systems is Jeffcom property and may be a public record.

Users shall not use Jeffcom email to send, receive, retain or proliferate content that is fraudulent, marketing anything, harassing, offensive, sexually explicit, racist, sexist or otherwise inappropriate. Do not forward or solicit jokes, pictures or inspirational stories. Do not send email to large email distribution groups or use "Reply All" to large groups unless required.

Emails containing PII or CJI sent outside the jeffcom.us domain must be encrypted. Users may force encryption by adding **[SECURE]** to the beginning of the email subject line.

De minimis personal and casual use of Jeffcom email systems is permitted if it is infrequent, brief, and does not interfere with official duties, but it is discouraged because such messages are archived and potentially public records.

Passwords

Users are responsible for safeguarding their authentication credentials.

Password best practices include:

- Using long, complex passwords or passphrases;
- Avoiding dictionary words and personal information;
- Memorizing passwords rather than writing them down; and
- Changing passwords when required or if compromise is suspected.

Portable Storage Devices

Use of removable media is restricted and must be authorized by Jeffcom IT.

Users shall:

- Encrypt removable media taken outside Jeffcom facilities;
- Properly label and store media according to data sensitivity;
- Protect media from loss or theft; and
- Ensure media is sanitized by Jeffcom IT before disposal or reuse.

Incident Reporting

All security incidents must be reported immediately to Jeffcom IT. A security incident may include misuse, lost or stolen equipment, privacy incidents, criminal activity or insider threat.

Users shall:

- Take reasonable steps to limit damage upon discovering an incident; and
- Cooperate fully with investigations and response actions.

Incidents may be reported by phone or email to **itstaff@jeffcom911.us**.

Social Engineering Awareness

Social engineering is the psychological manipulation of people into performing actions or divulging confidential information. Users must remain vigilant against social engineering attempts and shall not disclose sensitive information to unverified sources.

Users shall verify identities, refuse unsolicited requests for information and report suspected incidents immediately. Messaging applications may not be used for Jeffcom business unless explicitly approved.

Public Records

Most uses of Jeffcom computers and communications devices create and modify public records. These public records are subject to the retention schedules published by the State Archivist of the Washington Office of the Secretary of State. Additional information regarding emergency communications and 911 records is available at:

> https://www.sos.wa.gov/archives/help-government-agencies/managing-emergency-communications-911-records

These public records are also subject to the Washington State Public Records Act, Chapter 42.56 RCW:

> https://app.leg.wa.gov/rcw/default.aspx?cite=42.56

Users shall assume that all information created, transmitted, or stored using Jeffcom computer and communication systems is subject to the Public Records Act and related legal requirements.

Requirements for the creation, retention, redaction, release, and disposition of public records are governed by applicable laws and Jeffcom policy and are beyond the scope of this agreement. Users are responsible for consulting Jeffcom's public records officer, relevant Jeffcom policies and procedures, applicable retention schedules, and legal counsel as needed.

Resources Authorized for Personal Use

Jeffcom may explicitly authorize certain computer systems and resources for personal use, including standalone PCs and guest Wi-Fi. These systems are separate from mission-critical systems. Personal use may be restricted or discontinued to protect Jeffcom business operations or network performance.

Personal use is permitted only when it does not interfere with official duties, consume excessive resources or reflect poorly on Jeffcom. The provisions of this policy apply to personal use – notably Prohibited Activities, Ethical Use Guidelines and security requirements. Restrictions on personal use during working hours are determined by supervisors and management based on operational needs.

Connecting a personal device to guest Wi-Fi is preferable to using a standalone for personal use, though both are generally authorized. Standalones are provided primarily to access Jeffcom email and internet-based systems used for Jeffcom business.

Users are encouraged to access personal email accounts through a standalone or guest Wi-Fi rather than using Jeffcom email systems for personal or casual communication. Personal email accounts shall not be used to conduct official Jeffcom business. Any message sent or received in a personal email account that relates to Jeffcom business must be forwarded to the user's Jeffcom email account to ensure retention as a public record.

User Agreement and Acknowledgment

All Jeffcom employees, contractors, volunteers, and any other personnel who are granted access to Jeffcom IT systems or data must read and acknowledge this policy agreeing to the following:

- I will abide by the Jeffcom Policy on Use of Communications and Computer Systems and its rules of behavior for the use of Jeffcom communications, computer systems, and information resources.
- I will use Jeffcom communications, computer systems, and information resources only for authorized Jeffcom business and in accordance with my assigned job duties, except authorized personal use.
- I will use IT resources for personal use appropriately and only where specifically authorized, will not let personal use adversely affect performance of official duties and understand that personal use may be restricted or discontinued.
- I will comply with all Jeffcom policies, procedures, ethical standards, and system-specific rules governing the use of information technology resources.
- I will access only those systems, files, applications, and data for which I have been explicitly authorized.

- I will protect my user accounts, authentication credentials, and access privileges, including the use of strong, complex passwords, and not share credentials with any other person.
- I accept that Jeffcom systems may be monitored, logged and audited, including those authorized for personal use, and that I have no expectation of privacy when using Jeffcom information technology resources.
- I will complete all required information-security-awareness training and any role-based or system-specific training required for the systems to which I am granted access.
- I will protect sensitive, confidential, personally identifiable information (PII), and criminal justice information (CJI) data in accordance with Jeffcom policy, including encryption requirements.
- I will promptly report any suspected or confirmed security incident, privacy incident, misuse, loss of equipment or policy violation to Jeffcom IT.
- I will safeguard Jeffcom-issued equipment and return all equipment upon separation, reassignment, or when access is no longer required.
- I will notify Jeffcom IT when my access to any system is no longer needed due to a change in duties, employment status or extended non-use.
- I will not attempt to access, modify, disclose, or use information or systems for which I do not have authorization.
- I will not bypass, disable, or attempt to defeat security controls or safeguards.
- I will not introduce unauthorized software, hardware or storage media into Jeffcom systems or networks.
- I will not disclose, without authorization, any sensitive, confidential, PII or CJI data accessed or learned through my duties.
- I understand that my use of Jeffcom systems, including personal use, will almost certainly create public records that are subject to complex legal requirements.
- I understand that failure to comply with these requirements may result in disciplinary action, revocation of system access and legal consequences.
- I understand that this agreement and acknowledgment does not relieve me of responsibility to remain informed of, and comply with, all applicable Jeffcom policies and procedures.

_____

Signature Date