Information Services Policies
Table of Contents

1. Introduction

Computer information systems are an integral part of Kittitas County's daily operation. These policies have been approved by the Board of County Commissioners (BOCC) in Resolution 2009-____ in order to:

- Maintain the systems used to provide services to the citizens of Kittitas County and protect the substantial human and financial resources invested to create and maintain these systems.
- Safeguard the information contained within these systems.
- Minimize business and legal risk.

Violations

Violation of these policies by any employee may result in progressive disciplinary action, revoked network access, and possible criminal investigation in accordance with Kittitas County policy and applicable laws.

Administration

The Information Services (IS) Director is responsible for the administration of these policies.

Employee responsibilities

Managers and supervisors must ensure all personnel are aware of and comply with these policies.

Employees must:

1. Read, understand, and follow these policies.
2. Contact their supervisor or IS if they have any questions about these policies.

IS responsibilities

The IS Director must:

1. Develop and maintain written standards and procedures necessary to ensure implementation of and compliance with these policies.
2. Provide appropriate support and guidance to assist employees to fulfill their responsibilities under these policies.

2. Requests for Service

IS will track and prioritize all requests for assistance.

IS staff will prioritize requests for service based on the level of impact to the county and its citizens, urgency, and criticality. The IS Director is responsible for resolving prioritization conflicts.

IS will process service requests within 30 minutes during normal business hours from the time submitted unless the request is an emergency.

Usage

All employees requesting non-emergency assistance are required to use the service request system. The benefits of using the system are immediate submission to all available IS staff, and quick routing to, efficiency of, and response by the appropriate IS staff.

Tracking

All requests will be tracked to:

- Show patterns and areas of additional need.
- Allow employees and IS to track progress of service.
- Allow employees to interact with the assigned technician, update, or close a request as needed.

For more information see SOP IS-G0004.

Employee responsibilities

Employees must:

1. Use the service request system for all non-emergency requests.
2. Use any communication means appropriate for emergency requests.

IS responsibilities

IS staff must:

1. Track and prioritize all requests for assistance.
2. Acknowledge all requests for service within 30 minutes during normal business hours from the time submitted.

3. Purchasing Technology

For the purpose of this policy, **technology purchase** refers to any electronic item with a cost over $50 that connects to the network or a computer connected to the network.

All technology purchases will be made or reviewed by IS. Non-technology purchases for other departments will not be made by IS.

Examples of technology purchases are:

- Internal computer components
- Mice
- Keyboards
- Network devices: Wi-Fi access points
- Printers
- Off the shelf software and hardware
- External drives (portable hard drives, CD/DVD, network attached storage)
- USB devices (excluding flash drives)
- Camera (review only)
- Cell phones (review only)
- Copiers (review only)

Examples of non-technology purchases are:

- Flash drives, device memory cards
- CDs/DVDs
- Toner

Funding

- One-time costs will be funded by the department.
- Ongoing costs to the department must be approved by the DH/EO.
- Ongoing costs to county funds must be approved by the BOCC.

Software

All software installed on any computer owned by the county will be stored in and maintained by the IS department. IS will ensure compliance with software copyrights and licenses. For more information see SOP IS-G0003.

Inventory

- IS maintains inventory of all technology purchases, regardless of funding source.
- As with all purchases made with county funds, the inventory is owned by the BOCC.
- The DH/EO is responsible for maintaining the custodianship of all technology residing within their department.
- Disposal of all technology must go through IS.
- IS will ensure ALL data storage devices (including flash drives) are destroyed or erased prior to disposal/disposition.

Employee responsibilities

Employees must:

1. Make all technology purchases through IS.
2. Protect any county resources in their custody.

IS responsibilities

IS staff must:

1. Make all technology purchases.
2. Maintain inventory of all technology purchases.

4. Account Management

For the purpose of this policy, **account** will mean a user name and password combination used to access a computerized system.

Passwords

User names, passwords, and access codes assigned for the use of county technology are confidential.

1. Employees are responsible for any activity associated with their account.
2. Strong passwords are required. Passwords must include both alpha and numeric characters with a minimum length of nine (9) characters.
3. Employees will not allow Internet Explorer or any other software to store passwords. Encrypted password management software is exempt.
4. County network passwords will expire every 90 days and must be changed.
5. Employees will not disclose account passwords to anyone.
6. If an employee suspects their password has become known to others, the employee must notify their DH/EO and IS immediately.
7. Passwords will not be recorded in an unsecured location.
8. Entering a password incorrectly three times will automatically lock the employee's county network account. After a period of 15 minutes of inactivity the county network account will be automatically unlocked.
9. Passwords used to access county resources will not be identical to passwords used to access non-county or personal resources such as web sites, email accounts, state services, etc.
10. Upon termination, employees must disclose all passwords used to protect county data to their supervisor. See also Data Management and Protection.

Shared accounts

A **shared account** is one account with access shared among multiple employees, e.g. a department's public email mailbox. Shared accounts are not allowed unless a strong business case is made and the risks accepted by the DH/EO.

Group membership

A group contains users who will receive email mailed to the group (distribution list) or have access to network resources (security group).

- One individual (or position) will be designated as the owner of the group.
- The group owner will request membership changes of IS.

Changes to accounts

- HR will verify employment or personal information changes and request IS account updates, e.g., terminations, transfers, name changes.
- DH/EO will request account access changes, e.g., promotion, temporary assignment.

Account creation

- New accounts will be created in accordance with SOP IS-N0001.
- User names will be created as *first.last* name.

- An email account will be created for each new employee who has access to a computer unless the Pre-orientation Checklist directs otherwise.
- New user orientation is conducted by HR. Users must go through the IS security presentation at first login to the network during the new user orientation.

Terminated employees

- DH/EO will notify IS of terminated employees using the Notification of Separation from Service form.
- DH/EO will notify IS of high risk terminations concurrent with the termination (see High Risk Terminations).
- IS will disable a terminated employee's accounts after the last day worked as notified by the Notification of Separation from Service form.
- The employee's account (including email, see Email) will be deleted 30 days after termination.
- See SOP IS-N0002 Terminated Employee Checklist for more information.

IS staff

In the event an IS staff member is terminated, immediately after their last day worked IS will:

- Disable the staff member's county network account.
- Change passwords on the staff member's accounts.

Also see Physical Access.

High risk terminations

Classifying a high risk termination is at the discretion of the DH/EO or designee. High risk terminations will be handled by IS via use of the High Risk Termination Form. For more information see SOP IS-N0003.

Employee responsibilities

Employees must:

1. Ensure passwords are secure and confidential.
2. Notify IS and their DH/EO if they suspect their password has become known to others.
3. Not use county passwords for non-county or personal resources.

DH/EO responsibilities

DH/EO must:

1. Send employment or personnel account change information to HR.
2. Send account access changes through IS service requests.

IS responsibilities

IS staff must:

1. Set employee county network passwords to expire every 90 days.
2. Configure network security to require strong passwords when possible.
3. Immediately change passwords on or disable any account where the password is thought to be compromised.
4. Maintain one user as the owner for each group account.
5. Only accept employment or personnel account change information from HR.

6. Only accept account access changes from the employee's DH/EO.
7. Name accounts using the standard *first.last* naming convention.

5. Access

Remote access

County employees

CAMAS, NOVAtime, and county email may be made available from the Internet through https://camas.co.kittitas.wa.us. Utilization of this system does not supersede management's right to set work hours and location, nor ownership of data or work products.

Access to additional network resources may be permitted from a remote location (e.g. home, field or business travel via a personal computer or laptop) provided the following requirements are met:

1. Requests for remote access must be made by the employee's DH/EO.
2. Employees must ensure their personal equipment meets county standards outlined in Personal Equipment.
3. Remotely connecting to the network is an employee's acknowledgment and agreement that they are connecting to the county network at their own risk and the county is not responsible for any damage that may result to their device.

Vendors

Vendors must complete a Confidential Information Agreement - Vendor Remote or On-Site Support before access to their software will be provided. After a signed agreement is received, IS will create a vendor account. Vendor accounts will remain disabled by default. Upon request by a county employee, IS will enable the vendor account for a temporary session until 5:30 pm the next business day unless a longer period of time is required to resolve the issue.

Local access

Access to data will be limited to those resources required for an employee to perform their job. For more information on local access see Data Management and Protection.

Physical access

Physical access to the IS office is controlled by proximity-card authentication. Access will be restricted to IS staff, commissioners, and designated maintenance employees unless approved by the IS Director or a commissioner.

Doors

- Exterior exit door will remain locked at all times.
- Interior entrance door will be locked during non-office hours. During office hours, it will remain locked while IS staff is not present and may be unlocked while IS staff is present.

Restricted areas

There are two restricted areas in the IS office: the server room and the storage room. Restricted area doors will remain locked and closed at all times unless IS staff is physically present.

County employees

- Non-restricted areas: employees are allowed access unsupervised.
- Restricted areas: employees are allowed access with IS staff visual supervision.

Non county employees

- Non-restricted areas: non-employees are allowed access with employee supervision.
- Restricted areas: non-employees are allowed access with visual supervision by IS staff or IS director approved maintenance staff. Arrangements for access outside business hours must be made at least 48 hours in advance.

Terminated employees

Immediately upon termination of any employee having physical access to IS, access codes will be changed.

Employee responsibilities

Employees must:

1. Notify IS, with at least 48 hours notice, when a vendor needs physical access.
2. Notify IS when a vendor needs remote access.
3. Prevent non-employee access to IS without county employee supervision.
4. Prevent non-employee access to IS restricted areas.

IS responsibilities

IS staff must:

1. Ensure a vendor NDA is signed prior to creating a vendor account for remote access.
2. Enable remote access for existing vendor accounts in a timely fashion when requested by an employee.
3. Keep restricted area doors closed and locked.
4. Lock interior entrance door when IS staff is not present.

6. Personal Equipment

Personal equipment is any equipment (wired or wireless, including but not limited to computers, USB, Bluetooth, serial devices, flash memory, portable storage, MP3 players, etc.) not owned by the county, another government agency, or by contract through which county business is conducted.

Attaching to the network

Personal equipment may be connected to the county network only via remote access at the request of the employee's DH/EO, and when approved by IS.

Personal equipment attached to the network via remote access must meet the following requirements:

1. Employees must have installed current critical and security updates for their operating system (Microsoft update for Windows OS).
2. Employees must follow safety and security measures required in this policy, i.e., password protections on the system and on files pertaining to Kittitas County business.
3. The system must not be set up to store passwords automatically.

Vendor owned equipment

Vendor owned equipment must meet all requirements under Attaching to the network. For vendor remote access, see Access.

Visitor owned equipment

Visitors engaged in business with the county, e.g., trainers and guest presenters, must meet all requirements under Attaching to the network when connecting personal equipment directly to the network. By connecting they acknowledge that they are connecting to the county network at their own risk and the county is not responsible for any damage which may result to their device.

Portable storage devices

Portable storage devices including but not limited to, laptop computers, flash (USB) memory, cell phones, MP3 players, and portable hard drives, expose the county to security risks such as:

1. Loss/misplacement/theft of device and data.
2. Viruses and malware.
3. Multiple copies of documents creating possible version conflicts; see Data Management and Protection.
4. The possibility for third parties to reconstruct files after they have been deleted.

Employees will not copy county documents or data to personal portable storage devices. If transportation of documents or data is required, a county owned portable storage device will be used. For more information, see Data Management and Protection.

Cell phones

Cell phones used to conduct county business (including but not limited to placing phone calls, instant messaging, and reading or sending email) are subject to public disclosure laws and the phone and records may be searched and/or seized.

With DH/EO written approval, employees may connect their mail-enabled personal cell phone to the county's email system. In so doing the employee acknowledges:

1. The phone and records may need to be produced for public disclosure requests with or without their knowledge or consent.
2. The phone must be password protected to prevent unauthorized access to the county system.
3. If lost or stolen, they must immediately notify IS, and IS will take all steps necessary to secure the county network from the device.
4. They are connecting to the county network at their own risk and the county is not responsible for any damage which may result to their device.

Repairs

As an employee of the county, IS staff will *not* work on an employee's personal computer or equipment except for minimal phone troubleshooting for issues relating to remote electronic access.

As an independent contractor, IS staff may not work on an employee's personal computer or equipment for any issue related to county business (see Kittitas County Personnel Policy Manual (4-5) Outside Employment).

Employee responsibilities

Employees must:

1. Not connect personal equipment to the county network unless by a method approved in these policies.
2. Not copy county documents or data to a personal storage device.

IS responsibilities

IS staff must:

1. As an employee of the county, provide phone troubleshooting for employee's personal equipment related to remote access.
2. As an independent contractor, not work on an employee's personal equipment for any issue related to county business.

7. Data management, access, and protection

For the purpose of this policy, **data** are electronic files, i.e., any electronic document, database or report. **Electronic records** are any data used or created in the course of doing county business. It is Kittitas County policy to protect data from loss, misuse, destruction, theft, unauthorized access, and environmental hazards. Every employee shares in the responsibility for the security of data by following this policy.

Stored electronic records

All electronic records will be stored in a network storage location where they will be backed up and protected.

If working on an electronic record not stored on a network file server (such as on a laptop or a copy of a record stored on the network), the most recent version must be added to the server at the earliest opportunity.

G drive – Department

Electronic records that are departmentally accessible will be stored on the department's network storage location (G drive) in subfolders by subject and retained as provided in the department's document retention schedule. All department personnel have full read/write access to the department drive unless a change is requested by the DH/EO or their designee.

H drive – Secure

Secure electronic records will be stored in the employee's secure network storage location (H drive). Only the employee has access to their secure drive; however, as with all documents, these documents are subject to public disclosure and may be accessed by the employee's DH/EO or IS staff as directed by the Request for Access to Network Records form or court order. All employees will have an H drive unless a change is requested by the DH/EO or their designee.

T drive – Teams

Electronic records to be shared with other departments will be stored in the teams network storage location (T drive). IS will create the folder and set permissions before files may be added.

Additional locations

Some software applications may require a data store in a location specific to the application. Copies of such data are not required to be stored on the G, H, or T drives.

Access to stored data

Prior to granting access to any current employee's data in a local or network storage location, including email and data regarding the employee's network and internet usage, the Request for Access to Network Records form must be completed.

System access

A system is a software application (e.g., Cashtax and Cayenta) or file store (e.g., T drive subfolder) accessed via the county network and administered by a county department. IS will grant access to an employee under the following conditions:

1. A new employee begins work in a department that administers the software, as directed by the DH/EO or designee via HR Pre-Orientation form or IS service request.
2. An employee from a department other than the one who administers the system, upon approval of the DH/EO, via IS service request, of the department who administers the system.
3. Contractors, see Access, Vendors.

The Kittitas County Information systems and their component software and hardware are the property of Kittitas County. The records, files, and data of an office headed by an independently elected official are within the exclusive control of that elected official, while acting in that capacity, and shall transfer to either a subsequently elected official for that office or the Kittitas County Board of Commissioners in the absence of an elected official. Access to any records, files, or data under the control of such elected official is at the sole discretion and authority of said elected official. Access to, and sharing of such records, files, and data as necessary for the completion of work by other departments or offices shall not be unreasonably withheld. Disputes arising out of this policy shall be resolved by the Kittitas County Board of Commissioners who shall have the final authority over the dispute.

If allegations of misconduct involve an elected official, the Human Resource Director and Prosecutor must make a joint recommendation to the Board of County Commissioners to override this policy, based upon a determination that no other reasonable alternative to conduct an investigation without access to such records exists, and provide documented direction to IS via the Request for Access to Network Records form.

This policy will not supersede federal or state law governing access to data, e.g. criminal justice and health records.

Data access

Public disclosure

All public disclosure requests will be processed by the DH/EO, or their designated Public Disclosure Officer, of the department maintaining the requested record. IS will facilitate by providing access to records upon the DH/EO completing the Request for Access to Network Records form.

County email, like all other public records, is subject to public disclosure laws and may be disclosed without prior consent or knowledge of the sender or the receiver.

Investigations

Access to county data may be granted without the DH/EO's knowledge or consent:

1. As ordered by a court of law and as advised by the Kittitas County Prosecutor.
2. As governed by the Request for Access to Network Records form.

Auditing

Kittitas County reserves the right to audit all activity on the county network. Access to audit information is governed by the Request for Access to Network Records form.

Terminated employees

Upon termination, IS will provide the DH/EO or designee access to the employee's secure files (H drive) and email. It is the responsibility of the DH/EO to ensure retainable electronic records are moved into the appropriate location as defined in the county's record management policy. IS will delete the mailbox after 30 days. Upon termination, IS will prepare the terminated employee's computer for reassignment. Also see High Risk Terminations.

Backups

IS will backup all data stored on the county network servers on a routine basis. The backups will be maintained in a secure location. The backups are not the primary or secondary copy of the records and as such are not subject to public disclosure request searches. Backups are not a data storage system; they are for business continuity and disaster recovery only. For more information see SOP IS-N0004.

UPS and surge protectors

All servers on the county network will be maintained in the IS server room. All servers will be powered through a UPS (uninterruptable power supply) that conditions the power supplied to the server room protecting hardware and data from power related corruption. In the event of a power outage, the UPS will power the servers while they shut down automatically.

All computers must be plugged into a surge protector.

Locking computers

All employees must maintain the security of their computer and the county network from unauthorized access. When stepping away from control/view of their computer, employees will lock or log out of their computer. All computers will have the Windows Screen Saver set to engage after a maximum of 10 minutes of inactivity and require logon on resume. Computers in locations secured from view and physical access are exempt.

Temporary file deletion

Temporary files are defined as files IS makes in the course of troubleshooting and computer migration. IS will delete temporary files when they are no longer needed.

Transportation of county data

Employees who copy and transport data outside the county network must do so only on county equipment and are responsible for protecting that data and media from loss, misuse, destruction, theft, unauthorized access, and environmental hazards.

Physical transportation

Physical transportation is defined as copying data to removable media.

1. Employees will ensure that data transported on any portable storage device (not limited to flash memory, portable hard drives, laptops, CDs, DVDs) are encrypted. IS will provide tools and assistance for encryption.
2. Upon termination, employees must decrypt any encrypted data or disclose encryption passwords to their supervisor.
3. Portable storage devices must be stored in a secure location when not in use.
4. Environmental hazards to hardware, such as food, smoke, liquids, high or low humidity, direct sunlight, magnetic fields, and extreme heat or cold, must be avoided.

Electronic transportation

All confidential information must be encrypted when transported across any unsecure network. Many commonly used systems such as external email must not be considered a secure way to transport confidential information.

Destroying and erasing media

Destruction of physical media means to damage the media making its data unreadable and unrecoverable by any means. **Erasing media** means making data unrecoverable.

- After backup media has passed its overwrite protection period it may be destroyed, erased, or overwritten by IS staff, and will not be searched for data.
- Hard drives and removable media will be erased or destroyed by IS before being removed from county inventory.
- Optical disks (including software) will be destroyed when removed from county inventory. Documents containing license information must also be destroyed.

DH/EO responsibilities

DH/EO must:

1. Use the Request for Access to Network Records form if access to a current employee's files is required.

Employee responsibilities

Employees must:

1. Store data on a network file server in the appropriate location.
2. Lock computers when away from control/view and configure Windows Screen Saver to lock after 10 minutes of inactivity and require logon on resume.
3. Encrypt data on portable devices.
4. When being removed from county inventory, send any technology equipment or any media used for data storage to IS for proper disposition.

IS responsibilities

IS staff must:

1. Require use of the Request for Access to Network Records form to provide access to current employee's files.
2. Backup all data stored on the network servers as scheduled, and maintain them in a secure location (see SOP IS-N0004).
    a. Monitor backup log files and correct or repair failures.
    b. Test a restore from backup at least quarterly.

3. Maintain all county servers and ensure they are protected by a UPS.
4. Delete temporary files when they are no longer needed.
5. Destroy or erase storage media when removed from inventory and destroy license information for destroyed software.

8. Email

For the purpose of this policy, **county email** is defined as any email message including attachments that meet any of the following criteria:

1. Sent or received through the county email system.
2. Conducting county business.
3. Sent or received by an employee acting on behalf of the county, regardless of the email system used.

County email must be sent and received via the county email server. Exceptions are for IS staff troubleshooting email issues. If the county email server is unavailable and email communication is required to conduct essential county business, staff may utilize other email systems provided the email records are maintained on the county network.

Email is a document and is subject to public disclosure laws, documents retention schedules, investigations, and auditing.

Security

All confidential information must be encrypted when transported across any unsecure network.

Retention

Email retention is, like all other public record retention, based on content. DH/EOs are responsible for setting their document management policies and following the document retention schedule of the Secretary of State or setting their custom retention schedule.

Access

County email is the property of Kittitas County. Kittitas County reserves the right to access any county email for any and all purposes including but not limited to public disclosure, investigations and auditing. See Data Management and Protection.

Terminated employees

After an employee's separation from service, IS will provide the DH/EO access to the employee's email as directed on the Separation Notice form. IS will delete the terminated employee's mailbox after 30 days.

Personal email

Employees must not use their county email account for personal use.

SPAM and junk-mail filtering

Kittitas County provides email filtering of county email accounts. Employees are responsible for monitoring the filtered messages for mistakenly filtered email. Employees shall delete any SPAM or junk-mail filtered or received.

Phishing

Phishing is the criminally fraudulent process of attempting to acquire sensitive information such as user names, passwords, or credit card details by masquerading as a trustworthy entity in an electronic communication or via telephone.

Employees shall not click on unknown or unexpected links or provide any sensitive information (e.g. user name, password, and account numbers) via email, telephone, or web page without verifying that the requestor and method are authentic.

Attachments

Kittitas County limits attachment size. The recipient's email system may also place a size limit on emails (including attachments). If you need to send a file larger than the limit, see SOP IS-G0002.

Storage

1. Auto archiving is prohibited.
2. Email may only be stored on the Exchange server in an employee's mailbox or as an MSG file on a network file share.

Shared email accounts

A **shared email account** is defined as multiple users having access to one email account, i.e., access to accounts listed on the county's public web site: department_name@co.kittitas.wa.us.

1. Access to shared email must be requested by the DH/EO.
2. Group email access will be limited to three individuals.

DH/EO responsibilities

DH/EOs must:

1. Set their document management policies and follow the document retention schedule of the Secretary of State or set their own retention schedule.
2. Process public disclosure requests for email maintained by their department.
3. Request access to shared email for each required employee from IS.

Employee responsibilities

Employees must:

1. Send and receive county email through a county email account.
2. Retain county email based on content according to their department's retention schedule and document management policy.
3. Not use county email for personal use.
4. Monitor filtered messages for mistakenly filtered email.
5. Delete any SPAM or junk-mail received.
6. Not click on unknown or unexpected links or provide sensitive information unless the requestor and method are authenticated.
7. Not auto archive county email.
8. Store county email on the Exchange server in their mailbox or as an MSG file on a network file share, and not in PST files.
9. Not transmit copyrighted materials without permission of the copyright owner.
10. Encrypt confidential information sent via email.

IS responsibilities

IS staff must:

1. Facilitate processing public disclosure requests by providing departmental access to email accounts.
2. Provide investigative and audit access based on an approved Request for Access to Network Records form or valid court order.
3. Provide DH/EO access to their terminated employee's email as directed on the Change of Service form.
4. Delete terminated employees' mailboxes after 30 days.
5. Limit group email access to three individuals.

9. Internet

Access to the Web is provided to employees for the benefit of Kittitas County. Misuse or abuse may result in terminating an employee's access, progressive disciplinary action, and termination.

Acceptable use

See the Technology Use section of the Kittitas County Personnel Policy Manual for acceptable use.

Unacceptable use

Employees must not use the Internet for purposes that are illegal, unethical, or may be harmful to Kittitas County.

Internet communications

No Internet communications method, except those hosted on the county's network, may be used to conduct county business unless a contract, interlocal agreement, RCW, federal, or Washington State agency governs or provides for the service. This includes, but is not limited to the following:

1. Instant messaging
2. Blogs
3. Forums
4. Twitter
5. Social networking (MySpace and Facebook)
6. Media hosting sites (YouTube, PhotoBucket, Blip.tv)

Streaming media

Streaming media for non-Kittitas County use or personal use is prohibited. Use of streaming audio or video e.g. online radio, Real Audio, YouTube, Hulu, and Windows Media Player is limited to business use only.

Downloads

Employees will not install software downloaded from the internet unless it is in the IS approved Internet Software Download List (SOP IS-G0003).

IS staff exemption

IS Staff are exempt from these internet use policies for the purpose of testing and evaluating technologies for benefits from use by the county so long as the use is not illegal, unethical, or harmful to Kittitas County.

Internet Safety

See malware and viruses and the Safe Computing Best Practices SOP IS-G0008.

Monitoring

All Internet activity may be logged. Kittitas County reserves the right to monitor all activity traversing its network. Investigatory access to county data is governed by the Request for Access to Network Records form.

Employee responsibilities

Employees must:

1. Not misuse or abuse Internet access.
2. Not use streaming media for non-county business or personal use.
3. Not install downloaded software unless it is on the approved list (SOP IS-G0003).
4. Not click on unknown links or visit non-trusted Web pages.

IS responsibilities

IS staff must:

1. Maintain a list of software approved for download and installation.
2. Provide access to county data as governed by the Request for Access to Network Records form.

10. Viruses and Malware

Computer viruses and **malware** are programs designed with the malicious intent to infiltrate and/or damage a computer system without the owner's informed consent. IS shall maintain appropriate hardware and software security systems to guard against virus and malware intrusions.

All county employees will practice safe computing by scanning removable media, not knowingly introducing a virus, and not clicking on links or visiting non-trusted web pages. For more safe computing practices, see SOP IS-G0008.

If virus or malware infection is suspected, employees must notify IS immediately.

Any expense incurred due to the negligent or malicious use of county technology will be paid by the employee at the actual rate of expense. Outstanding debt may be recuperated through payroll deduction without the prior consent of the employee.

Employee responsibilities

Employees must:

1. Not knowingly introduce a virus into Kittitas County computers or network.
2. Scan incoming memory media (e.g. diskettes/CDs/DVDs/USB devices) for viruses before they are read.
3. Discontinue computer use and immediately contact IS if they suspect their workstation has been infected by a virus or virus protection software is disabled or suspected to be not up to date.
4. Not click on unknown links or visit non-trusted Web pages.

IS responsibilities

IS staff must:

1. Install and maintain appropriate anti-virus software on all computers and servers.
2. Respond appropriately to infections and intrusions. May include a quarantine of affected systems, destroying detected viruses, and repairing or destroying infected files.
3. Install all security related software patches in a timely manner. May include integration testing.
4. Ensure all applications developed in-house follow best practices to guard against known malicious attacks and intrusion methods.

11. Web policies

Kittitas County maintains a Web presence to facilitate communication to the public of its services.

Content is defined as what is presented, e.g., text, images, video, audio, and downloadable files.
Design is defined as how content is presented, e.g., the look and feel.

Roles

The Board of County Commissioners

The BOCC owns the county online presence in all forms, e.g., Web sites, user names, and email addresses. Only authorized persons may create, use, or promote any online presence intended to represent Kittitas County or a division thereof. The BOCC controls and is responsible for the content of any online presence and the design of the county Web sites.

The Information Technology Committee (ITC)

The ITC operates as an advisory board to the BOCC and is under its direction. The ITC oversees the county's web sites and ensures adherence to these policies.

Webmaster

The IS Application Development Manager acts as webmaster for all county Web sites, takes direction from the IS Director, and is a member of the ITC. The webmaster is responsible for overseeing and prioritizing development of the web sites and its supporting systems, and for the security of the web site. All content published to the county's Web sites will be uploaded by or in conjunction with the Webmaster.

Department Head/Elected Official (DH/EO)

Each DH/EO is responsible for the content within their area of operation as defined by this policy. The DH/EO or designee must approve all content and ensure it complies with these policies before it is put on their Web page.

Kittitas County web sites

http://www.co.kittitas.wa.us is the county's official web site. All public Web content will be placed within the co.kittitas.wa.us domain, except as provided within this policy.

http://www.kittitascountyfair.com is the official Kittitas County Fair Web site. The Fair Program Director, as advised by the Kittitas County Fair Board of Directors, and under the direction of the BOCC, is responsible for its content. The fair site will follow all publishing policies set forth in this document; however exception is granted to allow a distinctive design, information about Kittitas County Fair sponsors, and a hyperlink to each sponsor's official Web site.

http://www.kittitasvalleyeventcenter.com is a pointer domain that automatically redirects to the official KVEC Web site at http://www.co.kittitas.wa.us/kvec/ where the Kittitas Valley Event Center pages exist within the official Web site.

CAMAS is the county's intranet and is not accessible to the public. It is accessed inside the network through http://CAMAS and outside the network through https://camas.co.kittitas.wa.us by employees who have authenticated to the county network. Additional information on this resource is available at http://camas/is/web/.

The public site: http://www.co.kittitas.wa.us

Mission

The mission of the Web site is to support DH/EO's in providing services and information to the public in a highly usable, accessible, consistent, and intuitive manner.

Home page

The county home page is the portal to all county Web sites. It shall contain links to areas of the site such as departments, services, general county information, important topics, events, and employment.

Department pages

DH/EOs are responsible for providing information for their department Web page. DH/EO sites shall be accessed as "http://www.cokittitas.wa.us/[department name]".

County code

The Kittitas County Code is published on the public Web site. Updates to the code are made by the Webmaster as directed by BOCC resolutions. See SOP IS-A0002 for more information.

Emergency operations

When an emergency is declared by the federal government, state of Washington, or a Kittitas County local government, and for the duration of the activation of the Emergency Operations Center (EOC), IS will provide web development services to the EOC to facilitate communication between the Public Information Officer (PIO) and the public. For more information see SOP IS-G0012.

1. As soon after a declaration of emergency is signed as possible, the Incident Commander or PIO will contact the webmaster and outline EOC needs and expectations.
2. Content must be submitted to the webmaster by the PIO.
3. Content must meet all content and page requirements outlined in this policy; however, it does not need to be pre-approved by the ITC.
4. Press releases sent from the PIO to the media and IS that meet content requirements will be posted on the emergency page.

Content requirements

All content on the site must meet the following requirements; it must be:

1. In support of the public Web site mission.
2. Within the purview of the department adding the content to their own department site.
3. Information the public would expect to see on that department's site.
4. Freely publicly available through other means, i.e., not the original and therefore not a public record.
5. Void of broken links and out-of-date, irrelevant, or inappropriate content.
6. In compliance with all laws, i.e., copyright, privacy, and intellectual property.

7. Ready for public presentation, i.e., complete, accurate, void of spelling and grammar mistakes, and formatted generally as intended to be presented.
8. Photo, imagery, audio, and video content must be substantive and provide a necessary and significant addition to the text content.
9. Downloadable print media must:
    a. Be in PDF file format, made from the original electronic document when available
    b. Contain no viruses or malware
    c. If a county document, contain authoritative source information including, at a minimum, the county name, the department name, and a published date. It should also include the county logo, author's name, and credited source information.
    d. If a republished document, include the original publisher's author information. The DH/EO or designee must obtain the author's permission to reprint. If available on the publisher's site and the site falls within this policies hyperlinking provisions, the link will be to the publisher's page and not to a copy on the county's site.
    e. Contain metadata including, at a minimum, the title of the document, the county name, and the department name.
10. Audio files must be MP3, SRS, or FTR format. A link to the player will be provided.
11. Video files must be in WMV, MOV, AVI, or FLV format. A link to the player will be provided. Embedded video will be in FLV format.
12. Photographs taken by county employees in their capacity as county employees may be used on the public web site with the following exceptions:
    a. Photographs that include a person who appears to be a minor and is recognizable are prohibited.
    b. Photographs that include a person in a public venue, who does not appear to be a minor, are permitted without obtaining the person's permission except where:
        i. The image would be highly offensive to a reasonable person; and
        ii. The image is not of legitimate concern to the public.
    c. Photographs of people in private venues are prohibited.
13. Photographs not taken by county employees require a license agreement (for stock photography) or a signed release allowing use (for professional or amateur photographers).

Content must not:

14. Provide direct email addresses, except for those of elected officials. A web contact form must be used for all email communication.
15. Be for commercial, non-Kittitas County purposes, or personal or private gain.
16. Link or provide a URL to web sites or content not on its own site except where the page or content is controlled by one of the following:
    b. Agencies over which Kittitas County has
        i. appointing authority
        ii. a pass through contract
        iii. a contract to provide services
        iv. an agreement to provide or receive funding
    c. Other US government or United Nations controlled web sites
    d. Providers of file format reader software of county web published content, i.e., Adobe Acrobat Reader, FTR Player, etc.
    e. Providers with which Kittitas County has an agreement to provide a service
    f. Organizations and associations of which Kittitas County has requested and accepted membership

IS shall have the authority to deny linking to any site that is deemed not secure or which may pose a security risk to the Kittitas County IS systems or users.

Page requirements

17. All Web pages will adhere to the co.kittitas.wa.us Style Guide.
18. Each department home page will include the department's contact information.
19. Any page collecting information will describe how the information will be used and maintained.
20. No page will collect or store financial or other sensitive information. Payments will not be accepted directly through co.kittitas.wa.us.
21. Pages will be generally accessible to the public.
22. Pages will protect against unauthorized access to data and the network.

The intranet: http://CAMAS

Mission

The mission of the county's intranet is to provide information and applications to increase productivity and efficiencies in and between departments, committees, and employees.

Department pages

Each department will have a CAMAS home page. Each employee's Internet browser home page will be their department's CAMAS home page. The DH/EO is responsible for providing content for their CAMAS pages.

Access

CAMAS may be accessed by employees through the Internet at http://camas.co.kittitas.wa.us. Security is hierarchically controlled; pages and applications may display internal content viewable only by department employees, content restricted to only certain employees, or content for use by all county employees. Pages and applications with configurable security will be controlled through Multipass by DH/EO or designee. Utilization of this system does not supersede management's right to set work hours and location.

Applications

For CAMAS new application development, see SOP IS-G0010.

Web maintenance

The IS Applications division will perform all web site maintenance which includes editing and creating pages and application development for all county web sites. The webmaster will be responsible for scheduling web maintenance. Higher priority will be given to:

1. Increasing efficiencies of county employees
2. Providing service to the public
3. Providing time-sensitive information

Web maintenance requests must be submitted in electronic format through IS service requests. Minor edits will be made generally within 2 business days. Urgent requests may be accommodated as priorities permit. Major edits will be prioritized and scheduled.

A content management system may be employed, at the webmaster's discretion, to allow direct content management by DH/EO or their designee.

Violations of this web policy may result in removal of DH/EO's page(s).

Public content

1. New content will be submitted by the DH/EO or designee via IS service request to the ITC for approval.
2. Updates or additions to current content will be submitted by the DH/EO or designee via IS service request.

Semiannual review

A semiannual review of a department's web sites must be conducted by the DH/EO to ensure accuracy, completeness, and awareness of content. If approval is not provided within 30 days, the department page may be removed until approval is provided. See SOP IS-G0005.

Broken links and misspellings

DH/EOs are responsible for all content on their pages. Broken links and misspellings must be corrected within 10 days of notice. See SOP IS-G0005.

Webmaster email

The purpose of this policy is to direct the processing of email sent to webmaster@co.kittitas.wa.us.

The Web site will clearly note that the webmaster email is:

1. To be used to report problems encountered with the functionality of the Web site.
2. To suggest changes and enhancements.
3. Not intended for public disclosure requests. Public disclosure requests must be submitted to the department maintaining the records.
4. Monitored at least once a week.
5. Handled in the following manner:
    a. **Junk email** - Unsolicited email of a non-business nature that does not relate to county operations will be deleted with no reply.
    b. **Unsolicited email** - Product, service, or general information of a nature related to county operations will be forwarded to the appropriate DH/EO. No further action will be taken by the webmaster.
    c. **Direct requests for non-county information** - Requests for information not relating to county operations will be responded to by the webmaster. If an answer or referral for an answer can be determined within 5 minutes, it will be replied. If an answer or referral cannot be determined in 5 minutes, a reply stating the question/inquiry does not fall within county operation will be sent along with links to community resources that may provide assistance.
    d. **Direct requests for county information** - All requests for county information will be forwarded to the appropriate DH/EO copying the requestor. No further action will be taken by the webmaster.
    e. **Web site information** – Email regarding the operation of the web site will be handled and answered by the webmaster within one week.

Department Head/Elected Official

Each DH/EO will respond in a timely manner to email forwarded to them by the webmaster. In the event an email is forwarded incorrectly, the DH/EO will immediately forward the email to the correct office and copy the webmaster and the requestor.

Email notification subscription service (ENSS)

The county ENSS is an email signup list the public can join to receive emails on specific topics. Each department may make lists to which the public can sign up. For example, the Auditor has a list to notify subscribers of voter registration challenges, and CDS has a list to notify subscribers of comprehensive plan announcements and meetings. See SOP IS-G0009 for more information. DH/EOs will request creation of new subscription lists via IS service request for ITC approval.

Each email must:

1. Not violate county policies or laws governing email.
2. Be sent by the DH/EO or designee from the department email account or the DH/EO account.
3. Hide recipient email addresses from other recipients.
4. Include the approved anti-spam notice (http://camas/features/opt/instructions.asp).

ENSS functional requirements

The ENSS service must:

1. Allow public users to manage their subscription online.
2. Provide forgotten passwords via email to the email address registered.
3. Post a privacy notice in the subscription area on the public Web site.

DH/EO responsibilities

DH/EO must:

1. Ensure all web content submitted meets content requirements.
2. Allow for 2 business day turnaround time on all non-emergency requests.
3. Submit all requests in electronic format through IS service request.
4. Perform semiannual reviews of sites within 30 days of notice.
5. Monitor and correct broken links and misspellings.
6. Ensure all downloadable documents are virus-free, in the correct file format, contain authoritative source information, and contain appropriate metadata.
7. Respond in a timely manner to public email forwarded by the webmaster.
8. Request email notification lists in a service request to be approved by the ITC.
9. Only send ENSS email through department or DH/EO email address.
10. Ensure ENSS recipients email addresses are not seen by other recipients.
11. Ensure the anti-spam notice is included in any ENSS email.

IS responsibilities

IS Applications staff must:

1. Publish county code as directed by BOCC resolutions.
2. Provide web development to the PIO during a declaration of emergency.
3. Ensure all pages meet page requirements and style guidelines.
4. Perform all web site maintenance or provide a mechanism for secure management by DH/EO or designee.

5. Prioritize web maintenance and development.
6. Update the web sites as requested by the DH/EO and as approved by the ITC or policy.
7. Process all webmaster email in the manner defined above.
8. Provide ENSS with ability for public users to manage subscriptions, retrieve forgotten passwords, and display the privacy notice on the signup page.

12. GIS Policies

Geographic Information System (**GIS**) is a computer application used to store, view, and analyze geographic information.

County GIS Data

Ownership

Ownership, for the purpose of this policy, is intended to prevent orphaned data, not to control access. Many departments maintain data within the county's GIS. The department responsible for collecting and maintaining the data is the owner of the data; however, arrangements may be made between departments for one department to maintain another department's data.

Stewardship

IS serves as the GIS data steward. IS creates and maintains the systems and tools used to store, view, and analyze GIS data. The IS GIS Analyst will add all new data layers, that meet this policy's requirements, to the county's enterprise GIS database.

GIS data criteria

Data added to the county's GIS will meet the following criteria:

1. Use State Plain Washington South coordinate system
2. Use North American Datum 1983 (NAD83)
3. Display units in survey feet
4. DH/EO will develop accuracy standards to which their data will adhere.

Metadata requirements

All data will contain metadata as defined in SOP IS-G0006. Data without metadata will not be added to the county GIS data and will not be posted on the county Web site.

GIS data collection/creation

All data collected/created will follow procedures outlined in SOP IS-G0006.

Access to data

1. Only the data owner or their designee may edit their data.
2. IS will maintain a GIS mapping application for employee and public use.
3. All county-owned data meeting the requirements of this policy will be viewable through the county's mapping application and downloadable in raw ESRI data layer format on the county's public Website, unless the data owner DH/EO or designee makes arrangements with IS or the ITC designates the data as sensitive.

Third party data

IS may include third party data in the county's GIS. This data may be used by county agencies. Third party data will not be provided for download on the county's Web site.

GIS User Group

The GIS Analyst will regularly convene a user group meeting for all users of the county's GIS. The meeting will be an open forum in which the GIS Analyst will answer questions, demonstrate functions, and solicit feedback about the county's GIS.

DH/EO responsibilities

DH/EO must:

1. Ensure their GIS data is up-to-date and accurate.

Employee responsibilities

Employees must:

1. Follow the criteria requirements for all GIS data created, collected, and edited.

IS responsibilities

IS staff must:

1. Manage the GIS data and systems.
2. Make all county-owned GIS data available for download on the public Web site with exceptions noted above.
3. Maintain a mapping application for employee and public use.
4. Regularly convene GIS user group meetings.