Washoe County

Information Security Policy

April 2005

Washoe County

Information Security Policy

April 2005

Prepared for:

Information Technology Advisory Committee

Developed by:

Information Technology Standards Committee

ACKNOWLEDGEMENTS

Board of County Commissioners

Bonnie Weber, *District 5, Chair*
Bob Larken, *District 4, Vice-Chair*
Jim Galloway, *District 1*
David Humke, *District 2*
Pete Sferrazza, *District 3*

Information Technology Advisory Committee

Katy Singlaub, *County Manager, Chair*
Matt Beckstedt, *Director, Information Technology Department*
Justin Berg, *Internet Working Group Chairman*
Bill Berrum, *Treasurer*
Eileen Coulombe, *District Health*
Tom Gadd, *Director, Public Works*
Richard Gammick, *District Attorney*
Kathy Garcis, *Comptroller*
Amy Harvey, *County Clerk*
Ron Longtin, *Administrator, District Court*
Sandy Marz, *Law Librarian*
Arnie Maurins, *Associate Director, Library*
Don Means, *Sheriff's Office*
Joanne Ray, *Director, Human Resources*
John Sherman, *Director Finance*
Paula Valentin, *Standard's Committee Chairman*

Information Technology Standards Committee

Paula Valentin, *Water Resources – Chair*
Doug Johnson, *Information Technology – Vice-Chair*
Gary Beekman, *Information Technology*
John Blanke, *Information Technology*
Paul Burr, *Information Technology*
Larry Burtness, *Recorders Office*
Judy Chalmers, *Law Library*
Scott Chamberlain, *Sheriff's Office*
Paul Genco, *Information Technology*
Tracey Hilton, *Manager's Office - WINnet*
Mark Moser, *District Attorney's*
Margaret Spicher, *Library*
Greg Szachara, *Public Works*
Jerry Walker, *Information Technology*
Judy Zuppan, *District Health*

Contents

Overview

Washoe County is committed to protecting Washoe County's employees, partners and Washoe County from illegal or damaging actions by individuals, either knowingly or unknowingly.

Effective security is a team effort involving the participation and support of every Washoe County employee and Vendor who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

Purpose

The purpose of this policy is to outline the acceptable use of the Washoe County Information Infrastructure. These rules are in place to protect the employee and Washoe County. Inappropriate use exposes Washoe County to risks including virus attacks, compromise of network systems and services, and substantial legal liability.

The Washoe County Information Security Policy has been formulated with the following goals in mind:

- *Ensure the security of the Washoe County Information Infrastructure.*
- *Preserve the privacy and security of all Washoe County client information.*
- *Comply with all local, state and federal laws, statutes, and regulations.*
- *Preserve the integrity and validity of information belonging to Washoe County.*

Scope

This policy document applies to full-time, temporary and volunteer employees, contractors, consultants, and any other users of Washoe County Information Infrastructure, including all personnel affiliated with third parties. This policy document applies to all equipment and data that is owned or leased by Washoe County or used within the Washoe County Information Infrastructure. The policy statements contained within this document are by no means exhaustive, but attempt to provide a framework for activities that fall into the category of unacceptable use.

Definition of Terms

Archive media - Units of mass storage for backup purposes, such as tapes.

Archives - Electronic information copied to a long-term storage medium, such as tapes, for backup of data.

Backdoor - A method built into an application to bypass normal security mechanisms.

BIOS - The BIOS is built-in software that determines what a computer can do without accessing programs from a disk. On PCs, the BIOS contains all the code required to control the keyboard, display screen, disk drives, serial communications, and a number of miscellaneous functions. The BIOS is typically placed in a ROM chip that comes with the computer (it is often called a ROM BIOS). This ensures that the BIOS will always be available and will not be damaged by disk failures.

Confidential - Intended for or restricted to the use of a particular person, group, or class, containing information whose unauthorized disclosure could result in damage to the interest of Washoe County or Washoe County employees.

Critical – Information critical to the operation of the department.

Designated shares - Storage areas on servers accessed by and assigned to specific groups and/or users of the network.

Domain user name - User name assigned to a user to authenticate into the Windows NT domain for the purpose of controlling access to network resources.

Electronically monitored - Data transmissions captured and reviewed.

Employee computer account - See Domain user name.

Encryption technique - The translation of data into a secret code.

Firewall - A system designed to prevent unauthorized access to or from a private network.

Formal change control process - A structured method to control changes to operational systems.

Generic username - A common computer or network username usually shared within a group.

IDF - Intermediate distribution facility. A physical location for network connectivity devices, such as a telecommunications closet or server room.

Information Infrastructure - The totality of hardware and software systems and equipment that incorporates the computer network.

Managed development process - A structured method to analyze, create and deploy software.

MDF - Main distribution facility. The main physical location within a specific location for network connectivity devices, such as a telecommunications closet or server room.

Definition of Terms continued

Modem - A device for transmitting and receiving computer transmission over the public telephone network.

Network shares - Specified locations for accessing files on the network, controlled by access controls.

Patch - A software upgrade to an operating system or application or physical device.

Peripheral devices - A computer device, such as a CD-ROM drive or printer that is not part of the essential computer, i.e. the memory and microprocessor. Peripheral devices can be external -- such as a mouse, keyboard, printer, monitor, external Zip drive or scanner -- or internal, such as a CD-ROM drive, CD-R drive or internal modem. Internal peripheral devices are often referred to as integrated peripherals.

Program source libraries - Software programming language code, which defines the methods of operation for an application or applications.

Remote access - The ability to log onto a network from a distant location. Generally, this implies a computer, a modem, and some remote access software to connect to the network. Remote access means that the remote computer actually becomes a full-fledged host on the network. The remote access software dials in directly to the network server. The only difference between a remote host and workstations connected directly to the network is slower data transfer speeds.

Removable media - Physical objects on which data can be stored with the ability to be easily removed from a computer. These include floppy disks, CD-ROMs, tapes, flash and zip drives.

Router - A device that forwards data packets along networks. A router is connected to at least two networks, commonly two LANs or WANs, or a LAN and its ISP's network. Routers are located at gateways, the places where two or more networks connect.

Sensitive - Calling for tact, care, caution in treatment, discretionary authority

Sensitive Washoe County information - Information made confidential by law or of which the loss, misuse, unauthorized access to or modification of could adversely affect the Washoe County Information Infrastructure.

Special characters - Characters that are not numbers or letters, such as !@#$%^.

Switch - In networks, a device that filters and forwards packets between LAN segments. *Switches* operate at the data link layer (layer 2) and sometimes the network layer (layer 3) of the OSI Reference Model and therefore support any packet protocol. LANs that use *switches* to join segments are called switched LANs, or in the case of Ethernet networks, switched Ethernet LANs.

Synchronized - Coordinated, matching in time.

System level changes - Parameter changes made at the operating system level.

System logs - Files of application and/or operating system transactions.

Definition of Terms continued

Time protocols - An agreed-upon format for transmitting time data between two devices.

Unused ports - Physical ports on network devices currently not in use.

User level access - Defined and controlled access to computer and network resources specified by a username.

Vendor(s) - includes outsourcing, third parties and contractors: A party or parties who have been hired to perform duties or provide services to Washoe County and have been granted the proper security clearance for the assignment

Virus attacks - A program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes. Viruses can also replicate themselves. All computer viruses are man made. A simple virus that can make a copy of itself repeatedly is relatively easy to produce. Even such a simple virus is dangerous because it will quickly use all available memory and bring the system to a halt. An even more dangerous type of virus is one capable of transmitting itself across networks and bypassing security systems.

Virus protection software program - A software application that protects computers against software virus attacks.

Virus signature updates - Updates to anti-virus programs containing the latest data to combat newly created viruses.

VPN access - Virtual private network access; network access that is constructed by using public wires to connect nodes. For example, there are a number of systems that enable you to create networks using the Internet as the medium for transporting data. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.

Washoe County designated personnel - A Washoe County employee and/or authorized Vendor personnel, who has been assigned or hired to perform the specific Information Technology task or duty as defined in the Roles and Responsibilities Matrix (see appendix A).

Washoe County Information Technology Network Management Process - A structured method to manage changes to the Information Infrastructure.

Washoe County Information Infrastructure - All electronic equipment and connective cabling that comprises the totality of all Washoe County information systems to include all information stored and contained within these systems.

Washoe County Information Security Team - Washoe County Information Technology personnel responsible for the security of the Washoe County Information Infrastructure.

Web Island servers – A system of Internet servers that support World Wide Web applications that are cordoned off from the public Internet and the internal network.

Workstation - A desktop computer system for users.

Enforcement

This Policy shall be enforced pursuant to section 1100, Security Policy Enforcement.

Policy Changes

The Washoe County Information Security Policy is a living document and therefore, Washoe County reserves the right to make appropriate changes as needed to secure the Washoe County Information Infrastructure, pursuant to Washoe County Code 5.340.

Roles and Responsibilities

Appendix A (page 15) describes the roles and responsibilities for Washoe County designated personnel. These roles and responsibilities are consistent with those listed in the Washoe County Information Technology Policy Manual and as described in the Washoe County Information Technology Service Agreement Guidelines.

Roles and responsibilities pertaining to this document are classed and described as:

County I.T. Department: Washoe County Information Technology Department personnel with job duties specified in their job description or as assigned by the Department Head.

Department I.T.: A Washoe County Department, other than the Washoe County Information Technology Department, with Information Technology personnel with job duties specified in their job description or as assigned by the Department Head.

Department I.T.C.: A Washoe County Department, other than the Washoe County Information Technology Department, with Information Technology Coordinator(s) who's duties are described in the department's Information Technology Service Agreement or as assigned by the Department Head.

Department Head: The Division/Department Director, as described by Washoe County Human Resources or department head designee whose duties are described in the department's Information Technology Service Agreement.

End User: Any Washoe County employee, intern, volunteer, or Vendor who uses any information technology device with a connection to the Washoe County Information Infrastructure.

Vendor(s) - includes outsourcing, third parties and contractors: A party or parties who have been hired to perform duties or provide services to Washoe County and have been granted the proper security clearance for the assignment

Sensitive Material/Sensitive Information (100)

1. Access to files on the Washoe County Information Infrastructure shall be controlled so that only Washoe County personnel and authorized Vendors have the appropriate access to sensitive information.
2. When sending any information, the destination shall be checked by sender prior to sending to ensure information is not received by persons not authorized to view it.
3. Sensitive Washoe County information residing on removable media shall be stored securely in a locked area, file cabinet or safe. Locked areas, locked file cabinets and safes should be fireproof whenever possible. This activity shall be controlled and supervised by a department manager or such person acting in such a capacity. This person or persons may be held responsible for the physical security access to such locked areas.
4. Third parties must be authorized to receive all transmissions of sensitive Washoe County information.
5. The identity of persons requesting sensitive Washoe County information, or requesting password changes over the telephone must be verified, per standard operating procedures.

Users/Workstations (200)

1. The Washoe County Information Infrastructure is to be maintained and upgraded by Washoe County designated personnel only.
2. Repair of the Washoe County Information Infrastructure, shall only be carried out by Washoe County designated personnel.

3. All Software on Washoe County workstations shall be installed by Washoe County designated personnel. All software installed on Washoe County workstations shall be Washoe County approved software, except as defined in service level agreements.
4. Any movement of Washoe County Information Infrastructure equipment between Washoe County facilities to include its satellite facilities is to be controlled and coordinated by Washoe County designated personnel.
5. Physical changes made by non-designated personnel to Washoe County Information Infrastructure equipment are prohibited.
6. Any theft or damage incurred to any part of the Washoe County Information Infrastructure of any kind, whether deliberate or accidental, must be reported as soon as the matter is noticed.
7. Deliberate destruction or damage to any part of the Washoe County Information Infrastructure of any kind, for whatever purpose, is prohibited.
8. Use of removable media is restricted to authorized Washoe County use and only for the performance of work related duties.
9. A password for access to client computers' BIOS settings shall be set so only Washoe County designated personnel can access the BIOS setup.
10. Users are prohibited from violating or attempting to violate the security of the Washoe Information Infrastructure.
11. Access to the Washoe County computing equipment operating system commands may be restricted to the least access necessary to accomplish users' duties and job assignments.
12. Manipulation of operating system commands for purposes not relating to Washoe County official business or user's duties is prohibited.
13. All Washoe County employee workstations are to default to screensaver mode after ten (10) minutes of idle time. Domain user names and passwords shall be required to unlock screensavers, except as defined in service level agreements.
14. Unattended workstations shall be locked, logged off or shut down correctly.
15. Washoe County users shall attend security education and awareness classes as part of new employee orientation and as needed thereafter.
16. Files received through email of an unknown origin, or of a suspicious nature shall not be opened and shall be reported to Washoe County designated personnel.
17. Web browser software on the Washoe County Information Infrastructure shall be patched and updated on a continuing basis to minimize security risks.
18. Only Washoe County business-related data shall be stored on network shares.
19. Users shall observe caution when deleting or overwriting existing files.
20. Retired or "obsolete" equipment shall be inspected to ensure that all residual Washoe County information has been removed and rendered unrecoverable from these devices prior to disposal.
21. Network logins are assigned and are not to be shared except for maintenance and network administration. It is a violation of the Washoe County Information Security Policy to allow others to use your network login.
22. All activities while using a network login may be electronically monitored and/or recorded pursuant to Washoe County code 5.340 and the Washoe County Internet and Intranet Acceptable Use Policy.

23. Washoe County reserves the right to restrict employee downloading of any data not related to official Washoe County business pursuant to Washoe County code 5.340 and the Washoe County Internet and Intranet Acceptable Use Policy.

Portable devices (300)

1. Users' department management must authorize the use of all Washoe County owned laptop/portable and handheld devices for all Washoe County personnel.
2. Only Washoe County owned or approved devices shall be allowed to connect to the Washoe County Information Infrastructure.
3. Laptops and handheld computers must be issued with software images developed and/or approved by Washoe County.
4. Persons issued portable devices shall be held responsible for the security of the information contained within such devices.
5. Only Washoe County designated personnel shall install Washoe County owned or approved software on such devices.
6. All information contained within such devices is the property of Washoe County and is not considered personal information.
7. Maintenance for these devices shall be performed by Washoe County designated personnel.
8. Persons issued such devices may receive an orientation of security issues related to such devices to minimize security risks to Washoe County.

Remote Access (400)

1. Washoe County users accessing the Washoe County Information Infrastructure remotely shall use medium approved by Washoe County Information Technology.
2. Remote access to the Washoe County Information Infrastructure must use identification, authentication, and encryption techniques to safeguard all internal County computer systems.
3. All remote access must be approved and shall be restricted to those individuals with a specific purpose to access the internal network remotely.
4. Remote access users shall be given the least access privileges necessary to carry out their job related functions.
5. All remote access users may be given a security orientation to minimize security risks to Washoe County.
6. Modems are strictly forbidden for the use of dialing in or out of Washoe County computers unless authorized by the Washoe County Information Technology department. Alternative methods of network access shall be explored to include VPN access through the firewall.

Vendors (500)

1. All Vendor access to the Washoe County Information Infrastructure must be approved.
2. Access to the Washoe County Information Infrastructure shall be restricted to the lowest security level necessary to accomplish Vendors' tasks.
3. All Vendors for the Washoe County Information Infrastructure shall agree in writing to abide by the Washoe County Information Security Policy.
4. All Vendors shall sign a confidentiality agreement. Upon acceptance of a contract with Washoe County, Vendors shall agree to access and use the Washoe County Information Infrastructure responsibly according to this policy and in accordance with their Vendor role.
5. Vendors shall be held legally responsible for misuse of their access and use of the Washoe County Information Infrastructure.
6. Vendors may have their network activity monitored by the Washoe County Information Security Team.
7. Washoe County shall make every reasonable effort to ensure that reputable companies are used for outsourcing of computer processing.
8. Vendors shall not remotely access the Washoe County Information Infrastructure without the prior express permission of Washoe County. Access is generally granted by the Information Technology Department in the form of computer and network accounts granted to users and others, as appropriate, for such purposes as vendor support or contracted development.
9. Vendors will not attempt to disguise their identity, or the identity of their account. Vendors will not attempt to impersonate other persons or organizations. Vendors will not appropriate Washoe County's name, or its network names.
10. Vendors will not attempt to monitor other users' data communications unless specifically authorized. Vendors will not infringe upon the privacy of others' computer files. Vendors will not read, copy, change, or delete another user's computer files or software without the prior express permission of the owner.
11. Vendors shall not engage in actions that interfere with the use by others of any computers and networks, interfere with the supervisory or accounting functions of the systems, or are likely to have such effects. Such conduct includes, but is not limited to, placing of unlawful information on the system, transmitting data or programs likely to result in the loss of the recipient's work or system downtime, or any other use that causes congestion of the networks or interferes with the work of others.
12. Vendors will not attempt to bypass computer or network security mechanisms without the prior express permission of the Information Technology Department. Possession of tools that bypass security or probe security, or of files that may be used as input or output for such tools, shall be considered as the equivalent of such an attempt.
13. Vendors who require remote access to the County's network will be required to have a Washoe County approved virus protection software program installed. This program must be operational and be using the latest virus detecting upgrades for computers used for this purpose.

Systems Development and Applications (600)

1. Software developed by Washoe County Information Technology staff and/or Vendors for Washoe County official business must follow a managed development process to ensure its integrity.
2. Software developed by Washoe County Information Technology staff and/or Vendors for Washoe County official business shall be secured using application access controls and compartmentalization of application privileges.
3. Creation or installation of "backdoors" on applications to circumvent access controls is prohibited.
4. Washoe County management staff shall take steps on a continuing basis to segregate systems operations and systems development divisions, and their functions, in order to safeguard live systems.
5. New applications, enhancements and upgrades to Washoe County systems shall be coordinated by Washoe County designated personnel to ensure their successful integration.
6. Changes or additions to applications developed by Washoe County or Vendors, shall be deployed by designated personnel and in coordination with the supervisory staff of any affected department that uses the application.
7. All changes to programs running on the Washoe County Information Infrastructure shall be properly authorized and tested in a lab environment before moving to a production system.
8. Vendors shall coordinate with Washoe County prior to upgrading their Vendor-supported applications on County networks or systems to minimize risks and downtime.
9. Use of live data for testing a new system is prohibited.
10. Use of data for testing a new system or system changes shall be controlled by authorized Washoe County designated personnel to ensure the security of the live data.
11. All new and upgraded systems must be supported by training and documentation for all affected Washoe County users.
12. New databases shall be tested prior to production use.
13. All Washoe County databases shall be maintained, administered and secured by Washoe County designated personnel or Vendors to ensure their integrity and appropriate access.
14. Illegal and/or unauthorized use of Washoe County databases by anyone is prohibited.
15. Procedures performed on malfunctioning databases to restore the proper operation of such databases shall be administered by Washoe County designated personnel.
16. Only Washoe County designated personnel are allowed to control specified operational software.
17. Changes to operational software shall be restricted to Washoe County designated personnel authorized to amend such software and coordinate with that authorized group through an approved management development process.
18. System level changes made to operational software are discouraged, except in situations designated by Information Technology management.
19. Use, editing, and deletion of all program source libraries shall adhere to a formal change control process.
20. Access and changes to program source libraries may be restricted.

Systems Administration (700)

1. The Washoe County Information Infrastructure shall be administered by Washoe County designated personnel and/or Vendors using documented procedures in an efficient and secure manner.
2. The Washoe County physical infrastructure shall be managed by Washoe County Information Technology personnel only. Washoe County Information Technology personnel shall be responsible for all operations and security of these systems.
3. Administrative or root level access to the Washoe County Information Infrastructure shall be minimized and compartmentalized.
4. Network devices of any kind used to connect to the Washoe County Information Infrastructure shall be coordinated by Washoe County Information Technology staff. All network devices shall be prohibited unless approved by the Washoe County Information Technology network management process.
5. The structure of network directory locations shall be controlled by Washoe County designated personnel.
6. All critical Washoe County data files, as defined by each department, shall be saved on network shares or approved backup devices. All data files stored on local drives and removable media are subject to loss.
7. Access to Washoe County information stored on the Washoe County Information Infrastructure shall be restricted by access controls.
8. All software running on the Washoe County Information Infrastructure shall be legally licensed and owned by Washoe County.
9. All software may be verified on a periodic basis to ensure it is legally licensed. All non-Washoe County licensed or owned software will be removed.
10. Software patches for systems running on the Washoe County Information Infrastructure shall be applied by Washoe County designated personnel and/or authorized Vendors.
11. All Washoe County employees and Vendors shall keep confidential ALL sensitive electronic information they are exposed to in the performance of their duties.
12. All Washoe County Information Infrastructure documentation shall be kept current by the Washoe County Information Technology department. All Information Technology personnel are responsible for maintaining and updating documentation. All documentation shall be kept in a centralized secure location.
13. Archives of Washoe County data shall be maintained on a daily basis and stored in a secure area.
14. Archive media shall be cycled through secure, off-site storage.
15. All Washoe County related information stored on the Washoe County Information Infrastructure shall be retained for the time period necessary to meet legal and business requirements.
16. Documented system recovery procedures shall be maintained for all of the Washoe County Information Infrastructure.
17. Validity and effectiveness of all backups shall be reviewed on a continual basis to ensure that all data is being archived.

18. The integrity of existing data shall be protected by Washoe County designated personnel during the recovery of archived data, especially when archived files may replace existing files on the systems.
19. The Washoe County Information Infrastructure shall be protected against the risk of physical damage or loss.
20. Washoe County systems clocks shall be synchronized using available tools and/or time protocols.
21. Temporary files on the Washoe County Information Infrastructure shall be removed on a regular basis.
22. Confidential data residing on computer equipment that is it to be reused, sold or donated shall be removed and rendered unrecoverable prior to its release from Washoe County service.

Password Policy (800)

1. Access to the Washoe County Information Infrastructure shall be controlled with usernames and passwords.
2. Passwords are not to be shared with any unauthorized person for any reason, except as specified in the Service Level Agreement, and shall not be reused.
3. Domain user password changes shall be required every 3 months, except as specified in the Service Level Agreement.
4. Password length for user accounts shall be at least 7 characters of some combination of letters, numbers, and/or special characters.
5. Passwords for Washoe County designated personnel shall consist of two sets of 7, to make 14 characters. Each set of 7 characters shall contain numbers, letters, and special characters. For example: q1@#3cx*n43!@a.
6. Washoe County personnel shall avoid the use of words and names in their passwords.
7. Washoe County designated personnel shall change passwords on applications upon installation and on a consistent basis thereafter.
8. System and administrative passwords shall be changed immediately upon suspicion of any system or administrator password compromise.
9. Exchange of passwords via email is discouraged.
10. Password policies may be enforced using automated tools.
11. Use of passwords to secure individual documents is discouraged.
12. Passwords shall be kept in a secure location and not in open view.
13. Each department is responsible for notification of any employee change in status and the appropriate change in access rights.
14. Accounts of terminated employees and vendors shall be disabled immediately upon termination, and removed as soon as practicable thereafter.

Physical Access (900)

1. Physical access to all Intermediate Distribution Facilities and Main Distribution Facilities shall be restricted and may be monitored. All IDF and MDF locations shall be locked at all times.
2. Any area containing servers and/or network equipment shall be considered a high security area. Physical access to high security areas shall be restricted and not shared.
3. All ports on switches and routers shall be deactivated until needed except for emergency department control points.

Security Administration (1000)

1. Access controls shall be applied to the Washoe County Information Infrastructu*re* to maximize overall security.
2. Access control standards shall be established to maximize the complete security posture of the Washoe County Information Infrastructure while providing unhindered network access to meet business needs.
3. The Washoe County Information Infrastructure shall be configured to minimize security risks.
4. The Washoe County Information Infrastructure shall be patched on a continual basis to safeguard against new security threats.
5. Access to the Washoe County Information Infrastructure shall be strictly controlled to prevent unauthorized access.
6. Access to the Washoe County Information Infrastructure shall be restricted to the least access necessary to accomplish users' duties and job assignments.
7. Protective systems and devices may be installed, maintained, and monitored to minimize breaches of security.
8. The Washoe County Information Infrastructure is monitored continually to detect possible unauthorized use of such systems.
9. Security audits shall be conducted on a continual and periodic basis to detect potential security problems, and system vulnerabilities.
10. Overall security of the Washoe County Information Infrastructure shall be managed by the Washoe County Information Security Team in cooperation and coordination with Washoe County designated personnel and Information Technology management.
11. On a consistent and continual basis, the Washoe County Information Security Team shall evaluate any new security threats posed to the Washoe County Information Infrastructure, and shall implement countermeasures to circumvent them.
12. All system logs are monitored on a daily basis.
13. Information relating to Washoe County Information Infrastructure security incidents shall only be released to Washoe County designated personnel.
14. Procedures for computer forensics may be developed by the Washoe County Information Security Team for the collection of evidence relating to illegal computer activity targeting the Washoe County Information Infrastructure.
15. Washoe County may prosecute individuals engaged in illegal computer activity targeting the Washoe County Information Infrastructure.

16. Washoe County designated personnel may receive security training on a continual basis to maximize total systems security.
17. Risks posed by user Internet access may be minimized by security devices.
18. Washoe County designated personnel shall be responsible for determining and maintaining the appropriate level of security and types of devices needed for safe Internet access by Washoe County personnel.
19. The posting of web content to Washoe County public web servers and machines residing within the Web Island shall be restricted.
20. Appropriate access controls to Washoe County web servers and machines residing within the Web Island shall be maintained. Washoe County users shall have the least access necessary to accomplish appropriate job duties.
21. Posting of content by authorized Washoe County users to Web Island servers shall be restricted to content directly related to Washoe County official business pursuant to Washoe County code 5.340 and the Washoe County Internet and Intranet Acceptable Use Policy. Posting of illegal, unethical, inappropriate, personal or any other content not of a Washoe County official nature to Washoe County Web Island servers is prohibited.
22. Washoe County personnel shall report security discrepancies, weaknesses, and incidents to the Washoe County Information Security Team. The Washoe County Information Security Team shall investigate and take appropriate action as needed.
23. Human Resources shall authorize the Information Technology Department to obtain a weekly list of all Washoe County employee terminations, changes and transfers.
24. Whenever possible, all generic and guest accounts shall be disabled or removed from the Washoe County Information Infrastructure.
25. Unused/inactive user computer accounts shall be removed on a continuing and consistent basis.
26. Data files of a Washoe County terminated employee shall be turned over to that employee's supervisor.
27. Evidence relating to an information security breach shall be preserved and forwarded to the Washoe County Information Security Team.
28. File attachments in emails from the Internet shall be screened at the server level for malicious or potentially destructive code. Attachments containing such content shall be removed.
29. Antivirus software shall reside and be kept current on any computers connected to the Washoe County Information Infrastructure. Where possible, antivirus software with virus signature updates, along with virus scanning shall be automated on all devices connected to the Washoe County Information Infrastructure. Virus scanners shall scan all appropriate files.
30. Antivirus software shall reside and be kept current on all devices that are part of the Washoe County Information Infrastructure.
31. The Washoe County Information Security Team shall implement a formal incident tracking and reporting protocol.

Security Policy Enforcement (1100)

1. Washoe County shall fully comply with all local, state, and federal laws and statutes that may relate to data protection legislation within its operational functions.

2. All Washoe County employees shall be required to fully comply with the Washoe County Information Security Policy.
3. Washoe County management, at all levels, shall be responsible for monitoring compliance with the Washoe County Information Security Policy.
4. Washoe County Management, in consultation with appropriate staff, shall be responsible for enforcing the Washoe County Information Security Policy. Violation of this Policy may result in appropriate legal action and/or disciplinary action, up to and including termination.
5. The Washoe County Human Resources Department shall be responsible for maintaining a current copy of the Washoe County Information Security Policy on its website.
6. The Washoe County Human Resources representative for each department shall be responsible for providing a copy of the Washoe County Information Security Policy to employees, along with an acknowledgement to be signed and returned to Human Resources for maintenance in the employee's personnel file.
7. All Washoe County employees may be required to sign a nondisclosure agreement.
8. Washoe County reserves the right to access all information created and stored on the Washoe County Information Infrastructure.
9. Unless required by law, Washoe County shall not defend or indemnify an officer or employee against charges or claims resulting from any action that is found to be a violation of any part of this Policy.