Wasatch County School District
Information Technology Security Plan

1. Introduction.

This document, along with appendices, is a detailed description of security practices within WCSD. It is meant to be a dynamic plan that will, at least in part, be shared will all staff through appropriate training and media. Some of the information presented in this plan was borrowed from public sources, most notably the National Center for Education Statistics (NCES) web site (http://nces.ed.gov).

2. Security Management Processes

At the present time oversight of security at WCSD is somewhat decentralized with a designated security officer who shares security responsibilities with others and also has other assignments. Work is in progress to change this situation in the near future. Even though there is no dedicated security office at this time most of the practices and activities in this document are already being performed. Areas in which implementation is not complete at the present time are training, intrusion detection and to some extent quality assurance. If a fulltime security office were present they would also do the following.

2.1. Communicate to staff that protecting the system is not only in the organization's interests, but also in the best interest of users.

2.2. Increase staff awareness of security issues.

2.3. Provide for appropriate staff security training.

2.4. Monitor user activity to assess security implementation.

2.5. Be inclusive when building a security and contingency planning team by including:

2.5.1. Key policy-makers

2.5.2. The security manager

2.5.3. Building management

2.5.4. Technical support

2.5.5. End-users

2.5.6. Other representative staff

2.5.7. Local authorities

2.5.8. Key outside contacts (e.g., contractors and suppliers)

3. Physical Security

3.1. Building

3.1.1. Fire Protection. All buildings are protected by a fire detection system.

3.1.2. Building access. Other than regular school hours, all external doors are locked at all times and require an electronic key for entry.

3.1.3. Surveillance cameras. Cameras record key areas of buildings 24 hours a day. Administrators have access to external and internal surveillance cameras through interfaces in their schools.

3.1.4. Internal Building Access. After business hours all sections of the building except the main first floor hallway are also secured. The computer services section of all buildings is denied to all but authorized employees during non-work hours.

3.1.5. Employee Building Access. Employees are screened and given off hours access to appropriate areas of the building depending on their roles. All employees must wear WCSD badges at all times within the building.

3.2. Network Rooms

3.2.1. Water damage. All hardware and wiring is elevated off floors in racks or trays of some sort. Fire prevention sprinkler systems are currently in place in many of the rooms. A chemical based fire retardant system is being evaluated.

3.2.2. Physical Access. Only one inconspicuous door provides access to the network rooms and those doors will be secured by card key access in the future.

3.2.3. Electrical Overloads. Hardware VA rating and totals are assessed to make sure any one circuit is not being overloaded. When needed, more circuits are added to the network rooms. Total volt-amps and wattage is kept at 60% or lower of the maximum capacity of a circuit.

3.2.4. Earthquakes. Individual devices are securely attached to racks and racks are anchored to the ceiling, floor or other secured racks.

3.2.5. Power Backup. All network room hardware is on UPSs . Larger network centers are on UPSs and are or will be on powered generator backup power systems which are able to supply emergency power to the building for at least 24 hours.

3.2.6. Temperature control. If the temperature climbs past a predefined maximum, currently 80 degrees Fahrenheit, a monitoring system is triggered and automatic text messages are made to key WCSD computer services staff.

4. Data/Information Security & Privacy/Confidentiality (also see: **Data Access Security and** Appendix A for more details about privacy, FERPA and GRAMA at WCSD)

4.1. Policy Statement. Wasatch County School District (WCSD) makes every effort to abide by all applicable State and Federal guidelines, policies, regulations, statutes, and procedures pertaining to the confidentiality and privacy or data. WCSD does not permit access to, or the disclosure of, student records or personally identifiable information contained therein (other than directory information) except for purposes authorized under the Family Educational Rights and Privacy Act (FERPA). FERPA assures students that their records are protected from unauthorized access or disclosure and requires a clear understanding of the type of information that can be released without an individual's consent. WCSD also does not permit unauthorized access to, or the disclosure of educator and employee records or personally identifiable information contained therein.

As a result, it is important to handle all confidential information with discretion, safeguarding it when in use, storing it safely, updating or disposing of it properly, and discussing it only with those who have a need to know for a legitimate business reason. In most cases, data of a personally identifiable nature shall remain secure from public disclosure (release to third parties) without specific permission from the individual to whom those data apply.

4.2. Policy Purpose. This policy establishes the procedures and protocols for collecting, maintaining, disclosing, and disposing of education records containing personally identifiable information about students and educators or any other individual for whom WCSD maintains data. It is intended to be consistent with the disclosure provisions of the FERPA. All users of WCSD information systems must follow the practices outlined below.

4.3. Definitions.

4.3.1. Directory Information" means:
- 4.3.1.1. Student's name, address, telephone listing, and date of birth
- 4.3.1.2. Parent or lawful custodian's name, address, and telephone listing
- 4.3.1.3. Grade level classification
- 4.3.1.4. Dates of attendance, dates of enrollment, withdrawal, re-entry
- 4.3.1.5. Diplomas, certificates, awards and honors received
- 4.3.1.6. Most recent previous educational institution attended

4.3.2. "Disclose" or "Disclosure" means to permit access to, or to release, transfer, or otherwise communicate, personally-identifiable information contained in education records to any party, by any means, including oral, written, or electronic means.

4.3.3. "Education Records" means any information or data recorded in any medium, including but not limited to handwriting, print, tapes, film, microfilm, and microfiche, which contain information directly related to a

student and which are maintained by WCSD or any employee, agent, or contractor of WCSD.

4.3.4. "Maintain the Confidentiality" means to preserve the secrecy of information by not disclosing the information

4.3.5. "Personally-identifiable" means data or a record that includes any of the following:

4.3.5.1. The name of a student, the student's parent or other family member

4.3.5.2. The address of the student

4.3.5.3. A personal identifier, such as the student's social security number or an assigned student number

4.3.5.4. A list of personal characteristics which makes the student's identity easily traceable

4.3.5.5. Other information which makes the student's identity easily traceable

4.3.5.6. "Security" means technical procedures that are implemented to ensure that records are not lost, stolen, vandalized, illegally accessed, or improperly disclosed.

4.3.5.7. "Student" means any person who is or has attended public or accredited nonpublic school and for whom WCSD maintains education records or personally-identifiable information

4.3.5.8. “Educator” means someone who is or has been employee by a Utah public school or has applied for a Utah educator credential.

4.4. Information to be Maintained

It is anticipated that WCSD will collect and maintain personally-identifiable information from education records of Utah students, to include

4.4.1. Personal data which identify each student. These data may include, but are not limited to, name, student identification number, address, race/ethnicity, gender, date of birth, place of birth ,social security number (only in special cases), name and address of parent or lawful custodian

4.4.2. Attendance and other pupil accounting data

4.4.3. Data regarding student progress, including grade level completed, school attended, academic work completed, and date of graduation

4.4.4. Standardized test scores including SAGE, CRTs, NRTs, and UALPA.

4.4.5. Data regarding eligibility for special education and special education services provided to the student.

4.4.6. Data regarding eligibility for other compensatory programs and special program services provided to the student.

4.4.7. Professional Educator data including outcomes of background checks, education and teaching history and any disciplinary measures.

4.4.8. SIS and Fiscal data for hosted districts.

4.5. Practices to Maintain the Confidentiality of Student Information

WCSD shall utilize various procedures and security measures to ensure the confidentiality of student records. These procedures shall include assignment of a unique identifier to each student, a system of restricted access to data, and statistical cutoff procedures (not reporting aggregate measures of small groups of student subgroups).

4.5.1. A system has been developed to assign a unique Student ID to each Utah student. The Student ID shall be computer generated and contain no embedded meaning. After being checked for duplicates, it shall become permanently assigned.

4.5.2. Security protocols shall be designed and implemented by WCSD. They shall limit who has access to the data and for what purposes.

4.5.3. WCSD also shall adopt statistical cutoff procedures (not reporting aggregate measures of small groups of student subgroups) to ensure that confidentiality is maintained. For example, if there are less than ten students in a give racial group within a school, that group's average score on a standardized test would not be publicly reported.

4.5.4. All WCSD personnel collecting or using personally-identifiable student information shall be provided instruction regarding procedures adopted in accordance with this policy. They will also be required to sign a confidentiality agreement.

4.5.5. WCSD shall maintain a current listing of personnel who have access to personally-identifiable student information.

4.6. Individual Employee Rules

4.6.1. Data originated or stored on district computer systems are WCSD property. Employees will access only data that are required for their job. Employees will not make or permit unauthorized use of any WCSD data. They will not seek personal or financial benefit or allow others to benefit personally or financially by knowledge of any data that has come to them by virtue of their work assignment.

4.6.2. Employees will not release District data in any format except as required in the performance of their job. Employees will not remove, electronically or printed, an official record or report, or copy of one, from the office where it is maintained, except as may be necessary in the performance of their job.

They will not exhibit or divulge the contents of any record or report to any unauthorized person except in the conduct of their work assignment and in accordance with WCSD policies and procedures.

4.6.3. Employees will not share their computer login information, including password(s) with others or leave their written password(s) in a place that could be accessible by others. If a user has reason to believe others have learned their password(s), they will report the problem to their supervisor and will take appropriate action to have the password(s) reset. Employees will not attempt to use the logins and passwords of others, nor allow their logins and passwords to be used by others.

4.6.4. Employees will maintain the security of all WCSD data in their possession or to which they have access by protecting computer media, forms and printouts from unauthorized access and will dispose them in a safe manner. Further, employees will not leave their PC signed on when unauthorized people could access it, will change their password(s) on a regular basis, and will take other precautionary measures necessary to protect and secure, confidential, or sensitive data.

4.7. Disclosure of Data for Research

WCSD may disclose confidential personally identifiable information of students to organizations for research and analysis purposes to improve instruction in public schools. Any such disclosure shall be made only if the following requirements are met.

4.7.1. The conditions in FERPA regulation 34 CFR 99.31(a)(6) are met.

4.7.2. The research project is approved by the Superintendent of Public Education or an Associate Superintendent, utilizing WCSD's criteria for approving research requests.

4.7.3. The recipient organization has signed WCSD Confidentiality Agreement.

4.8. Record of Access

WCSD shall maintain a record which indicates the name of any individual or organization external to WCSD that requests and is allowed access to students' educational records. The record of access also shall indicate the interest such person or organization had in obtaining the information, as well as the date the requested data were disclosed.

4.9. Other Important Privacy and Confidentiality needs. Besides data governed by FERPA, WCSD is also responsible for providing controls over processes and procedures around educator licensing data, rehabilitation systems and records as well as school funding, budgeting and financing records and systems. Personally identifiable data in these datasets will also be maintained in a

confidential and secure manner.

4.10. Data/Information Integrity (Preventing Unauthorized Creation, Modification, or Deletion of Information):

4.10.1. WCSD staff is never to send sensitive information as e-mail. If e-mail absolutely must be used, the file is to be encrypted and sent an attachment rather than in the text of the e-mail message.

4.10.2. All data are to be encrypted before it leaves a server or workstation.

4.10.3. Secure FTP and SSL are always to be employed when transmitting data to and from district facing applications.

4.10.4. All data encryption devices and keys are to be physically protected. They must be stored away from the computer.

4.10.5. All staff are to be informed that all messages sent with or over the organization's computers belong to the organization and therefore subject to monitoring.

4.10.6. The receiver's authenticity must be verified before sending any WCSD data or information. Everyone sending data outside the district must ensure that users on the receiving end are who they represent themselves to be by verifying: 1) Something they should know-a password or encryption key (this is the least expensive measure but also the least secure) or 2) Something they should have-for example, an electronic keycard or smart card.

4.10.7. Likewise, all data senders need to consider setting up pre-arranged transmission times with regular information trading partners: If you expect transmissions from your trading partners at specific times and suddenly find yourself receiving a message at a different time, you'll know to scrutinize that message more closely.

4.10.8. Likewise everyone must maintain security when shipping and receiving materials: When sending sensitive information through the mail, or by messenger or courier, require that all outside service providers meet or exceed your security requirements.

4.11. Practice the following safe data storage:

4.11.1. Backup files require the same levels of security as do the master files (e.g., if the original file is confidential, so is its backup).

4.11.2. Clearly label disks, flash drives, containers, cabinets, and other storage devices: Contents and sensitivity should be prominently marked so that there is less chance of mistaken identity.

4.11.3. Never store sensitive data/information in such a way that it co-mingles with other data on disks or other removable data storage media.

4.11.4. Information, programs, and other data should be entered into, or exported from the system only through acceptable channels and by staff with appropriate clearance and technical knowledge.

4.11.5. Write-protection should be used to limit accidental or malicious modification of files. Note that while write-protection is effective against some viruses, it is by no means adequate virus protection in itself.

4.11.6. Train staff to promptly notify the system administrator/security manager when data are, or are suspected of being, lost or damaged.

4.12. Dispose of Information in a Timely and Thorough Manner:

4.12.1. Follow all WCSD and State of Utah retention schedules for specific information or data sets.

4.12.2. Mark files to indicate the contents, their expected life cycle, and appropriate destruction dates.

4.12.3. Before discarding or surplusing obsolete or old media, it will be scrubbed or overwritten to make data recovery impossible. CD ROMs will be physically shredded.

4.12.4. Consider degaussing (a technique to erase information on a magnetic media by introducing it to a stronger magnetic field) as an erasure option.

4.12.5. Burn, shred, or otherwise physically destroy storage media (e.g., paper) that cannot be effectively overwritten or degaussed or scrubbed.

4.13. Data Availability:

Where data access is permissible WCSD must prevent any unauthorized delay or denial of information to qualified parties. Strict adherence must be given to FERPA and GRAMA at all times.

4.14. Law Enforcement Notification of Security Breaches or Unacceptable Behavior.

If any of the following are discovered on WCSD network, in consultation with WCSD legal staff, appropriate law enforcement officials must be notified.

4.14.1. Child pornography
4.14.2. Attempts to solicit a minor
4.14.3. Death threats
4.14.4. Disclosure of Social Security Numbers
4.14.5. Disclosure of credit card numbers or other personal financial numbers.

5. Software Security

5.1. Software installation.

Only network administrators and admin users (see Appendix B) have rights to install or otherwise add software to any server, desktop or notebook systems. Only network administrators can install or add software to servers. Admin users must sign a use agreement and receive special network training.

5.2. Storage of master copies.

Master copies of all software, licenses and documentation are retained in a secure location within the technology department. Spreadsheets or other software applications for the management of licenses are maintained along with expiration and renewal schedules.

5.3. Approved Software.

Only WCSD Computer Services approved and purchased software is installed by WCSD network staff or WCSD admin users may be used on WCSD machines. With permission, admin users may install individually purchased copies of software acquired personally or through their department. However, they must have licenses for all such software available at all times.

5.4. Non-Computer Services approved and purchased software.

Before permission will be given to an admin user for the installation of any non-approved software the user must submit a written request describing the nature of such software and the purpose for which it is to be installed.

5.5. Monitoring of software.

To counter possible copyright infringements caused by unlicensed software on organizational equipment that puts the entire organization at risk for fines and other penalties stemming from copyright violations, software inventories will be done on a regular basis. These comprehensive network-wide inventories will include the: the product, name of the manufacturer, version number, and the computer on which he software is installed. This inventory will be reconciled against the WCSD software license inventory to verify that no unlicensed software or software for which WCSD has inadequate licenses is installed anywhere on the system.

5.6. Train staff on software use and security policies.

The best designed software for accessing and manipulating information is useless if staff are unable to use it properly. In conjunction with human resources, WCSD should prepare and conduct software and technology awareness workshops.

5.7. Regulate Software Development and Changes:

5.7.1. Software development life cycle. All custom software is developed following a prescribed software development life cycle

5.7.2. Authorization of software changes. Before anyone modifies or creates any software, a formal, written change request must be submitted to the IT director or an IT manager. Such requests must be signed by a section director or superintendent and result in an audit trail of artifacts and events as the request is processed.

5.7.3. Design Reviews. Continued feedback is expected from users during the software development process to ensure that the new or changed software will satisfy functional specifications and security requirements.

5.7.4. Production vs. Development Copies. To avoid putting active applications and files at risk all new development is done in a separate development/testing environment with separate test networks and servers were applicable. Once the modified or new copy/version of the software is thoroughly tested by the software development staff and prospective end-users, then and only then will it be deployed to the production or "live" environment.

5.7.5. Program review. Before new or changed programs are put into production the code changes are reviewed by at least one other person who understands the change request that initiated the new or changed code. This step, of course, precedes actually testing and is just one step in the quality assurance/quality control process.

5.7.6. Vulnerability checking: As much as possible program code should also be reviewed and tested for potential vulnerabilities such as buffer overflows and SQL injection attacks that would make it susceptible to various software exploits.

5.7.7. Master files. Master files of all developed software are maintained independently of the development staff: Software belongs to the organization, not the programmer. All original copies are controlled and the organization clearly guarantees this ownership. It is required that any new or modified software be tested rigorously and certified as fully operational before releasing it for general use.

5.7.8. Required documentation. For all new or revised programming, requisite documentation includes among others: the name of the developer, the name of the system, the modules/objects impacted, programming languages/technologies, the development/change dates, nature of the revision, the revision number etc.

5.7.9. Public programs: If software downloaded from the Internet must be used with sensitive information, be sure that it has not been tampered with by checking for a digital signature to verify its authenticity.

5.7.10. Software Verification: Before putting the software into operation, verify that all software user functions are working properly. Check that new software meets anticipated user needs, current system requirements, and all organizational security standards. This recommendation is also applicable when upgrading software.

5.7.11. Upgrade backups: Before installing new software or software upgrades: The latest copies of data files must be backed-up until the new software or upgrade is proven to be running properly.

5.7.12. Application software testing: Developers must never risk losing live data with newly installed software. Always run dummy files and/or copies of non-sensitive files through the software to verify software's integrity and proper functioning.

5.7.13. Test machine isolation: Initial software testing should occur on test machines and a test network if at all possible. By maintaining a separate test environment, the entire system is not at risk if the software malfunctions.

5.7.14. Parallel software testing: Run old software at the same time and with the same data as the new software. It should be confirmed that the new versions of the software must generate the same results as the existing system.

5.7.15. Backup of Custom Software: Like all other data on WCSD servers, all custom developed software, including commercial software that has been modified with permission, is backed up on a predefined schedule. See backup plan in section 6.4.

6. Data Access Security (Data/Information Security & Privacy/Confidentiality)

While the vast majority of system users are trustworthy, there are occasional computing accidents. Most system problems are the result of human error. By instituting security procedures, the organization protects not only the system and its information, but also each user who could at some point unintentionally damage a valued file. By knowing that "their" information is maintained in a secure fashion, employees will feel more comfortable and confident about their computing activities.

6.1. Passwords:

After an independent audit of WCSD it was recommended that these actions be taken to improve security. The majority of the old passwords in the password database were cracked within 3 seconds.

6.1.1. All passwords be at least eight characters in length (ten or more is preferable).

6.1.2. No passwords are permitted that are words, names, dates, or other commonly expected formats.

6.1.3. Passwords should not reflect or identify the account owner (e.g., no birthdates, initials, or names of pets).

6.1.4. The password character string must contain one character from three of these four character types:

6.1.4.1. Uppercase letters

6.1.4.2. Lowercase letters

6.1.4.3. Numerals

6.1.4.4. Non-alphanumeric characters such as: (, . ; : * % &)

6.1.5. All users should change passwords at least once every school year.

6.1.6. No users may share passwords.

6.1.7. Unsecured storage of personal passwords is forbidden (e.g., they should not be written on a Post-It™ note and taped to the side of a monitor).

6.1.8. A password may never be used as part of an e-mail message.

6.1.9. Users should be warned not to type their password when someone may be watching.

6.1.10. Mask (or otherwise obscure) password display on the monitor when users type it in.

6.1.11. Remind users that it is easy to change passwords if they think that theirs may have been compromised.

6.1.12. No new password may be the same as an old password unless at least four other unique passwords have been used in between.

6.1.13. Users are discouraged from using the same password for two or more systems.

6.2. Walk-in/Guest users:

Any walk-in or guest user must abide by the policies set forth above.

6.3. VNP Connections:

All connections made through VNP (Virtual Private Networking) by telecommuters or wireless users outside of the building must be made through district owned and maintained devices or district approved devices. These machines will be allowed access only through proper identification and protocols.

6.4. Remote Access Monitoring:

Staff must be reminded that remote access is particularly subject to monitoring activities. Increased risk requires increased vigilance.

6.5. Message Authentication:

Use software that requires "message authentication" in addition to "user authentication": Even if a user can provide the right password, each message sent and received must have its delivery verified to ensure that an unauthorized user didn't interrupt the transmission.

6.6. Social Engineering: No one will ever legitimately ask you for your password, inspect you machine for devices attached to your USB ports or added to your keyboard, etc. If you see any strange machine or device hooked to network or laying around how to report it, how to handle phone calls asking for information, etc.

6.7. Terminated Employees: Technology Services must be immediately notified of the pending termination of any employee regardless of the reason. Reinstatement of terminated employee files must be approved before access can be granted.

7. Network Security:

An "access node" is a point on a network through which you can access the system. If even one such point is left unsecured, then the entire system is at risk. All modular jacks and wireless base stations represent potential nodes to which a computing device could be attached.

7.1. Protection of cables and wires:

All cabling and wires should be protected as much as possible. This means they should reside in trays in cubicles or within walls or ceilings. If a sophisticated intruder can access a span of cable that is used as a connector between pieces of equipment, he or she may be able to access the entire system.

7.2. Boot secured servers:

Secure all servers so they cannot be booted from removable devices or their BIOSs altered with administrative access.

7.3. Screen savers:

Screen savers with mandatory locking features should be installed on all staff machines to prevent information from being read by anyone who happens to be walking past the display monitor. They should be set to activate after no more than 10 minutes on inactivity.

7.4. Firewalls:

Firewalls must be installed at all external access points: Only allow trusted (authenticated) messages to pass into your internal network from the outside. Only predefined ports may be opened.

7.5. Intrusion detection:

In conjunction with its firewalls, WCSD will maintain intrusion prevention//detection software running in an appropriate configuration but probably within the firewall's demilitarized zone (DMZ). Such software will detect possible intrusions, hacks, or other exploits aimed at compromising the system.

7.6. Modems:

Only in very special cases should a modem be necessary. There is no need to provide a viable line of access to and from the system unless it's absolutely necessary. A modem could provide just such access.

7.7. USB Drives:

Hacked USB drives inserted into machines with auto-run enabled and can run malicious code and act as a means of disseminating Trojans and other spyware. USB and for that matter CDs and DVDs must be from reliable sources. Beware of freebie USB drives picked or given as gifts. Consider disabling auto-run on all machines and USB ports on all but the ones that really need them.

Special care must also be taken when placing data of any sort, especially confidential data on a USB due to ease by which they can be lost or misplaced. In general, USBs should be avoided as a means of moving any type of sensitive data even if encrypted.

7.8. Internet Access:

Internet access is granted to all district account users. Users need to be aware that some type of filtering will be in force for all.

7.9. Job related sites: Remind all users that the Internet (and all system activity for that matter) is for approved use only: There are countless Internet sites and activities that have no positive influence on the public education environment.

7.10. Acceptable Use and Confidentiality Agreements:

All users are required to sign WCSD's Acceptable Use and Confidentiality agreements before receiving access to the network. Signed and filed agreements verify that users have been informed of their responsibilities and understand that they will be held accountable for their actions.

7.11. Placement of Resources and Firewall:

All servers, data and information that are intended for direct access by external and in many cases public users must be located outside of the firewall or in a

DMZ sub-network. These will generally be static web pages. Dynamic pages which retrieve data from backend databases will make secure calls to those databases which will reside behind firewalls.

7.11.1. WCSD's public Web servers that are intended to provide information and services to the public must be located in such a DMZ. Such Web servers must not be able to access confidential information that resides inside the firewall. This way, if the public Web server should ever be compromised, confidential information is still protected. All development for such Web servers must take place within a testing environment within the network.

7.12. Protection of transmissions sent over the Internet:

7.12.1. SSL: Secure Sockets Layer (SSL) Servers must be used to secure all private information transactions made with a Web browser: In a secure Web session, the Web browser generates a random encryption key and sends it to the Web site host to be matched with its public encryption key. The browser and the Web site then encrypt and decrypt all transmissions

7.12.2. Digital signatures/certificates: Wherever possible digital signatures are recommended for transmission of sensitive documents over the network via e-mail of other means. By requiring an authentication agent or digital certificate, you force the person on the other end of the transmission to prove his or her identity. In the digital world, trusted third parties can serve as certificate authorities--entities that verify who a user is for you.

7.12.3. Secure Cloud Storage: WCSD has established a secure storage site where authentication is required and all transmissions to and from the site are encrypted. All files whether or not they contain private or otherwise sensitive information coming into or leaving WCSD network must make use of this site. All files are included. If we provide any place to transfer files that is not secure the chance of data being placed there is a risk.

7.13. Virus Protection

7.13.1. Client antivirus, anti-spyware and firewall software: All devices, clients and servers attached to WCSD network must have the district's prescribed antivirus, anti-spyware and firewall software installed.

7.13.2. Installation: All machines come to the user with the antivirus, anti-spyware and firewall software agents pre-installed by network staff. .

7.13.3. Upgrade/Updates: All updates/upgrades to either the antivirus engine or data files (used to identify virus signatures) are automatically pushed to the individual client machines at logon. Likewise for anti-spyware and personal firewalls.

7.13.4. Monitoring: All clients are monitored for currency of their antivirus, anti-spyware and firewall software. Sometimes machines are so infrequently attached to the network or the automatic updating is unsuccessful that

manual intervention is required.

7.13.5. Communication with vendor: Although the latest data/ID “patches” are automatically pushed to WCSD by the vendor, WCSD network staff also monitors vendor initiated and other virus and spyware alerts.

7.13.6. Response to attacks: In the case of an actual virus or other attack a response plan has been established.

7.14. Backups – WCSD has long had in place a comprehensive back up system of some sort.

7.14.1. Hardware Scope: All servers are backed-up as well as critical operating software for various switches, routers and firewalls. Individual client workstations are not backed up and users are so advised to keep any important data on network servers.

7.14.2. Software scope: All original operating system software, along with service packs and other upgrades, are securely backed up and kept offsite. Also all commercially purchased and custom developed software are also backed up and kept offsite. This includes all application software.

7.14.3. Backup hardware and software: WCSD uses the latest versions of nationally known and highly rated backup software and the models of popular backup drives. Service and support contracts are in place for all backup software and hardware.

7.14.4. Data scope: All user “U:” drives and Cloud storage drives are backed up. Also, all database software, documents, web pages etc. are backed-up on all servers.

7.14.5. Backup schedule: (see Appendix F)

7.14.6. Encryption: Backup software includes an encryption option when backing up sensitive information to ensure that unauthorized users cannot access backup files.

7.14.7. Verification: WCSD’s backup software allows for verification of backups to ensure they are written to the disk or tape accurately:

7.14.8. Rotation of backup media: New media space is routinely cycled into the backup library in sets and ones that have gone through too many backup cycles are replaced.

7.14.9. Logs: Logs of all backup dates, locations, and responsible personnel are kept on a daily basis. They are very important if and when data of any type needs to be retrieved form offsite storage.

7.14.10. Test of backup system: In the course of normal events the backup system is periodically tested when users ask to retrieve some data that was accidentally deleted. Restorations of full servers should also be

tested. More comprehensive restorations exercises are also scheduled.

7.14.11. Off-site location for critical backup copies: Backups of any and all software, databases, and information that serve critical functions reside in a very secure off-site location and are readily accessible when and if needed. Backup data is treated with the same level of confidentiality as production copies. Periodically checks are made to make sure the backups function as expected.

7.14.12. Off-site frequency: Backups are made to the offsite storage and are rotated on a regular basis.

7.15. Inventories:

Inventories of all assets are maintained, including information (data), software, hardware, documentation and supplies. For each server, client workstation and networking device there is included: the manufacturer's name, model, serial number, and other supporting information like operating system, date of install and responsible party.

8. Training.

8.1. Keep the Acceptable Use Policies and this WCSD Security Plan visible throughout the workplace (e.g., banner pages, posters, FYI memos, and e-mail broadcasts).

8.2. Security training in general

8.2.1. Training should be tailored to meet the requirements of the security policy and staffing needs.

8.2.2. Many computer users have never been trained to properly use technology. At most, they many have learned only how to use a particular piece of software or a specific application or two.

8.2.3. The majority may have little understanding of security issues, and there is no reason to expect that to change unless the organization does its part to correct the situation.

8.2.4. Staff must be adequately prepared for making security policies a part of the work environment.

8.3. Training schedule:

In addition to new employee training sessions, security refresher workshops should also be held.

8.4. Reference materials:

Whenever possible develop and distribute reference materials (e.g., checklists, brochures, and summaries).

8.5. Notification: Employees will be told in writing:

8.5.1. What is and is not acceptable use of technology resources.

8.5.2. What the penalties for violating regulations will be.

8.5.3. That their activities may be monitored.

8.5.4. That district computers are not for personal use and must not be misused

8.5.5. There should be no expectation of privacy for personal employee information stored on or transmitted with the organization's technology infrastructure. This will pertain mostly to e-mail

8.6. Acceptable Use and Confidential Policies Acknowledgements

Employees are required to sign the district acceptable use and confidentiality agreements that include security provisions to acknowledge that they are aware of their responsibilities and verify that they will comply with these policies. This requires that:

8.6.1. Staff should have ample opportunity to read and review all policies and regulations for which they will be held accountable.

8.6.2. Staff should be provided an appropriate forum for clarifying questions or concerns they may have about the organization's expectations.

8.6.3. Staff should not be given access to the system until signed agreements are accounted for and maintained in a safe place.

8.6.4. All new employees should be expected to meet the organization's security requirements and procedures as a part of their job description. Once hired, new employees should be informed of, and trained on, acceptable use and security policies as a part of their initial orientation in order to impress the importance of security upon them.

8.7. Security Training Outline

8.7.1. Raise staff awareness of information technology security issues in general.

8.7.2. Include broad overview

8.7.2.1. What is information security?
8.7.2.2. Why does it matter?

8.7.3. Ensure that staff are aware of local, state, and federal laws and regulations governing confidentiality and security

8.7.4. Stress Federal laws

8.7.4.1. FERPA overview
8.7.4.2. FERPA relevance and application (include specific examples that relate to audience duties)

8.7.5. Stress state laws, regulations, and standards including GRAMA (Government Records Access and Management Act)

8.7.6. Explain organizational security policies and procedures.

8.7.7. Ensure that all employees understand that security is a team effort and that each person has an important role to play in meeting security goals and objectives.

8.7.8. Train staff to meet the specific security responsibilities of their positions.

8.7.9. Inform staff that security activities will be monitored.

8.7.10. Remind staff that breaches in security carry consequences.

8.7.11. Assure staff that reporting potential and realized security breakdowns and vulnerabilities is responsible and necessary behavior (and not trouble-making).

8.7.12. Stress that unintentionally destructive acts (e.g., accidental downloading of computer viruses, programming errors, and unwise use of magnetic materials in the office) are the source of many security risks.

8.7.13. Review results of risk assessment findings along three broad areas that include: assets, threats and vulnerabilities.

8.7.14. Review WCSD security policies, procedures, and regulations within the main areas and focus on those related to audience's duties.

8.7.14.1. Physical security regulations

8.7.14.2. Information security regulations

8.7.14.3. Software security regulations

8.7.14.4. User access security regulations

8.7.14.5. Network security regulations

Appendix A

PRIVACY AND WCSD DATA

FERPA

1. ***Purpose:*** The federal Family Education Rights and Privacy Act assures parents access to their students' education records and protects the parents' and students' right to privacy by limiting the availability of student records without parental consent.

2. ***Rights established by FERPA:*** There are three general rights: (1) the right to inspect and review education records relating to the student and maintained by the school the child attends or has attended; (2) the right to challenge and require the school to amend a record concerning the student that is inaccurate, misleading or otherwise in violation of the student's privacy rights; (3) the right to require the school to obtain written consent prior to the disclosure of personally identifiable information, subject to specific exceptions.

3. ***"Education records":*** Usually defined as "…those records, files, documents, and other materials which contain information directly related to a student; and are maintained by an educational district or institution …" regardless of the format the record is in. The definition includes personally identifiable information about students collected and maintained by WCSD. This would include student test answers, it does not include the actual tests.

4. ***Parental Consent NOT required:*** WCSD does not need to have parental consent to provide data:
   a. ***That is not personally identifiable—***aggregate test scores, for example.
   b. ***To school officials, including teachers, who WCSD determines have a legitimate educational interest in the student.*** This might include disclosing the information to the student's teacher, but might not include disclosing it to someone the teacher says should see it.
   c. ***To officials of another school, school system or postsecondary institution where the student seeks or intends to enroll.***
   d. ***To the comptroller general of the United States or the Secretary of Education of state and local educational authorities*** *in connection with an audit or evaluation of federal or state supported education programs, or for the enforcement of or in compliance with requirements related to those programs.*
   e. ***To an organization conducting studies on behalf of WCSD*** *to (A) develop, administer or evaluate predictive tests; (B) administer student aid programs; or (C) improve instruction.*
   f. ***To accrediting organizations*** *to carry out their accrediting functions.*
   g. ***To the parents of the student,*** *custodial or non-custodial.*
   h. ***To comply with a judicial order or subpoena****, though the district must make a reasonable effort to notify the parents about the subpoena before complying with it.*
   i. ***In connection with a health or safety emergency****.*

5. ***When disclosures are made:***
   a. WCSD must create a log whenever it provides personally identifiable information to someone other than the parents. The log should include: (1) the parties who have requested or received the education records; and (2) the legitimate interest the parties had in requesting and obtaining the records. The log should also include the date the request was received and the date records were actually provided.
   b. WCSD may charge for the reasonable costs of producing records and need not provide the records in any particular format.
   c. If a parent requests a record, WCSD has 45 days to make the record available. FERPA gives parents the right to "inspect" the record, which does not include having copies sent to them. The only time FERPA requires copies is if refusing to copy the record would effectively deny the parent access to the record, i.e. if the parent lives in another state.

6. ***What records does WCSD maintain that would be subject to FERPA?***
   d. Test scores attributable to an identifiable individual. Parents have a right under FERPA to see the results of their student's tests. Parents **do not** have a right to see the actual state tests.
   e. Aggregate data that identifies the student because the numbers are so small. For example, an aggregate of the ethnic students who dropout of a particular school or even a district may include so few Asian students that the students become identifiable because there are only two Asian students in the district. Data that does identify students in this matter must be used in compliance with FERPA.
   f. Student enrollment data. WCSD is **not** a general source of information regarding the location of students. Persons seeking to know where a student is enrolled must be the parent of the student and/or have court documentation requiring WCSD to release the data, per FERPA

7. **Additional FERPA Information**

   FERPA which became law in 1974 has been amended many times since it became law. In protecting the privacy of student education records the law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education FERPA Fundamentals. See:
   http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html

   FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level. Students to whom the rights have transferred are "eligible students.

      i. Parents or eligible students have the right to request that a school correct records which they believe to be inaccurate or misleading. If the school decides not to amend the record, the parent or eligible student then has the right to a formal hearing. After the hearing, if the school still decides not to amend the record, the parent or eligible

student has the right to place a statement with the record setting forth his or her view about the contested information.

ii. Schools must have written permission from the parent or eligible student in order to release any information from a student's education record except for those cases listed in part 4 above

iii. Schools may disclose, without consent, "directory" information such as a student's name, address, telephone number, date and place of birth, honors and awards, and dates of attendance. However, schools must tell parents and eligible students about directory information and allow parents and eligible students a reasonable amount of time to request that the school not disclose directory information about them. Schools must notify parents and eligible students annually of their rights under FERPA. The actual means of notification (special letter, inclusion in a PTA bulletin, student handbook, or newspaper article) is left to the discretion of each school.

b. FERPA and WCSD. WCSD collects large and detailed amounts of data from schools each year including data about individual students within the Utah public education system.

i. Although these data are necessary for accurate state and federal accountability reporting, many of these data sets are essentially “on loan” from the individual school districts of Utah. Usually only the districts ever release such data to outside parties. Therefore WCSD does not, as a general rule, ever release a district’s student level data unless it is back to the originating/owning district or to a research entity that has been granted permission by the district(s) involved. The federal government does not receive individual student level data, just aggregates of some sort.

ii. The identity of a student is masked as much as possible. No names are associated and linking identifiers or keys have been encrypted to prevent such linking and identification of individual students from the district accessible portion of the Statewide Student Identifier (SSID) system.

GRAMA—Government Records Access and Management Act

1. Teacher records: CACTUS records are not protected by FERPA. Anyone can request access to CACTUS data, but GRAMA only requires WCSD to provide certain specified information about employees: work phone numbers and addresses, gross compensation, job descriptions and the teacher’s qualifications for the job, such as college degrees earned.
2. WCSD must respond to a GRAMA request within 10 days of receiving it. The response may be “no, and here’s why (the information doesn’t exist, you aren’t entitled to receive it, etc),” “Yes, and here you go,” “yes to the attached items and no to the rest of your request,” or “yes, but we need x number of

days or weeks to compile the data." GRAMA requests for anything other than data that is clearly public record should be forwarded to WCSD Legal for review.

Appendix B

WCSD Admin users Guide
2014-15

Definitions:

Standard User: Most WCSD users, about ninety percent, fall into this category. These users have full access to WCSD services and, where appropriate, they have permission to write to certain directories on certain servers. The services include among others: e-mail, customer applications, Internet browsing, desktop productivity tools (word processing, spreadsheets etc.), as well as the ability to store data on local storage devices and sync handheld devices. What a standard user cannot do is alter the basic configuration of or install software on district computers. As with the other user definitions given here, this a general one. Actual definitions can be customized according to multiple sets of rights (e.g changing the system time, installing DLLs) and permissions (e.g. read only, write).

Master User: This user generally has complete access to all WCSD technology resources. There should probably no more than a handful of master users in the organization. Such users can install and configure servers as well as desktop machines. They can control the access and permissions other types of users have to technology resources.

Admin user: An admin user is closer to a standard user in capabilities than to the master user, having a similar range of rights and permissions. The admin user has more control of the local machine than the standard user. While the standard user can save data on the local machine and change certain properties such as desktop themes, the admin user can install software after receiving permission from the network administration staff. The software the admin user can install may include new versions or enhancements to the basic operating system or other system software such as PDA synchronization devices. In the case of an admin user who is also a WCSD Zone Administrator, they will also be able to perform those same services for standard users within their zone.

Qualifying to be an Admin user:

- Network Professionals: By definition, administrative users, who are almost always professional network specialists and are very limited in number, are also admin users.

- Zone Administrators and System Support Specialists: By nature of their special assignments, in sections where such individuals have been designated, they are power uses. In some cases, due to the duties specific to their assignments they may have even more rights and permissions than the typical admin user. Examples include someone who needs to grant security permissions to users on a server or install software on other users' machines.

- Developers/Programmers/Web Masters: Anyone who develops custom software may have a need to have greater access to their local machine resources than a standard user. Such positions frequently require the installation and removal of various types of software that include but are not limited: to software development software, database systems, and software management tools.

- Other users who may qualify as admin users: Although requests for the status of admin user will ultimately have to be considered on a case-by-case basis by the professional network staff and, require the sign-off of the requesting user's supervisor; the following is a representative list of those who may qualify. Ultimately, qualification depends on the scope and frequency of activities such as those described herein.

    - Curriculum specialists who frequently need to evaluate various computer based instructional packages from commercial and other sources

    - Media specialists who often need to install software used in the production of media or various computer based instructional packages from commercial and other sources

    - Statisticians who frequently need to install and/or upgrade software required to do various types of statistical analyses

    - Others who can demonstrate admin user needs similar to those described herein.

Procedures:

- The prospective admin user can be identified either by himself or herself, a supervisor, or the network staff.

- The prospective admin user is required to submit a written request to WCSD IT Manager explaining admin user status should be granted. This request must be signed by his or her supervisor or forwarded via e-mail from his or her supervisor.

- The IT Manager along with network administration staff will review this request and notify the applicant and supervisor whether or not they agree with the request. If the request is agreed upon the applicant will be granted appropriate rights and permissions.

- While functioning as an admin user, the user is still required to follow the district's acceptable use policy.

- The admin user must always notify network staff what software they are planning to install before doing so. Network staff will review and respond to these requests as top priority items. Special arrangements may have to be made in some cases to cover emergency situations.

- The admin user must be especially vigilant to ensure against installing any unlicensed software.

- In the event the admin user has technical problems with his or her machine as a result of some installation or modification they perform, and need assistance, they will need to submit the usual help desk request. Their status as admin users does not imply priority service from the network staff.

If the admin user encounters repeated problems requiring network staff intervention, they may be referred to additional training or have the admin user status revoked.

WCSD Admin user and Local Administrator Agreement

I have requested _____ privileges on WCSD
(Admin user or Local Administrator)

devices on the WCSD network, and agree to the following:

1. I attended WCSD Admin user and Local Administrator Security Training on

   _____.
   (Date)

2. I will not add, remove, or disable ***any software*** on devices under my control without IT permission.

3. I will not add, remove, or modify any local administrator accounts without IT Permission.

4. In the event that any software fails to function properly on the above listed machine due to my not following this agreement, I will assume full responsibility. Should I require IT assistance, I will submit a help desk ticket and understand that IT assistance will be provided as their time permits.

5. I understand that violation of my administrator privileges will result in my privileges being revoked until further review.

Employee Signature: _____ **Date:**_____

Director: _____ **Date:** _____

-

Appendix C

WCSD Network Standards and Connection Policy

(Definitions of *bold & italicized* terms are listed at the bottom.)

Three classes of computers may connect to WCSD *network*. Please note the restrictions that apply to each class.

Owned by WCSD.

This computer may be connected directly to WCSD ***domain*** via cable.

All WCSD owned machines are purchased, installed, configured, and maintained according to ***WCSD hardware and software standards*** by network administrators.

Additional software may be installed only with the approval of WCSD network administrators. If WCSD owned computer is a notebook, it may also be used for ***telecommuting.*** It may be configured for ***VPN*** to access WCSD ***domain*** from the Internet or through WCSD ***wireless network segment***.

Employee owned and approved for *telecommuting*.

The employee must assure WCSD in writing the employee owned computer meets requirements for ***telecommuting***. This includes meeting WCSD ***secure computer*** requirements. ***VPN*** can be used to connect to WCSD ***domain*** over the Internet, usually from home. WCSD network administrators may not directly assist in the installation, configuration, or maintenance of an employee owned computer.

A WCSD employee who has had an employee owned notebook computer approved for ***telecommuting,*** may bring that device on site. However, it may only be connected to WCSD ***domain*** through proper credentials.

Only WCSD owned computers and employee owned computers approved for *telecommuting* may be connected to WCSD *wireless network segment* and to WCSD *domain* through *VPN* or any other means.

No other employee-owned devices are permissible and all connections must be made in the above manner. Machines in violation of this policy will be disconnected from the network, and the user will be denied further access until WCSD network administration has discussed the violation with the violator's supervisor. **Violators may be subject to disciplinary action**.

Privately owned and brought into WCSD by a business visitor.

A business visitor may access the Internet, but not WCSD ***domain***. To access the Internet they must receive permission along with current codes from a WCSD sponsor/host in order to connect to WCSD ***wireless network segment***. With these codes the business visitor is responsible for configuring, and establishing only a wireless Internet connection. If the business visitor does not have a wireless network

adapter, they may still connect to the Internet via cable and specially marked data jacks in conference rooms throughout the building.

The business visitor must be asked to assure their host they are using a ***secure computer*** and are willing to abide by the ***Acceptable Use Policy***.

WCSD is not responsible for lost data or damage to any privately owned machine that is connected to *WCSD wireless network segment* or WCSD *domain*.

Definitions

Acceptable Use Policy. All employees and business visitors, regardless of how they are connected to WCSD network are required to follow WCSD acceptable use policy. Also note the acceptable use policy states:

Also, please note the acceptable use policy states that the use of resources for personal reasons on a more than incidental basis or for mass distribution of chain letters, jokes, etc., or other uses that waste resources or disrupts performance, is prohibited.

This includes use of district machines for streaming audio and video when not work-related. **Violations of the acceptable use policy may be grounds for termination.**

Secured computer. In order to be secured, a computer must meet the following criteria. It must have the latest up-to-date virus protection software installed and running. The computer must also have strong-password protection and not have any of the following services running at any time it is connected to WCSD network: peer-to-peer networking, file-sharing, instant messaging, or network broadcasts of any kind. Virus protection software is available for home use by any WCSD employee. Please see a network administrator for a copy.

Telecommuting. WCSD employees may telecommute with management approval. In the application process Computer Services reviews and approves the telecommuter's computer configuration. While the telecommuter is given freedom to choose the employee owned computer's make and model; the machine must still be documented as being able to perform the tasks required of the telecommuter and be secure, posing no foreseeable threat to WCSD network. If the telecommuter desires to connect to WCSD ***domain*** through the Internet and ***VPN***, they must secure their own Internet connection and configure any employee owned machine to do so. Only general directions for ***VPN*** configuration and virus protection software installation will be available to those using employee owned machines for telecommuting.

WCSD domain. WCSD domain is the secure network of shared computers at WCSD. It is a subset of the more generally defined ***WCSD network***. The domain includes all servers and user computers, each connected to one or more of those servers. These machines are all behind a firewall and other security devices and software such as intrusion detection and filtering servers. When a user connects to WCSD domain from within the building by supplying a logon name and password they also receive Internet

access. Business visitors are permitted to connect to WCSD wiring infrastructure and obtain Internet access without connecting to WCSD domain. Such use is permitted only through WCSD ***wireless network segment***.

WCSD hardware and software standards. In order to maximize usability, reliability, security, and efficiency of WCSD information technology resources; WCSD has defined hardware and software standards. A summary of the current hardware/software standards will be published from time-to-time by the technology department. As part of WCSD standard setup features, these machines are all configured as ***secured computers***. Other hardware and software standards exist in WCSD, but most involve network infrastructure and custom application development and deployments. Always check with network administrators before purchasing software or hardware to see if it is compatible with WCSD network, and if a district license agreement (in the case of software) already exists.

WCSD network. WCSD network is defined as the entire computer infrastructure within WCSD including all wiring, communication devices, routers, switches, servers, desktops and other connected computers. WCSD ***domain*** is a subset of this network.

WCSD wireless network Segment. A secure wireless network segment is available for WCSD staff and sponsored business visitors. This network provides access to the Internet and optionally to WCSD domain via VPN. In order to connect to WCSD for Internet and/or WCSD domain access, WCSD employee or business visitor must first acquire the current wireless SSID (secure site ID) and WEP (wireless encryption protocol) codes and configure the computer to recognize and connect to WCSD wireless network segment. For security reasons these codes will change periodically. When this happens they will be distributed to all WCSD employees who have a VPN account. Currently WCSD supports the IEEE 801.11bgn wireless protocols.

VPN (virtual private network). VPN allows those with WCSD domain accounts to access WCSD network remotely or through the firewall. You must have a VPN account established by a WCSD network administrator before you can access the domain using VPN. Only general directions for VPN configuration and virus protection software installation will be available to those using employee owned machines for ***telecommuting***.

Appendix D

Information Technology Resources
Acceptable Use Policy

This statement of policy has been adapted (as of 1/26/98) from Appendices A and B to the State of Utah Information Technology Resources Acceptable Use Policy as adopted by the Information Technology Policy and Strategy Committee on August 15, 1996. It is also consistent with the UEN Public Education Acceptable Use Policy

WCSD/USOE characterizes as unacceptable and just cause for termination of use privileges, disciplinary action, and/or legal action, any of the following uses of information technology resources--e.g., computers, copiers, e-mail, fax, Internet, printed material, printers, video--provided by the district:

1. Illegal Use. Any use for or in support of activities that violate local, state, or federal laws.

2. Infringement of Intellectual Property Rights. Any use in violation of software license agreements or other contractual arrangements relating to the use of copyrighted information.

3. Commercial Use. Any use for commercial purposes or activities resulting in personal financial gain, including product advertisements.

4. Personal Use. Any use for personal reasons on a more than incidental basis or for mass distribution of chain letters, jokes, etc.

5. Offensive or Harassing Material. Any use of material which may be deemed vulgar, sexually explicit or disparaging of others based on race, national origin, sex, sexual orientation, age, disability, or political or religious beliefs.

6. Religious or Political Lobbying. Any use for religious or political lobbying.

7. Security Violations. Any action which threatens the security of district resources, including but not limited to such actions as: giving your password to another person; accessing accounts for which you are not authorized; or spreading computer viruses.

8. Confidential Information. Transmitting information classified as other than "public" under the Government Records Access and Management Act without proper security; or violating the privacy of others by reading e-mail or other private communications (unless you are specifically authorized to support communication systems).

9. Unnecessary Use. Otherwise appropriate use which intentionally wastes resources or disrupts performance by excessively consuming operating time, storage, paper, etc.

Appendix E

WCSD COMPUTER VIRUS RESPONSE PLAN

WCSD Anti-virus Environment

E-mail Servers - All incoming e-mail and attachments are scanned and cleaned, if necessary, by the IronPort, Barracuda SPAM, and anti-virus Firewall before going to the e-mail server. Signature files are updated on a daily basis. If an e-mail message or attachment is found to have a virus it is deleted, logged and replaced with a message notifying the user that this has occurred.

Servers - All servers, including e-mail servers, have a virus scan product installed to check on a daily basis for updated DATS (signature files). It is also checks on a biweekly basis for any upgrades of the anti-virus scanning engine. This product checks all files coming into the server for viruses.

Clients - All client Machines have a virus scan product installed in such a way that it checks on a daily basis for updated DATS (signature files). It is also checks on a biweekly basis for any upgrades of the anti-virus scanning engine. These products check all files coming into the computer for viruses.

Virus Outbreak Procedure

Virus attacks are an ongoing occurrence. Every day hundreds or thousands of infected e-mails arrive at the e-mail server. Over 99% of these are successfully intercepted by the IronPort or Barracuda SPAM Firewall (deleted and logged) and cause no damage. A virus can also be introduced from downloads or file copies from other magnetic media. In these cases, the vast majority are detected and deleted by the anti-virus software. However, on occasion, a machine or machines can get infected. The following is a procedure to be followed in these events. Note, that not every instance of an infection warrants network-wide response. Often the problem can be isolated and dealt with on one machine.

- As a regular preemptive step, the administrator should regularly check the log generated by the Firewall system to determine if WCSD network is being hit by a heavier that normal number of e-mails or virus contained in messages or attachments. Although the log indicates when viruses have be intercepted and "cleaned", either event may be cause to be on the lookout for other incidents.

- As soon as a reported problem (usually via the help desk) on a client machine or desktop looks as if it is a possible virus, the machine should be disconnected

from the network, until the machine can be fully scanned by the most current anti-virus software and it can be determined that it is free from any new undocumented virus.

- If a virus is identified, the anti-virus software web sites should be searched to determine the behavior or the new virus. If no virus is found, but an apparent infection has taken place, an attempt should be made to match the symptoms with those of newly reported viruses in an attempt to identify the cause of the infection. Again, the anti-virus software vendor web sites should be employed.

- Once the virus has be researched and identified. The directives from the web sites should be followed to mitigate the impact on the internal and external networks.

- If the virus is high risk or widespread, consideration should be made for either shutting down the e-mail server, disconnecting the internal WCSD network from the external (Internet) network or both. This decision should be made by the coordinator and communicated from the help desk by e-mail (if possible) to all users, or by phone if e-mail is not operable. In part, this decision may be made based on the volume of e-mail leaving the e-mail server for internal, or more importantly, external destinations. A rapidly increasing volume of e-mail may indicate the virus is being proliferated by WCSD's e-mail server.

- The decision to disconnect the network may also need to be made if the network or parts of the network are under attack from a hacker of some type. Such attacks will more than likely affect only isolated machines (clients or servers), but the potential exists for having to isolate the entire network.

- After all affected machine or mailboxes have been identified and the virus has been contained and cleaned, there may be the need to recovery corrupted data from backup servers or tapes. If the damage is widespread, ad hoc priorities by have to be defined and communicated concerning whose files and/or mail will be restored first.

- Finally, the incident should be described and logged, with recommendations for future prevention.

Appendix F

WCSD Back-up/Data File Recovery Procedures

Definitions:

Full	A full backup is a complete back up of files and the archive bit is reset.
Differential	A differential backup **does not** reset the archive bit and will back up all files that have changed since the previous resetting of archive bit.
Incremental	An incremental backup **does** reset the archive bit and will backup all files that have changed since the previous resetting of the archive bit.

Appendix G

RECOVERY OF LOST DATA AND HARDWARE

1. RECOVERY OF LOST DATA AND SOFTWARE

1.1 Lost data and software will usually be recovered by a network administrator from backup devices.
From now on any reference to lost data or recovery of data also implies loss or recovery of software (programs). All network servers are incrementally backed-up on a nightly basis with full system backups occurring during the weekends. In some cases, LAN policies, procedures, and installation notes are backed-up separately on diskette or smaller tape backup devices. This allows the recovery of the systems needed to "boot strap" the LAN and restore recovery subsystems. Also, some larger databases are not included in the incremental schedule since they would cause too much nightly volume. All users are encouraged to save any data worth backing-up on network devices to take advantage of these tape backups. Individual "local" client drives are not backed-up unless the user does so on his or her own and employs diskettes or a standalone tape backup sub-system.

An offsite backup set is kept at the offsite storage location for one year. When the month corresponding to the one on the set is passed in the next calendar year that set is returned to WCSD and recycled one time as full-system or incremental backup. The exceptions to this are the July backup sets. They are kept offsite indefinitely (at lease 5 years). If backup systems change, care must be taken to insure that backup set created before the system change can still be retrieved. Two incremental sets are created during the course of one "back-up month". The first is started on the Monday preceding the first Tuesday of the month. It is kept in for two weeks. On the second Monday following the first Tuesday, this first incremental backup set is removed and placed in the safe and a second incremental backup for the month is begun. Both incremental backup tape sets are sent off-site with the full-backup set for the new month on the first Tuesday of the new month.

1.2 Using backup/restore software, restore procedures may be performed for any server. Entire volumes (disk drive or disk array sub-system) may be restored as well as selected directories or individual files within a volume.

1.3 The amount of time required for any recovery will vary greatly depending on the volume of data lost, and how long ago the loss occurred. A full volume lost at the end of the month would require the recovery of the first of the month's full volume backup as well as any incremental backups which took place on intervening days.

1.4 In the event of catastrophic loss of data such as in a fire, flood or earthquake, the first useable full system tape backup set must be determined. If the current (last written) full system tape backup set were onsite and useable, then that set would be used, otherwise the most current set stored offsite would be used. Following

the restoration of the most recent available full system backup, any incremental backups which are intact and followed that backup should also be applied.

1.5 The estimated amount of time needed to recover the most current recoverable data in a worst case situation is 12 hours and would require the services of only one lan administrator. However, if the most current recoverable media is old (for example, a month or two) considerable time and effort will be needed to manually recover parts of the data. If any hardware necessary for recovery needs to be replaced before data recovery, that process would have to occur first. These procedures are discussed in the next section.

2. RECOVERY OF HARDWARE

2.1 The following is an analysis of the time required to restore district hardware to the state it was in before the disaster. It assumes a worst case scenario in which all hardware within the building, including the entire LAN room has been lost and must be replaced. Estimates of time and costs necessary for a “partial” disaster could be inferred from this information. Depending on the nature of the disaster which caused loss of hardware the activities described below may have to take place in a new or temporary facility.

With the exception of the LAN room the assumption is made that all necessary telecommunications wiring (Fiber, VOIP, data-circuits, wiring panels, and jacks) are in place and functional. If this is not the case additional time (anywhere from a few days to a few weeks) will be needed to install these network components. If we were dealing with a large earthquake this could be much longer. In any event outside communications may take much longer to establish than restoration of services within the district.

2.1.1 Rewiring of the LAN room in order to accommodate pre-disaster hardware would require about 24-36 hours of work. This assumes assistance from outside vendors which would help with connections to telecommunications panels and circuits.

2.1.2 Each device which makes up the LAN room component of the network will have to be reinstalled and configured.

2.1.3 In a worst case scenario all desktop client machines and network printers would also need to be replaced. The time necessary for the installation of each machine, which includes unpacking, assembly (including any special hardware installation) and software installation and configuration is estimated to be 1 hour per machine.

2.1.4 To estimate the total elapsed time necessary for recovery of all hardware to its pre-disaster state we need to consider: number and type of available staff, length of work week, actual time on task, and unforeseen contingencies.

2.1.4.1 Regardless of the number of qualified staff available the estimated 82 hours needs to be adjusted upward by some factor to account for: planning, actual time on task and unanticipated problems. For the purposes of this analysis we will set this factor at 1.4. Thus the real hours needed to recover hardware could be substantial. However it is possible that data and software recovery could begin before all servers are recovered thus saving some total elapsed time.

2.1.4.3 Finally we need to consider how much total elapsed time would be necessary for the replacement/recovery of desktop machines. While the LAN room hardware is being recovered it may be feasible that programming staff, LAN zone leaders (part-time “admin users”) and some of the specialists, could install and recover the desktop machines throughout the district. This may require some initial training (a few hours) from the LAN administration staff who are recovering the LAN room hardware and other specialists. The above applies to only computer hardware and not to other office equipment.