

USOE Information Technology Security Plan

1. Introduction.

This document, along with appendices, is a detailed description of security practices within the USOE. It is meant to be a dynamic plan that will, at least in part, be shared with 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 the USOE 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. The building is protected by a fire detection system.
- 3.1.2. Building access. All external doors, but one, are locked at all times and require an electronic key for entry.
- 3.1.3. Onsite Guard. Only one door is unlocked from the outside during business hours (7:00 AM to 5:30 PM) and monitored by a guard.
- 3.1.4. Surveillance cameras. The guard, during business hours, also has access to external and internal surveillance cameras.
- 3.1.5. Internal Building Access. After business hours all sections of the building except the main first floor hallway are also secured. The computer services section is in the basement of the building to which access is denied to all but authorized employees during non-work hours.
- 3.1.6. 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 USOE badges at all times within the building.

3.2. Network Room

- 3.2.1. Water damage. All hardware and wiring is elevated off floors in racks or trays of some sort. The fire prevention sprinkler system is dry loaded (no water immediately overhead), meaning that water can only be released if an actual fire triggers a valve behind the actual sprinkler system. A chemical based fire retardant system is being evaluated.
- 3.2.2. Physical Access. Only one inconspicuous door provides access to the network room and that door is secure by a key pad lock.
- 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 room. 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 and all UPSs are on a diesel powered generator backup power system which is 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 75 degrees Fahrenheit, automatic alarms are triggered and automatic phone calls are made to key USOE computer services staff and state DFCM (Division of Facilities and Construction Maintenance).

3.2.7. The HV/AC system is also on diesel powered generator backup power. When power is lost to the building the air conditioning continues to function for up to 24 hours by running off the diesel generated power. Without continuous air conditioning the heat generated by the electronic equipment would quickly cause the temperatures to rise to levels which would be hazardous to the electrical equipment.

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

4.1. Policy Statement. The Utah State Office of Education (USOE) makes every effort to abide by all applicable State and Federal guidelines, policies, regulations, statutes, and procedures pertaining to the confidentiality and privacy of data. The USOE 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. The USOE 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 the USOE maintains data. It is intended to be consistent with the disclosure provisions of the FERPA. All users of USOE 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 USOE or any employee, agent, or contractor of USOE.
- 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 USOE 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 the USOE 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

- 4.6.1. Data originated or stored on agency computer systems are USOE property. Employees will access only data that are required for their job. Employees will not make or permit unauthorized use of any USOE 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 Agency 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 USOE 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 USOE 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
- The USOE 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 USOE's criteria for approving research requests (See Appendix N).
 - 4.7.3. The recipient organization has signed the USOE Confidentiality Agreement.
- 4.8. Record of Access

The USOE shall maintain a record which indicates the name of any individual or organization external to USOE 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, the USOE 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. USOE 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 USOE data or information. Everyone sending data outside the agency 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, tapes, 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 floppy 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 USOE 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 surplusizing 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 the USOE 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 the USOE network, in consultation with USOE 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 power 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. For a list of software. (see Appendix C and Appendix D. Power users must sign a use agreement and receive special network training. (see Appendix O and Appendix P).

5.2. Storage of master copies.

Master copies of all software, licenses and documentation are retained in a secure location within the secure network room. Spreadsheets of licenses are maintained along with expiration and renewal schedules.

5.3. Approved Software.

Only USOE Computer Services approved and purchased software (see Appendix C) that is installed by USOE network staff or USOE power users may be used on USOE machines. With permission, power users may install individually purchased copies of software acquired personally or through their UOSE section. 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 a power user for the installation of any non-CS 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 Computer Services software license inventory to verify that no unlicensed software or software for which the USOE 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, Computer Services 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. (see Appendix E)
- 5.7.2. Authorization of software changes. Before anyone modifies or creates any software, a formal, written change request (see Appendix F) must be submitted to the IT director or an IT manager. Such requests must be signed by a section director or associate 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. (see Appendix G)

- 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 USOE 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 the USOE 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 are forced to change passwords at least once every 90 days.
- 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.
- 6.1.14. There have been questions about people wanting to keep their passwords the same across multiple systems such as: BASE, CACTUS, local network, PATI, AIMS, and IRIS. This is not a recommended practice. If your password were the same across multiple systems then a hacker who cracks one password would be able to access all of the other

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 must be installed on all user 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, the USOE 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 should be granted to employees only to the extent they need it to perform their jobs. More and more staff are finding useful, job related, services on the internet. However, some job functions do not require unlimited access. At least some 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 the USOE's Acceptable Use and Confidentiality agreements before receiving access to the network. Signed and filed agreements (see Appendix I and Appendix M) 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. The USOE'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.

7.11.2. After testing, public web pages are published to a staging Web server inside the firewall that continually synchronizes or updates the production Web server outside the firewall. If the public Web server ever fails it can be quickly be rebuilt from this staging Web server.

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 or 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 FTP: The USOE has established a secure FTP 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 the USOE 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 the USOE network must have the agency'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 the USOE by the vendor, the USOE 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. (see Appendix J).

7.14. Backups – USOE Computer Services 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: USOE 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 "H:" drives and group "G:" drive are backed up. Also, all database software, documents, web pages etc. are backed-up on all servers.
- 7.14.5. Backup schedule: (see Appendix K)
- 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: USOE'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 tapes: New tapes are routinely cycled into the tape library 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 from 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: Tapes are transported to offsite storage and are picked up on a weekly basis.
- 7.15. Disaster Recovery/Contingency plans:

In 2002 the USOE, in general, developed its first comprehensive contingency

and disaster recovery plan. Information Technology was a big part of that plan. The plan is now reviewed and updated twice a year in December and June. The contents of the plan are burned to multiple CD ROMs and distributed to key agency personnel including an associate superintendent, the IT director and the network administrator. Among other items it contains: all emergency contact numbers, hardware inventories; network diagrams; descriptions of how and where all software and data are backed up; formatted descriptions of all USOE systems; circuit lists; and a plan for rebuilding the data center from scratch – (see Appendix L)

7.16. 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.

7.17. Cold or off-site facility:

Although a "cold" site that includes everything necessary for resuming operations is not sitting ready and stocked with all the necessary equipment to get up and running after a disaster; the disaster recovery/contingency plan does include some recommended possible sites. Such sites, of course, must have the necessary access and services such as power and telecommunications. After assessing the risks to the USOE the disaster recovery/contingency plan committee decided some delay (up to two weeks) was acceptable, and that the expense to rebuild the entire network can be incurred if and when necessary. The committee identified at least two potential cold sites which have been contacted, and the USOE has received permission to use those sites if necessary. This information is kept as part of the disaster recovery/contingency plan (see Appendix Q).

8. Training.

8.1. Keep the acceptable Use Policies and this USOE 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. Help Desk:

The USOE help desk must be continually promoting security by being alert for situations that might compromise the safety of the USOE network and be ready with security advice and recommendations to individuals and groups of individuals.

8.5. Reference materials:

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

8.6. Handbook:

Keep the USOE HR rules and employee handbook updated with relevant and current security policies, including the following:

8.6.1. Who approved the policies

8.6.2. Whose authority sustains the policies

8.6.3. Which laws or regulations, if any, on which the policies are based.

8.6.4. Who will enforce the policies

8.6.5. How the policies will be enforced.

8.6.6. Whom the policies affect.

8.6.7. What information assets are being protected

8.6.8. What users are actually required to do

8.6.9. How security breaches and violations should be reported

8.7. Notification: Employees will be told in writing:

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

8.7.2. What the penalties for violating regulations will be.

8.7.3. That their activities may be monitored.

8.7.4. That agency computers are not for personal use and must not be misused

8.7.5. 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

8.8. Acceptable Use and Confidential Policies Acknowledgements

Employees are required to sign the agency acceptable use and confidentiality agreements that include security provisions (see Appendix I and Appendix M) to acknowledge that they are aware of their responsibilities and verify that they will comply with these policies. This requires that:

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

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

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

8.8.4. 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.

8.9. Security Training Outline

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

8.9.2. Include broad overview

8.9.2.1. What is information security?

8.9.2.2. Why does it matter?

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

8.9.4. Stress Federal laws

8.9.4.1. FERPA overview

8.9.4.2. FERPA relevance and application (include specific examples that relate to audience duties)

- 8.9.5. Stress state laws, regulations, and standards including GRAMA (Government Records Access and Management Act)
- 8.9.6. Explain organizational security policies and procedures.
- 8.9.7. 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.
- 8.9.8. Train staff to meet the specific security responsibilities of their positions.
- 8.9.9. Inform staff that security activities will be monitored.
- 8.9.10. Remind staff that breaches in security carry consequences.
- 8.9.11. Assure staff that reporting potential and realized security breakdowns and vulnerabilities is responsible and necessary behavior (and not trouble-making).
- 8.9.12. 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.
- 8.9.13. Review results of risk assessment findings along three broad areas that include: assets, threats and vulnerabilities.
- 8.9.14. Review USOE security policies, procedures, and regulations within the main areas and focus on those related to audience's duties.
 - 8.9.14.1. Physical security regulations
 - 8.9.14.2. Information security regulations
 - 8.9.14.3. Software security regulations
 - 8.9.14.4. User access security regulations
 - 8.9.14.5. Network security regulations

PRIVACY AND USOE 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 agency or institution ..." regardless of the format the record is in. The definition includes personally identifiable information about students collected and maintained by USOE. This would include student test answers, it does not include the actual tests.
4. **Parental Consent NOT required:** USOE 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 USOE 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 USOE 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 agency 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. USOE 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. USOE 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, USOE 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 USOE 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. USOE 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 USOE to release the data, per FERPA

7. **Additional FERPA Information**

FERPA which became law in 1974 has been amended 29 times to date (20 U.S.C. § 1232g; 34 CFR Part 99). 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 USOE. The USOE 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 the USOE 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 USOE 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. USOE 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 USOE Legal for review.

DRAFT

USOE Power Users Guide 03-11-2004 (to be revised)

Definitions:

Standard User: Most USOE users, about ninety percent, fall into this category. These users have full access to USOE 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 agency 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).

Administrative User: This user generally has complete access to all the USOE technology resources. There should probably no more than a handful of administrative 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.

Power User: A power user is closer to a standard user in capabilities than to the administrative user, having a similar range of rights and permissions. The power 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 power user can install software after receiving permission from the network administration staff. The software the power 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 a power user who is also a USOE Zone Administrator, they will also be able to perform those same services for standard users within their zone.

Qualifying to be a Power User:

- **Network Professionals:** By definition, administrative users, who are almost always professional network specialists and are very limited in number, are also power users.
- **Zone Administrators and Automated System Support Specialists:** By nature of their special assignments, in sections where such individuals have been designated, they are power users. In some cases, due to the duties specific to their assignments they may have even more rights and permissions than the typical power 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 power users: Although requests for the status of power 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 power user needs similar to those described herein.

Procedures:

- The prospective power user can be identified either by himself or herself, a supervisor, or the network staff.
- The prospective power user is required to submit a written request to the USOE IT Manager explaining power 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 a power user, the user is still required to follow the agency's and state's acceptable use policy.
- The power 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 power user must be especially vigilant to ensure against installing any unlicensed software.
- In the event the power 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 power users does not imply priority service from the network staff.

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

USOE Power User and Local Administrator Agreement

I have requested _____ privileges on the
(Power User or Local Administrator)

following machine: _____, and agree to the following:
(Machine Name)

1. I attended the USOE Power User and Local Administrator Security Training on _____.
(Date)
2. I will not add, remove, or disable **any software** on the above machine without IT permission. (See the USOE Software Approval Form to request 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 box 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:** _____

Division Director: _____ **Date:** _____

(July 27, 2005)

Appendix C

DRAFT

DATABASE SOFTWARE				
Access 2.0	MS	x	x	
Access 7.0	MS	x	x	
Works for Mac	MS	x	x	
PRESENTATION SOFTWARE				
PowerPoint (Win 3.1)	MS	x	x	
PowerPoint (Win 95)	MS	x	x	
PowerPoint for Mac	MS	x	x	
WordPerfect Presentation (Win 3.1)	Corel	x	x	
WordPerfect Presentation (Win 95)	Corel	x	x	
Astound	Gold...			
OTHER DESKTOP SOFTWARE				
Calendar Creator Plus				
WinZip 3.x				
WinZip 95				
PK Zip Utilities				
Windows 95 Plus	MS	?	?	
Informs	Novell	x	x	
Slide Sshow Screen Saver				
PageMaker for Mac	Aldus			
PageMaker for Windows	Aldus			
Microsoft Project (Windows)	MS	x	x	
Norton Utilities for Windows	Symantic			
Norton Utilities for Mac	Symantic			
PageMill HTML Editor				
FrontPage HTML Editor	MS	x	x	
SAM Anti Virus for Mac				
PowerBuilder (Enterprise Developer)	PowerSoft	x	x	x
Harvard Graphics	SPC	x		
LAN Workplace (Win)	Novell	x	x	
Desktop DBA	Datura			
Net FAX				
SQA Team Test				
Natural Connection	Software AG	x		
ECS (Job Scheduler)		x		
Realia Cobol	CA	x		
Robo Help	Blue Sky			
Erwin	Logic Works			
Falcon	Phoenix	x	x	
SNA				
FiNet				
Rumba	Wall Data	x		
Visual Basic	Microsoft	x	x	
DSDesigner (FiNet)				
Sybase Sql Anywhere	Sybase	x		
SPSS for Windows				
Quattro Pro V.7	Corel			
Nutri Kids				
Disney Interactive				
MS Frontpage	MS			
MS Publisher	MS			
MS Works (Windows)	MS			
PrintShop Deluxe				

DRAFT

USOE (Agency) CUSTOM SYSTEMS

Division	Name	Purpose	Hardware	Network
Agency Support	CACTUS	Statewide tracking of certificated educators	Intel	UEN
Agency Support	AFR	Annual Financial Report from school districts	Intel	UEN
Agency Support	S3	Annual Student Statistical Reports (Year End, Fall, Class Size, Adult Ed etc.)	Intel	UEN
Rehabilitation	IRIS	Integrated Rehabilitation Information System (clients & payments)	Intel	ITS
Agency Support	Minimum School	Disbursement of funds to school districts, detailed revenue & recipient accounting	IBM Mainframe	ITS
Agency Support	Transportation	Collection and accounting of school busing data	Intel	UEN
Agency Support	Network Inventory	Local LAN resource control	Intel	Local LAN only
Agency Support	Warehouse	State and Federal Reporting	Intel	UEN
Instructional Services	AIMS	Approved and pending Instructional materials database	Intel	UEN

USOE (District) CUSTOM SYSTEMS

Name	Purpose	Software	Database	External Interfaces
Student Information System Mainframe	Student Service Applications	Cobol MVS	Adabas/VSAM	School Districts
SchoolNet	Student Service Applications	Visual Foxpro	SQL Server	School Districts
Fiscal Systems Mainframe	Financial Services	Cobol MVS	ADABAS VSAM	School Districts
Fiscal Systems Micros	Financial Services	Foxpro 2.6	Foxpro	School Districts
Testing Systems	Scanning and Scoring of statewide CRT and SAT tests	Cobol MVS Visual Foxpro	Adabas VSAM	
Clearinghouse	Collection and distribution of ACCT & Student DATA	Foxpro Cobol MVS	Sybase 1.1x	
District Billing	Billing Statements to Districts for Services	Cobol MVS	VSAM	

Appendix D

USOE SOFTWARE LICENSES

DRAFT

Company	Product
Adobe	Acrobat 5.0
Adobe	Fireworks 4.0
Adobe	Paintshop Pro 6
Adobe	Photoshop 6.0
Adobe	Photoshop 7.0
Adobe	Pagemaker 6.5
Bluesky	Robohelp
Boreland	Jbuilder
Cisco	Advantage Firewall PIX 525 Maintenance
Computer Assoc	ERWin
Computer Assoc	Desktop DBA
Corel	Office Suite Standard Edition
Corel	WordPerfect 6
Embarcadero	DBArtisan
eEye Digital Sec	Retina Professional Edition-32 IP Pack 4.0 Windows
Harvard	Harvard Graphics - Obsolete?
IDM Computer S	UltraEdit-32
InstallShield	InstallShield 5.5
LinkPro	Powersync Server
Lotus	ScreenCam NU WIN/NT 5.0
Macromedia	Dreamweaver 4.0
Macromedia	UltraDev 4.0
McAfee	Active Virus Defense Suite
Microsoft	Exchange CAL 2000
Microsoft	Windows CAL 2000
Microsoft	Project 4.1
Microsoft	Publisher 97
Microsoft	Visual Basic 5
Microsoft	Frontpage 97
Microsoft	Frontpage 2000
Microsoft	Exchange ACD Exch Conn V5.0 B
Microsoft	Exchange ACD Exch Intnet Mail B
Microsoft	Exchange ACD Exch Srv Ent v5.0 B
Microsoft	Exchange ACD Win NT Srvr v4.0 Lev
Microsoft	Multiview Viewer Royalties for 105 copies
Microsoft	Office Professional 2000
Microsoft	Office Professional XP
Microsoft	Windows 98 Upgrade
Microsoft	Windows XP
Microsoft	Windows 2000 Professional
Microsoft	Windows Terminal Services CAL
Microsoft	Windows Terminal Services Internet Connector 2000
Microsoft	Powerpoint 2000
Microsoft	Paintshop Pro 7
Microsoft	Windows Advanced Server 2000
Microsoft	Windows Server Enterprise 2003
Microsoft	Windows NT Server 4.0
Microsoft	SQL Svr 2000
Microsoft	Visio Pro 2002
Nemx	Nemx Anti Virus MXS-R
Netopia	Timbuktu Pro 32
Network Associ	Sniffer Basic 3.5
Phoenix	Falcon 5 User, Networked
Powerquest	Drivelmage Pro
PowerQuest	Partition Magic

DRAFT

Appendix E

Software Development Life Cycles: Outline for Developing a Traceability Matrix

By Diana Baldwin, AccuReg Inc.

1. Software Life Cycle
 1. The FDA does not prescribe a specific software development life cycle, but requires manufacturers to identify and follow what makes sense for them
 2. Manufacturers choose a software life cycle model and development methodology appropriate for their device and organization
 1. Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices, May 1998
 3. Software Life Cycle must include:
 1. Risk management
 2. Requirements analysis and specification
 3. Design (both top level and detailed)
 4. Implementation (coding)
 5. Integration
 6. Validation
 7. Maintenance
 4. A software life cycle model should be understandable, thoroughly documented, results oriented, auditable, and traceable.
 1. Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices, May 1998
2. What is required to demonstrate traceability?
 1. Provide a traceability analysis or matrix which links requirements, design specifications, hazards, and validation. Traceability among these activities and documents is essential. This document acts as a map, providing the links necessary for determining where information is located.
 1. Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices, May 1998
3. How Does Traceability Ensure the Life Cycle is Followed?
 1. It demonstrates the relationship between design inputs and design outputs
 2. It ensures that design is based on predecessor, established requirements
 3. It helps ensure that design specifications are appropriately verified, that functional requirements are appropriately validated
 4. Important: Traceability is a 2-way street. Maintain "backwards" and "forwards" -- Tunnel Vision not acceptable in the Software Life Cycle!
4. Traceability Across the Life Cycle
 1. Risk Analysis (Initial and Ongoing Activities)
 1. Trace potential hazards to their specific cause
 2. Trace identified mitigations to the potential hazards
 3. Trace specific causes of software-related hazards to their location in the software
 2. Requirements Analysis and Specification
 1. Trace Software Requirements to System Requirements
 2. Trace Software Requirements to hardware, user, operator and software interface requirements
 3. Trace Software Requirements to Risk Analysis mitigations
 3. Design Analysis and Specification

1. Trace High-Level Design Specifications to Software Requirements
2. Trace Design Interfaces to hardware, user, operator and software interface requirements
3. Evaluate design for introduction of hazards; trace to Hazard Analysis as appropriate
4. Design Analysis and Specification
 1. Trace Detailed Design Specifications to High-Level Design
 2. IMPORTANT: Ability to demonstrate traceability of safety critical software functions and safety critical software controls to the detailed design specifications
5. Source Code Analysis (Implementation)
 1. Trace Source Code to Detailed Design Specifications
 2. Trace unit tests to Source Code and to Design Specifications
 1. Verify an appropriate relationship between the Source Code and Design Specifications being challenged
6. Source Code Analysis (Implementation)
 1. Trace Source Code to Design Specifications
 2. Trace unit tests to Source Code and to Design Specifications
 1. Verify an appropriate relationship between the Source Code and Design Specifications being challenged
7. Integration
 1. Trace integration tests to High-Level Design Specifications
 2. IMPORTANT: Use High-Level Design Specifications to establish a rational approach to integration, to determine regression testing when changes are made
8. Validation
 1. Trace system tests to Software Requirement Specifications
 2. Use a variety of test types
 1. Design test cases to address concerns such as robustness, stress, security, recovery, usability, etc.
 3. Use traceability to assure that the necessary level of coverage is achieved
5. Plan Ahead for Traceability
 1. Options
 1. Manual methods
 1. Word processors
 2. Spreadsheets
 2. "Home-built" Automated Systems
 1. Relational Databases
 3. Commercial Automated Systems
 1. DOORS
 2. Requisite Pro

Appendix F

USOE CHANGE REQUEST FORM FOR COMPUTER SERVICES (CR-1 Aug 2004)

Section 1: Change Request Information To be completed by Requester except shaded areas, see DETAILED INSTRUCTIONS BELOW All requests should be e-mailed by an Associate Superintendent to dwhite@usoe.k12.ut.us			
Originator (Title)		CR Type: <input type="checkbox"/> Change to Existing System or Project <input type="checkbox"/> New System or project <input type="checkbox"/> Other Temporary or One-Time Project	
Director/Coordinator			
System Name			
Or... Project Name		CR No:	
Or... Other		CR Log Date:	
		CR Resolved Date:	
Desired Date			
1A – Description of Change Being Requested: (Describe the requested change. Provide attachments if additional explanation is needed.)			
1B - Proposed Solution: (Provide your opinion regarding the best course of action, based on factors such as cost, schedule, or product quality. Provide attachments if additional explanation is needed.)			
1C - Risk Impact: (Provide your opinion regarding the risk of not doing the change, based on factors such as cost, schedule, or product quality. Provide attachments if additional explanation is needed)			
1D – Quality Assurance/Controls: (Describe how you plan to help provide for quality of the data/information involved in the system/project. What controls will be implemented and who will be responsible to work with Computer Services to ensure			

USOE CHANGE REQUEST FORM FOR COMPUTER SERVICES (CR-1 Aug 2004)

such quality and controls. Provide attachments if additional explanation is needed.)

Section 2: Priority Assessment (Use Service Level Agreements in Change Management Process Document)

Service Level Agreement Applications Project Other

Used:

Assigned Service Level: (1) (2) (3) (4) (5) New Project Required

2A – Justification for Priority

Section 3: Impact Analysis (To be completed by Computer Services or Project Management)

3A - List Artifacts Affected

5B- Overall Impact:

Business Assessment: (Briefly describe the anticipated benefits, and document any changes to the workflow/operational procedures which might result from this change.)

Completed by:

Date:

Technical Assessment: (Briefly describe how existing services or deliverables will be affected as a result of the requested change. Describe acceptance criteria for changed deliverables. Attach documentation such as the functional

USOE CHANGE REQUEST FORM FOR COMPUTER SERVICES (CR-1 Aug 2004)

specification to illustrate, as needed.)		
<i>Completed by:</i>		
<i>Date:</i>		
Cost Assessment: (Briefly describe changes to the Resource Plan that would result from this change.)		
Time Assessment: (Briefly describe changes to the Project Schedule that would result from this change. Attach copies of existing and new schedules showing new tasks, subtasks, and milestones.)		
<i>Completed by:</i>		
<i>Date:</i>		
3C- Potential Risks:		
3D – Management Approval:	Phone:	Date:

Section 4: Disposition of CCB (To be completed by Computer Services or Project Management)

Disposition Assigned: Pre-Approved Approve Deny Defer More Info

Assigned Service Level: 1 (Pre-Approved) 2 3 4 5 New Project Required

Changes which are not approved within ten (10) work days will be considered to be rejected.

4A – Recommendations and Communication Plan/:

4B – Action Items

Action Item	Due Date	Responsible	Status

4C - CCB Approval: (Project Management Office)

CCB Date:

Section 5 - Closure

Completed

Date Completed

- Communication to impacted parties
- Artifacts updated
- Project Plan updated

Instructions

- Originator fills in Section 1 (*excluding the CR number assignment, Logged Date and Resolved Date*)
 - *Specify if CR is for an existing system (including IT infrastructure) OR existing project OR other*
 - *If CR is for an existing system or project, specify the parts of the system/application needing change. Provide details in section 1. See examples below.*
 - *If CR is for a project, specify the deliverable where the change would occur.*
- PMO assigns the next available Change Request Number
- Project Management completes Section 2
- CCB completes Section 3
- Project Management completes Section 4

Section 1 (General information)

- Provide unique description
- Enter Priority Rating
- Enter date needed by

Examples: Forms, Reports, Data Field, Labels, Color, Business Rules, Error messages, Desired services, Desktop environment, etc.

Section 1A (Requester's Description of Change)

- Explain why the change is required
- Provide a narrative of any problem

Provide business or technical justification. Provide a step by step description of any problem so that it can be reproduced by the computer services staff.

Section 1B (Proposed Solution)

- Provide a brief description of proposed solution

Section 1C (Risk Impact)

- Provide a brief description of risk if change is not made

Describe the consequence of not implementing the CR. Describe consequences of implementing the CR

Section 2A (Impact Analysis)

- List Artifacts affected and their owners

Identify who performed the assessment in each sub-section.

List all artifacts requiring work if the change is implemented. Use *Impact Analysis For*. Place summary of impact in this section. List all new, modified or deleted artifacts

Section 2B (Overall Impact)

- Explain how each artifact or function is affected
- List all processes and functions affected

Describe the following criteria:

- **Work:** Expected number of hours to complete the change
- **Resources:** The types of resources needed and their availability. Describe conflicts with other work assignments
- **Schedule:** Estimate the amount of time in calendar weeks to implement the change. For projects, calendar days should be used.
-

Section 2C (Potential Risk)

- Identify potential risk(s)
- Obtain Project Manager's approval

Section 2D (Track Lead Approval)

-
- Director of Computer Services must approve all CR's in order to be submitted to CCB for disposition

Section 3 (Priority Assessment)

- Service Level Agreement Used
- Priority Assigned
- Justification for Priority

Section 3 (Disposition of CCB)

- Status
- Recommendation
- Action Items
- CCB Approval

Section 4 (Closure)

- Notify affected entities
- Artifacts updated
- Project Plan updated

DRAFT

ACS Custom Software Applications Requests

Definitions

- The application **owner** is the business or organizational unit responsible for the data and business processes the application is designed to facilitate through automation. Examples include the Educator Licensing, Internal Accounting and School Finance sections.
- **Request books** (Excel workbooks), one for each development team, are stored in the following directories: //begroups/acs\$/requests/team_name.xls where **team_name** can be: cactus-iris, financial, or warehouse. Individual, detail **request documents** are stored in the same directories and follow the naming convention: **team_name** + **developer**_initials + date + alpha_character. The date should be in the format of yymmdd. The alpha character should be "a", "b" etc. and only used to distinguish two or more request documents created by the same **developer** on the same day.
- The application **liaison** is the person who provides the primary means of communication between the **owner** of the application and the application development team, specifically the team **leader**. As problems or issues with the application arise the liaison does the initial screening to determine which problems or issues need to be defined as **requests** for the development team. Such raw requests should initially flow from the **liaison** to the team **leader**.

Later in the request process additional individuals from both the **owner** community (also called **customers**) and the development team may need to become involved. Regularly scheduled project or application meetings in which both **customers** and **developers** are present may also serve as a place for the initial definition of a request.

- The development team **leader** is the person responsible for defining the request in the request book after communications with the application **liaison**. The **leader** also assigns and monitors the progress of the request. More details follow in the **Status and Procedures** section.
- The application **developer** (programmer or database analyst classification) is ultimately responsible for the completion of the request. Often the team leader will also assume the role of the application **developer**. See status descriptions below for more details on how the developed and team leader move the request through the various steps to completion.
- **IT management** is the individual(s) responsible for the general delivery of information technology to the Utah State Office of Education, and specifically in the the form of custom software applications.

Status and Procedures

Unassigned

The team **leader** makes an initial evaluation of the request received from the application **liaison**. If more clarification is necessary the **leader** will communicate with the **liaison** or other **customers** to gain more understanding of the request and establish a **priority**. The three **priority** levels are: **1** (high), **2** (normal), and **3** (low). Throughout the course of the request only the **leader** should modify the request's **priority**.

At this point the team **leader** creates a row for the request in the appropriate **request book**. All columns must be completed except the **assigned-to** column, unless the status is going to immediately be changed to **assigned**. The request **description** should be kept reasonably brief. The **request document** linked to from the **request document** column should contain the detailed problem, design, and testing information.

Assigned

When the team **leader** decides which application **developer** is to be assigned to the request, the **assigned-to** column is filled-in and the status is changed to **assigned**. When this change of status occurs a message will be emailed to the **liaison**, the **developer**, and any designated **management**. All messages triggered by status changes will include: the **description** of the request, the **liaison**, the **request date**, the **due date** (if specified) and the **developer** to whom the request was assigned.

In-progress

The **developer** to whom the request is assigned changes its status to **in-progress** when he actually begins work on the request. This is done only after he has completed the **request document** and have inserted a link pointing to that document. The naming convention for the **request document** is described in the **request books** paragraph at the top of this page. Changing the status to **in-progress** will trigger a message to the **leader** and the **liaison**.

If, for whatever reason, progress towards the completion of the request is stopped (usually for a week or more) the status of the request may be moved back to just **assigned** or even **unassigned**. Only the **team leader** should make such a change.

Completed

After the new or changed features of the request have been fully tested by the **developer** he will change the status of the request to **completed**. When this

change of status occurs a message will be sent to the **liaison** originating the request and the **leader**. This should only be done after the **developer** has reviewed their work against the **request document**. In some cases a code walk-through with another **developer(s)** may be desirable.

Production

After the **leader** agrees the request has been satisfactorily completed he will move the request to **production** status; but only after the necessary components that were added or modified have been physically moved to the **production code directory** and any **production database** changes have been made.

Sometimes the **leader** may instruct the **liaison** or their designees to do some "beta" testing with test data before this is done. If, for whatever reason, the **leader** thinks more work needs to be done he may move the request back into **active** status after discussing the problem with the **developer**.

The exact process of moving the new code into **production** will vary depending on the architecture. Here us an example in which Powerbuilder is the architecture and BASE is the application.

- All source code libraries (.PBLs) are moved from //begroups/acs\$/pb/base to //beusoe2/acsapplibs\$/base/source.
- The source code in //beusoe2/acsapplibs\$/base/source is compiled into .PBDs and .EXEs in //beusoe2/acsapplibs\$/base/object.
- These new PBDs and .EXEs are copied into the appropriate directories on servers for: launching by users, synchronization by standalone installations or packaging into Installshield zip files. In the case of CACTUS these directories would respectively be: //beusoe1/winapps/cactus, //beweb/pub/acs/cactus/sync and //begroups/acs\$/install/55/cactus/pbds.

Appendix H

USOE Network Standards and Connection Policy (Definitions of *bold & italicized* terms are listed at the bottom.)

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

1. Owned by the USOE.

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

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

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

2. Employee owned and approved for *telecommuting*.

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

A USOE 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 the *USOE domain* through the *USOE wireless network segment* in conjunction with *VPN*.

Only USOE owned computers and employee owned computers approved for *telecommuting* may be connected to the *USOE wireless network segment* and to the *USOE 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 USOE network administration has discussed the violation with the violator's supervisor. **Violators may be subject to disciplinary action.** Prohibited devices include all peripherals (e.g. printers and scanners). See note about PDAs below.

3. Privately owned and brought into the USOE by a business visitor.

A business visitor may access the Internet, but not the *USOE domain*. To access the Internet they must receive permission along with current codes from a USOE sponsor/host in order to connect to the *USOE 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**.

Note about PDAs (personal digital assistants). No PDA or other handheld device may, by itself, be directly connected to the USOE network, wirelessly or with cable. When properly configured such devices may be used to synchronize with the host computer or download network files including those in Outlook, This is only permissible through a USOE owned or **telecommuting** computer by means of an attached cradle or Bluetooth wireless technology. **Violators of this policy may be subject to disciplinary action.**

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

Definitions

Acceptable Use Policy. All employees and business visitors, regardless of how they are connected to the USOE network are required to follow the USOE acceptable use policy. See: <http://www.usoe.k12.ut.us/hrm/acceptuse.htm> & <http://www.governor.utah.gov/lan/aup.htm>.

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 agency 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 the USOE network: peer-to-peer networking, file-sharing, instant messaging, or network broadcasts of any kind. McAfee virus protection software is available for home use by any USOE employee. Please see a network administrator for a copy.

Telecommuting. USOE 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 the USOE network. If the telecommuter desires to connect to the **USOE 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. See <http://www.usoe.k12.ut.us/hrm/rules2002.pdf> for more information about telecommuting.

USOE domain. The USOE domain is the secure network of shared computers at the USOE. It is a subset of the more generally defined **USOE 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 the USOE domain from within the building by supplying a logon name and password they also receive Internet access. Business visitors are permitted to connect to the USOE wiring infrastructure and obtain Internet access without connecting to the USOE domain. Such use is permitted only through the **USOE wireless network segment**.

USOE hardware and software standards. In order to maximize usability, reliability, security, and efficiency of USOE information technology resources; the USOE has defined hardware and software standards. A summary of the current hardware/software standards include: a Dell or MPC desktop or notebook running Windows XP with Service Pack 1 installed, and the Microsoft Office 2000 suite of productivity applications including the Outlook e-mail/groupware client. As part of the USOE standard setup features, these machines are all configured as **secured computers**. Other hardware and software standards exist in the USOE, 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 the USOE network, and if an agency license agreement (in the case of software) already exists.

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

USOE wireless network Segment. A secure wireless network segment is available for USOE staff and sponsored business visitors. This network provides access to the Internet and optionally to the USOE domain via VPN. In order to connect to the USOE for Internet and/or USOE domain access, the USOE 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 the USOE wireless network segment. For security reasons these codes will change periodically. When this happens they will be distributed to all USOE employees who have a VPN account. Currently the USOE supports the IEEE 801.11b and 801.11g wireless protocols.

VPN (virtual private network). VPN allows those with USOE domain accounts to access the USOE network remotely or through the firewall. You must have a VPN account established by a USOE 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***.

DRAFT

Appendix I

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

The USOE/USOR 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 agency:

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 agency 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.

USOE COMPUTER VIRUS RESPONSE PLAN

USOE Anti-virus Environment

E-mail Servers - All incoming e-mail and attachments are scanned and cleaned, if necessary, by the Barracuda SPAM and anti-virus Firewall before going to the e-mail server. Barracuda 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 the McAfee 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 the McAfee 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. This product checks all files coming into the computer for viruses.

Staffing assignments

Baarracuda Spam Firewall (Jared Southwick/ Dave Hughes)

Coordinator/Mail Server Administrator (Mark Wagstsaff / Jared Southwick)

Client & Server Anti-Virus Software/Data Recovery (Alan Ericksen/ Jared Southwick)

Help Desk/Telecommunication (Carla Worthen / Alan Ericksen)

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 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 McAfee 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 Barracuda Firewall administrator should regularly check the log generated by the Barracuda system to determine if the USOE network is being hit by a heavier than normal number of e-mails or virus contained in messages or attachments. Although the log indicates when viruses have been 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 of 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 been 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 USOE 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 the USOE'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 recover corrupted data from backup servers or tapes. If the damage is widespread, ad hoc priorities should 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.

USOE 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.

A contract with an off-site storage facility, Perpetual Storage Inc., has been executed. Telephone number: (801) 942-1950. (See Attachment A) This facility is a fully finished, multi-mezzanine storage area located in a granite vault. It is a guarded facility to which only Perpetual Storage personnel are allowed. Backups are created, labeled and put in boxes, which are picked up and taken to the storage facility on a regularly scheduled basis. Taped back ups are scheduled to leave the USOE building every Tuesday morning of the year. (USOE staff is responsible to schedule pick up times during holidays.)

The process is as follows: (Figure 1, Tape Backup Schedule)

- A full back up is run the first weekend prior to the first Tuesday of the month.
- On the first Tuesday of each month, the full back up tapes are labeled, placed in the storage container and subsequently picked up by storage company personnel and taken to the storage facility.
- Each week thereafter, on Tuesday, a storage box is returned to the USOE to accommodate the differential and incremental tapes. On Monday through Thursday the backups start at 5:00 p.m. and complete by 1:00 or 2:00 a.m. The incremental backup is done in the early hours of Saturday morning (12:00 a.m.) This process repeats for the remaining weeks of the month and at the end of the month the full backup process starts again.
- The process is repeated each month.

TAPE BACKUP SCHEDULE

Figure 1

Septembe 2002						
S	M	T	W	T	F	S
					Full Back Up	
	Differential	Differential	Differential	Differential		Incremental
	Differential	Differential	Differential	Differential		Incremental
	Differential	Differential	Differential	Differential		Incremental

Note: Using the above example, there would be FIVE labels for the month as follows:

A1 MONTH_YEAR FULL
 B2 MONTH_YEAR DIFF & INCR
 B3 MONTH_YEAR & INCR
 B4 MONTH_YEAR & INCR
 A1 MONTH_YEAR FULL

The letter signifies the set, so there are four different sets listed. The number identifies the slot where the tape was located in the tape backup device. If more than one tape is used for a backup, they would be labeled as follows: **A1 MONTH_YEAR FULL, A2 MONTH_YEAR FULL, A3 MONTH_YEAR FULL**; or

Currently, a Dell Server configured with Windows 2000 Advanced Server with Veritas Backup Exec, Version 8.6 build 3878 is being used for the backup process. It is connected via SCSI to an ADIC FastStor, Model DA-DLT-7000, and Part #62-0124-01. DLT media is used in the tape drive.

The above configuration would be required to replace the system if necessary.

The Veritas support telephone number is 1-800-634-4747 or 1-407-531-7200. The USOE Contract ID is 7315-3051-1624, VIP Agreement #0000003418 and VIP customer #48187. The activation code for Backup Exec Remote Agent NT/2000 is 08-7373-9994-000900. The activation code for Backup Exec Remote Agent NT/2000 is 01-4717-9997-003969, which activates 23 remote agents. The Backup Exec IDR Server and remote activation codes are 04-4898-9994-000535, 04-7230-9998-002231.

An electronic log of the tapes in the individual boxes is kept off site at the perpetual storage company. The electronic log can be found at [\\begroups\acs\\$backup logs.xls](\\begroups\acs$backup logs.xls). A printed copy of the log is placed in the box with the tapes. Tapes are identified by box # and month.

Example:

BOX #	1425
--------------	------

Month	Month-03
--------------	----------

ACS Tapes	
	A1 Month 2003 Full
	A2 Month 2003 Full
	A3 Month 2003 Full
	A4 Month 2003 Full

Jobs are labeled with the server name and the type of backup such as: BEAIMS DIFF, BEAIMS FULL, and BEAIMS DIFF & INCR. These jobs are located in the Backup Exec software; and are custom jobs that the software user could set up.

BEAIMS DIFF

- C\$ is backed up in its entirety
- D\$ is backed up in its entirety
- System State is backed up in its entirety

BEASEPRD DIFF

- C\$ is backed up in its entirety
- E\$ is backed up in its entirety
- F\$ is backed up in its entirety
- System State is backed up in its entirety

BECERT DIFF

- C\$ is backed up in its entirety
- E\$ is backed up in its entirety
- F\$ is backed up in its entirety
- G\$ is backed up in its entirety

BECOGNOS DIFF

- C\$ is backed up in its entirety
- D\$ is backed up in its entirety
- System State is backed up in its entirety

BEDC13 DIFF

- C\$ is backed up in its entirety
- System State is backed up in its entirety

BEDC14 DIFF

- C\$ is backed up in its entirety
- System State is backed up in its entirety

BEDNS2 DIFF

- C\$ is backed up in its entirety
- System State is backed up in its entirety

BEDRIRIS2 DIFF

- C\$ is backed up in its entirety, with exception no backup done on Timbuk2
- E\$ is backed up in its entirety
- F\$ is backed up in its entirety
- System State is backed up in its entirety

BEEASERV DIFF

- C\$ is backed up in its entirety

D\$ is backed up in its entirety
System State is backed up in its entirety

BEEBRIGHT DIFF

C\$ is backed up in its entirety
D\$ is backed up in its entirety
E\$ is backed up in its entirety.
System State is backed up in its entirety

BEGROUPS DIFF

C\$ is backed up in its entirety
D\$ is backed up in its entirety
System State is backed up in its entirety

BEIMC DIFF

C\$ is backed up in its entirety
System State is backed up in its entirety

BENTBKUP2 DIFF

C\$ is backed up in its entirety
D\$ is backed up in its entirety, with exception no backup done on images, and images\$.
System State is backed up in its entirety

BEPS1 DIFF

C\$ is backed up in its entirety
D\$ is backed up in its entirety
System State is backed up in its entirety

BEPS2 DIFF

C\$ is backed up in its entirety
D\$ is backed up in its entirety
System State is backed up in its entirety

BESYBASE1 DIFF

C\$ is backed up in its entirety
E\$ is backed up in its entirety
F\$ is backed up in its entirety

BETERM DIFF

C\$ is backed up in its entirety
D\$ is backed up in its entirety
System State is backed up in its entirety

BEUSOE1 DIFF

C\$ is backed up in its entirety
D\$ is backed up in its entirety
System State is backed up in its entirety

BEWEB DIFF

C\$ is backed up in its entirety
D\$ is backed up in its entirety
System State is backed up in its entirety

ALOGAN DIFF

C\$ is backed up in its entirety
D\$ is backed up in its entirety
System State is backed up in its entirety

THEBER DIFF

C\$ is backed up in its entirety
D\$ is backed up in its entirety
System State is backed up in its entirety

RECOVERY OF LOST DATA AND HARDWARE (Needs Updating)

1. RECOVERY OF LOST DATA AND SOFTWARE

1.1 Lost data and software will usually be recovered by a network administrator from backup tapes.

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 weekend preceding the first Tuesday. The full system backup just completed plus the incremental backup tape set from the month just ended is picked up by Perpetual Storage for offsite storage on this Tuesday. 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 tape set is kept at the offsite storage location for one year. When the month corresponding to the one on the tape set is passed in the next calendar year that set is returned to the USOE and recycled one time as full-system or incremental tapes. When they make their way back to the USOE the second time from offsite storage they are discarded. The exceptions to this are the July tape sets. They are kept offsite indefinitely (at least 5 years). If tape backup systems change, care must be taken to insure that tapes backed up before the system change can still be retrieved. Two incremental tape 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 the drive 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.

If it is necessary to recover any files from tapes in off-site storage Perpetual Storage will deliver any needed tape sets within 90 minutes for approximately \$24.00. You will usually get a given month's full-backup and the preceding month's incremental backups in the same safe box. You must specify which month's or months' boxes you need based on the restoration needs of the user. In some cases both full and incremental sets will be needed. Once a box of tape sets is returned to the USOE it will be kept on-site in the safe until the first Tuesday of the following month, at which time it will be returned to Perpetual Storage unless its one year in off-site storage has passed.

- 1.2 Using the Conner 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 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 by Perpetual Storage would be used. Offsite tapes are retrievable within 1.5 hours. 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. Backups of specialized servers such as teacher certification's imaging system also need to be reviewed. It is believed that at this time their optical diskettes are also being kept off-site at an employee's home.
- 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 agency 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 (PBX, 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. Currently US West is running at least 60 days behind on installations. US West could take at least 30 days to install any new circuits unless we could get them to escalate our order. 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 agency.

- 2.1.1 Rewiring of the LAN room in order to accommodate pre-disaster hardware would require about 8 hours of work. This assumes assistance from an ITS wiring crew 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. The following list addresses each type of device and attempts to estimate the average amount of time to reinstall and configure such a device. These times are then multiplied by the number of devices to come up with a total amount of time needed to reinstall and configure all such devices.

Note that reinstallation cannot begin until at least some of the replacement devices have been ordered and delivered. Usually machines can be ordered and delivered within seven working days. To complete a large order could take considerably longer. Total recovery cannot be completed until all replacement hardware has been delivered. It has been recommended that Risk Management be approached with the suggestion that they keep some spare servers on hand for use by any state agency needing replacements thus expediting this process. Note that time needed includes hardware configuration as well as installation of any system software not available from tape backup restores.

<u>TYPE OF DEVICE</u>	<u>TIME NEEDED</u>	<u>UNITS</u>	<u>TOTAL TIME</u>
Novell servers (subsystems such as disk arrays factored into estimate)	5 hours	9	45 hours
Unix servers	8 hours	1	8 hours
Tape backup system (Includes server & Carousel)	9 hours	1	9 hours
Concentrators	5 mins	40	4 hours
Ether-switch	2 hours	1	2 hours
Routers	2 hours	2	4 hours
Imaging System	2 days (informational, responsibility of Comgraphix)		
Miscellaneous	10 hours		<u>10 hours</u>
		TOTAL	82 hours

- 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. This amounts to a total of 43 (340 / 8) man work days given approximately 340 desktop machines and printers. Any standalone software/data recovery (from backup diskettes or tape) which needs to be done for desktop machines will be the responsibility of the user of that 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 There are two staff members available for recovery of LAN room hardware. It is possible that two USOR (Dewey Dipoma, Abdul Matin) and one DCS (Mike Wilde) LAN administration specialists may also be able to assist in LAN room recovery as well as with recovery of desktop machines. This would depend on obligations to their respective sections. Having up to three additional persons would speed up this process as would acquiring help from outside computer consultants. However we will see in the desktop discussion below that assignments of staff needs to be balanced between LAN room and desktop tasks.

2.1.4.2 Regardless of the number of qualified staff available the estimated 82 hours need 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 is 115 hours.

Dividing this by two LAN specialists yields approximately 60 hours or 6 and ½ work days. Adding this to the 12 hours estimated for recovery of software and data from tape gives approximately 8 or more elapsed work days. We cannot divide data and software recovery time by 2 persons, since we have only one backup/restore system. 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 “power users”) and some of the DCS or USOR LAN specialists, could install and recover the desktop machines throughout the building. This may require some initial training (a few hours) from the LAN administration staff who are recovering the LAN room hardware and the ACS Macintosh specialist. Above we estimated 43 work days for recovery of desktop machines. Multiplying this by our 1.4 factor and dividing by an expected 7 staff members we come up with 8.6 work days. The above applies to only computer hardware and not to other office equipment.

Since this activity can proceed concurrently (with the exception of server connection testing) with the LAN room hardware recovery; and since its elapsed time for completion is approximately the same (8.6 work days verses 8+ workdays) we have both major hardware recovery activities finishing in approximately two work weeks. Of course this timetable could be accelerated through longer hours and/or outside help. Also, unskilled agency staff could be used to help unbox equipment, move it into place and plug them into power strips.

3. COSTS OF HARDWARE RECOVERY

3.1 The following is a table which estimates the cost of replacing all the hardware within the Utah State Office of Education. These costs are based on rounded estimates of the number of units of various hardware as well as current replacement costs. Funding of such replacements will not be discussed at this time. The assumption is that State Insurance/Risk Management would cover most of this loss.

Appendix M – Confidentiality Agreement

Appendix N – Institutional Review Board letter permitting furnishing of data to external research organization

Appendix O – Power User Agreement

Appendix P – Power user training.

Appendix Q – Disaster Recovery Plan

DRAFT

USOE Approved Software

The applications below are standard installations on new and rebuilt machines:

- McAfee
- Windows Media Player
- RealOne Player
- Macromedia Flash Play
- Java
- Adobe Acrobat
- Microsoft Office
- Word Perfect
- Microsoft Anti-Spyware
- USOE Custom Software, i.e., Base, Cactus, etc.

USOE Non-Approved Software

Any installations of the following applications should be removed:

- Web Shots
- Instant Messenger
- Peer to Peer applications, i.e., Kaza, Bearshare, etc.,

Any other software installed on a USOE Computer needs to be approved utilizing the USOE Software Approval Form.

USOE Software Approval Form

Date: _____

Software to be installed:

Machine name software will be installed on:

Person requesting installation:

Department:

Phone Number: _____

Purpose for the use of this software:

Signature of person requesting software:

Signature of Supervisor:

Software license is on file at:

Mark Wagstaff's Approval: _____

Software Installed by:

Date of Installation:

(July 28, 2005)

DRAFT