

UTAH SCHOOLS FOR THE DEAF AND THE BLIND COMPUTER SECURITY POLICIES

(Keep for employee reference)

PREFACE

As the computer system at USDB grows and becomes more complex, and as the amount and variety of stored data increases, it becomes more important that policies be established and that all users be made aware of them. The policies are formed, not to place users under unreasonable constraints, but to reduce liability to the state as well as minimize potential damage to stored data and data systems.

1 USER RESPONSIBILITIES

Each person using computing resources owned by the state of Utah, has a personal responsibility to protect both the state and our own agency from liability from the potential misuse of computer hardware, software, or stored data. Also, because personal data must be maintained to ensure the mission of our agency, each user must take every effort to protect the system from intrusion or other malicious actions.

2 SOFTWARE

- 2.1 Software Licensing and Software Copying: A software license is purchased to run software applications either on an individual computer or on the network server. Copies can only be made for backup purposes to protect licensees against storage or utilization hazards. Every effort is made to stay in compliance with software license agreements by having sufficient licenses for every user or by restricting access to a limited number of licenses. Copies of software licensed by our agency should never be copied from our PC's or PC network for utilization elsewhere. As backup copies are made on a daily system level, users should never have a need to make personal copies.
- 2.2 Personal Software Licenses: In the event that users have purchased software licenses for personal use on home computers, users are not authorized to install copies of that software on agency owned computers.
- 2.3 Public Domain Software and Shareware: As a rule, public domain software should not be installed on agency machines without first obtaining permission from the systems administrator. Shareware is distributed by individuals sharing copies with each other. Shareware must be properly licensed to use it for purposes other than evaluation.
- 2.4 Software obtained via the web: If the software is freeware, permission should be obtained from a system administrator before installing on your PC. Screen savers and other utilities downloaded from the web and installed on user machines have frequently "crashed" the system and expense and lost productivity is experienced by our agency and the state of Utah for the cost of restoration. If the software is not freeware, permission from a system administrator should be obtained before installing and proper licensing should occur before continued use. If the proper license is not obtained, the software should be uninstalled from the user machine.

3 WORK STATION SECURITY

- 3.1 System Passwords: Security to system computing resources is controlled, in part, by assigning users personal passwords. **Passwords should be kept confidential! Do not allow other individuals to use your workstation and to use system resources by giving them your password.** Any individual who requires access to system resources, can be authorized to use them by their supervisor, and can obtain their own password by application. It is not appropriate for a supervisor to require a subordinate to share their password. Because passwords are so vital to system security, users are required to change passwords at a maximum of 180 day intervals.

- 3.2 Unattended Work Stations: Work stations should not be left unattended without taking measures to prevent intrusion or unauthorized access. One of the following methods should be utilized to ensure system security when leaving a work station unattended for even short periods of time.
 - 3.2.1 Log off the system: When you log off of the system, other persons can not obtain access to the system without knowledge of a valid password associated with a valid user. You haven't shared your password, have you?
 - 3.2.2 Place a software lock on your station: Screen savers that ship with Windows can be password protected.
 - 3.2.3 With the Dell GX machines there is a key to the right of the f12 key with a moon shape on it. Press this key and it will put your machine asleep and lock it down until you return.

4 CONFIDENTIALITY AND PERSONAL USE

- 4.1 **Personal Use of Agency Computing Resources:** As a general rule, agency computers should not be used for personal use. Agency computers are purchased and provided to users to ensure their success in performing their agency related duties. Personal data should not be saved on system storage devices.
- 4.2 **Non-confidentiality:** Although an effort is made to ensure confidentiality on system storage devices and software systems and email systems, **confidentiality can not be guaranteed!** Transmissions over wiring and cabling systems, as well as long distance transmissions on public systems, are at potential risk. The possibility of disgruntled employees, with high system security, accessing and revealing sensitive information exists. Intrusion into the system from unattended work stations is a very high risk. Sensitive information can be saved on floppy disks where it can be locked up or transported via a controlled method.

5 VIRUS PROTECTION

- 5.1 Software viruses are becoming more common and account for millions of dollars in losses annually in lost productivity or lost data. Viruses have also caused great losses in computer systems owned by agencies of the state of Utah. Each user has the responsibility to do his/her part in reducing the likelihood of introducing a virus into agency owned computing systems.
- 5.2 The following are some suggestions to assist users in reducing the possibility of introducing a virus into agency systems:
 - 5.2.1 Public domain software that has been down loaded from an electronic bulletin board system should never be installed on a system without first being scanned for viruses.
 - 5.2.2 Diskettes used on non-system machines should be virus checked before being used on a system machine.
 - 5.2.3 E-Mail is a common medium by which viruses are propagated. Always be cautious whenever you receive email messages that contain attachments. If you are not expecting an attachment or if there is not something in the body of the message that would uniquely identify a known reason for receiving the attachment, delete the email without opening the attachment.
 - 5.2.4 All computer systems used by our agency have virus scanners installed. Never let virus patterns age beyond 2 weeks. If you need help updating your virus patterns on your computer, or if you suspect that the virus scanner on your machine is not functioning properly, please contact a member of the IT team for assistance.

6 SECURITY AUDITS

- 6.1 Periodic, unannounced, random audits will be conducted to safeguard state liability with regard to licensing of software. If, after a warning of software license violation, a user persists in installing unauthorized software on agency machines, a formal reprimand will be placed in a user's personnel file.

Request For Computing Resources

LOCATION (Campus or Non-Campus)	APPLICATIONS (E-Mail, Word Processing, Spreadsheet, Registry, etc)
1. _____	_____
2. _____	_____
3. _____	_____
4. _____	_____
5. _____	_____
6. _____	_____
7. _____	_____
8. _____	_____

Date of Request: _____ Date Resources Required: _____

Employee Status: **Full Time** **Temporary** If Temporary: Estimated Termination Date: _____
Circle the one that applies

First Name/MI: _____ Last Name: _____

Title: _____ Department: _____

Primary Work Address (Street,City): _____

Telephone: _____ Fax: _____ Supervisor: _____

I have read and agree to comply with the policies contained in the 'USDB Computer Security Policies' document.

Signed _____ Date _____
Employee

Supervisory Permissions: (All information in this section must be completed for this application to be processed)

This employee replaces a terminated employee. **Yes** **No** (Circle appropriate answer)

If yes, terminated employee's name _____

I have reviewed the policies regarding computer resource utilization with this employee and give my permission to allow security to the resources listed above.

Signed _____ Date _____
Supervisor

Date security set up on system _____ Initials _____

Date E-mail set up on system _____ Initials _____

Utah Schools for the Deaf and the Blind Internet Acceptable Use Agreement

(Keep for employee reference)

PURPOSE

The purpose of UtahLink, the educational network supported by the Utah Education Network (UEN), is to advance and promote a world-class public education in Utah. UtahLink is intended to assist in the collaboration and exchange of information between and among schools, school offices, the Utah Education Network, and other State and educational entities as well as to provide access to the "world of information" via networking facilities like the Internet.

GOAL

Internet access is now available to teachers and staff who work for USDB through collaboration with UtahLink and the Utah Education Network. We are pleased to bring this access to USDB and believe the Internet offers vast, diverse, and unique resources to both students and teachers. Our goal in providing this service to teachers, students, and staff is to promote educational excellence at USDB by facilitating resource sharing, innovation, and communication. The Internet is an electronic highway connecting thousands of computers and millions of individual subscribers all over the world. Students, teachers, and staff will have access to such resources as:

1. Electronic mail communication with each other as well as with people all over the world.
2. Information and news from NASA as well as the opportunity to correspond with the scientists at NASA and other research institutions.
3. Public domain software and shareware of all types.
4. Discussion groups on a wide variety of topics.
5. Access to many library catalogs including university libraries, the Library of Congress, and soon, the USDB Educational Resource Center catalog.
6. Access to a wide variety of educational databases.

GUIDELINES

With access to computers and people all over the world also comes the availability of material that may not be considered to be of educational value in context of the school setting. UtahLink has taken precautions to restrict access to controversial materials. However, on a global network it is impossible to control all materials and an industrious user may discover controversial information. USDB firmly believes that the valuable information and interaction available on this worldwide network far outweighs the possibility that users may access material that is not consistent with USDB educational goals. Internet access is coordinated through a complex association of government agencies and regional and state networks. In addition, the smooth operation of the network relies upon the proper conduct of the end users who must adhere to strict guidelines. These guidelines are provided here so that you, as an end user, are aware of the responsibilities you are about to acquire. It is imperative that UtahLink members conduct themselves in a responsible, decent, ethical, and polite manner while using the network. In general this requires efficient, ethical and legal utilization of the network resources. If a USDB user violates any of these provisions, his or her account will be terminated and future access could possibly be denied. The signature(s) at the end of this document is (are) legally binding and indicates the party (parties) who signed has (have) read the terms and conditions carefully and understand(s) their significance.

INTERNET TERMS AND CONDITIONS]

1. **ACCEPTABLE USE:** The purpose of UFSNET, which is the national backbone network to the Internet, is to support research and education in and among academic institutions in the U.S. By providing access to unique resources and the opportunity for collaborative work. The use of your account must be in support of world class public education and research and consistent with the educational objectives of USDB. Use of another organization's network or computing resources must comply with the rules appropriate for that network. Transmission of any material in violation of any US or state regulation is prohibited. This includes, but is not limited to, copyrighted material, threatening or obscene material, or material protected by trade secret. The following uses are also prohibited: any use for commercial purposes or financial gain; any use for product advertisement or political lobbying; or any use which shall serve to disrupt use of the network by other users.
2. **PRIVILEGES:** The use of the Internet is a privilege, not a right, and inappropriate use will result in cancellation of those privileges and/or disciplinary action. USDB has formed a Technology Committee which includes the Educational Technology Specialist, the Local Area Network Administration Specialist, the ERC Director, and

the Superintendent. The Technology Committee will deem what is inappropriate use based on the rules and policies of the Utah State Board of Education and their decision is final. Continued misuse may result in disciplinary action appropriate with USDB and state personnel policies. The administration, faculty, and staff of USDB may request the Technology Committee to investigate complaints of misuse. Network accounts should be used only by the authorized owner of the account. Account owners are ultimately responsible for all activity under their account. At present, secondary students enrolled at USDB may acquire dial-in accounts through their local district server. Each student who receives an account will be part of a discussion with a USDB faculty member pertaining to the proper use of the network.

3. NETWORK ETIQUETTE: You are expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to the following:
 - A. Be polite. Do not be abusive in your messages to others.
 - B. Use appropriate language. Do not swear, use vulgarities or any other inappropriate language.
 - C. Illegal activities are strictly forbidden. Illegal activities shall be defined as a violation of local, state, and/or federal laws.
 - D. All communications and information accessible via the network should be assumed to be private property. Great care is taken by the network administrators to ensure the right of privacy of users. However, it is recommended that you do not reveal your personal address or phone number or those of students or colleagues.
 - E. Note that although privacy rights are important, they are not guaranteed. People who administer the system do have access to all email. Messages relating to or in support of illegal activities may be reported to the authorities.
 - F. Do not use the network in such a way that you would disrupt the use of the network by other users. You are cautioned to exercise prudence in the shared use of this resource.
4. WARRANTIES: USDB makes no warranties of any kind, whether expressed or implied, for the service it is providing. USDB will not be responsible for any damages you suffer. This includes loss of data resulting from delays, nondeliveries, misdeliveries, or service interruptions caused by its own negligence or your errors or omissions. Use of any information obtained via the Internet is at your own risk. USDB specifically denies any responsibility for the accuracy or quality of information obtained through its services.
5. SECURITY: Security on any computer system is a high priority, especially when the system involves many users. If you feel you can identify a security problem on the Internet, you must notify a system administrator or a member of the Technology Committee. Do not demonstrate the problem to other users. Do not use another individual's account. Attempts to log-on to any server for which specific security or authorization has not been granted will result in cancellation of user privileges. Any user identified as a security risk or having a history of problems with other computer systems may be subject to disciplinary action.
6. VANDALISM: Vandalism will result in cancellation of privileges. Vandalism is defined as any malicious attempt to harm or destroy data of another user, the Internet, or any of the above listed agencies or other networks that are connected to the NSFNET Internet backbone. This includes, but is not limited to, the uploading or creation of computer viruses.

INTERNET USE AGREEMENT (submit to IT department)

ACCOUNT OWNER

Name (please print) _____

I understand and will abide by the above Internet Use Agreement. I further understand that any violation of the regulations above is unethical and may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked and school disciplinary action and/or appropriate legal action may be taken.

EMPLOYEE SIGNATURE: _____ **DATE:** _____
