

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.