

Title: Computer and Data Security**I. PURPOSE**

Information used by the University to conduct business is a valuable asset that needs to be protected. Because much of this information is generated and stored on electronic media, precautions should be taken by employees and users of campus electronic data resources to ensure such data is not compromised.

II. POLICY

BYU-Idaho is committed to information security and will comply with applicable laws and best practices for system and data security. Access to information created, transmitted, and stored on University systems is monitored and logged. Employees and users of campus electronic data resources should understand their responsibilities to protect confidential information and thereby improve security.

III. IMPLEMENTATION

Employees and users of campus electronic data resources are to:

A. Protect against improper handling and loss of information by:

1. Leaving confidential information on centralized systems as much as possible and encrypting this data when stored on local and portable devices (such as PC local hard drives, laptops, USB drives, PDA devices, cell phones, etc.)
2. Not sending unencrypted confidential information by e-mail
3. Sending confidential information by fax carefully to the correct recipient
4. Verifying the identity and authorization of those requesting confidential data
5. Securely erasing confidential information from a computer prior to it being discarded, sent to surplus, or used elsewhere

B. Be responsible for their actions and contribute to the security of the network by:

1. Keeping their NetID and passwords confidential by not sharing them with others, not writing them down where they can be seen or easily found, and not storing them in an unencrypted computer file
2. Changing passwords regularly and using passwords that combine upper and lower case letters, numbers, and special characters, and are not dictionary words or common names
3. Immediately changing passwords if they think they may have been exposed
4. Reporting perceived security breaches or suspicious activities through appropriate channels as quickly as possible

C. Protect the computers they use on the campus network by:

1. Having a firewall, automatic anti-virus software and patch updates
2. Password-locking when leaving the work area
3. Shutting down when leaving for an extended period, such as overnight

4. Performing regular backups in order to restore the information should it become corrupted or lost
 5. Considering where e-mail attachments came from before opening them, since they are a potential source of viruses and other malicious software
 6. Considering some web sites contain malicious software and merely visiting them can infect your system or make it susceptible to attack
 7. Running software applications that are legally licensed
- D. Learn and fulfill their responsibilities for the security of information assets by:
1. Becoming aware of the *Information Privacy (1-29)* policy
 2. For those being granted access to confidential information or systems, participating in briefings on information security roles and responsibilities
 3. For those involved in credit card processing, becoming aware of the Payment Card Industry (PCI) *Data Security Standard (DSS)*
 4. For those involved in the management of information systems and confidential data, referring to the *Information Systems Security* policy
- E. Seek Information Technology approval and assistance for:
1. Agreements with third parties to transmit, process, or store University information
 2. Exceptions to firewall and Internet filtering rules
 3. Any need to add, modify or extend information processing infrastructure (applications, services, servers, cabling, network, switches, routers, wireless, etc.)