

BRIGHAM YOUNG
UNIVERSITY

IDAHO

Information Technology

Information Systems Security Policy

1	<i>Introduction</i>	3
2	<i>Terms</i>	3
3	<i>University Information Security Policy</i>	5
4	<i>Risk Management</i>	6
5	<i>Information Security Policy</i>	6
6	<i>Organization of Information Security</i>	6
7	<i>Information Asset Management</i>	7
8	<i>Human Resources Security</i>	7
9	<i>Physical and Environmental Security</i>	8
10	<i>Communications and Operations Management</i>	9
11	<i>Access Control</i>	11
12	<i>Systems Acquisition, Development, and Maintenance</i>	15
13	<i>Information Security Incident Management</i>	17
14	<i>Business Continuity Management</i>	17
15	<i>Compliance</i>	18

1 Introduction

Information used by the University to conduct business is a critical asset that must be available for the University to carry out its mission. This valuable asset must be protected from abuse for the sake of the University, employees, students, and patrons of the University. For example, the loss of private information could cause damage to the reputation of the University as well as expose a student to the threat of identity theft. The University must do everything it reasonably can to insure the confidentiality, integrity, and availability of information.

University administration must balance the security and the availability of information. They must also balance security risks and the cost to mitigate those risks. One way to mitigate risks is to put in place controls or rules by way of policy. This information security policy is one of many ways of putting in place controls that help the University make accurate information available for proper use. It also informs users of their responsibilities to make campus electronic data resources more secure.

2 Terms

For the purposes of this document, the following terms and definitions apply.

Availability- reliable access to information by authorized users for legitimate purposes

Confidential information- information protected by law, policy, or contract that can be disclosed only to those authorized, for example social security, bank account, credit card numbers and student grades

Confidentiality- the disclosure of information for legitimate purposes only to those who are authorized

Data custodian- a person, often a computer programmer, who uses information according to rules set forth by the data steward

Data steward- a delegated representative, often referred to as the data owner, who is responsible for a set of information collected and used by the University

Information security- the preservation of the confidentiality, integrity, and availability of information

Integrity- authenticity and assurance that information is not altered, except as authorized for legitimate reasons

Malicious code- any program or procedure activated with the intention of compromising the security of information systems through unauthorized access or disclosure of information, corrupting information, denying service, or stealing resources, such as a virus, worm, or Trojan horse

Mobile code- software modules obtained from remote systems, transferred across a network, and then downloaded and executed on a local system without explicit installation or execution by the recipient

Owner of information- the person who is the owner of or has responsibility for information assets, such as an individual who creates information, a designated data steward, or an individual who is the owner of their personally private information

Removable media- any device that allows the removal of information (i.e. a laptop, USB drive, CD, DVD, etc.)

Risk- potential negative impact to an asset resulting from vulnerability in the system

Risk management- coordinated activities within an organization that assess risk, communicate risk, and decide how to address risk

Personally identifiable information (PII) - information that can be used to uniquely identify a single person, which could be used to commit identity theft, such as a person's name and social security, drivers license, or credit card number.

Public information- information that may or must be disclosed to the public

Proprietary information- sensitive information not legally protected, but which should be disclosed only to those authorized (i.e. salary information, budget figures, etc.)

Social engineering- any number of tactics (such as pretending to be someone else or proclaiming a false emergency) used by a person to gain access to information, systems, or facilities to which they are not authorized

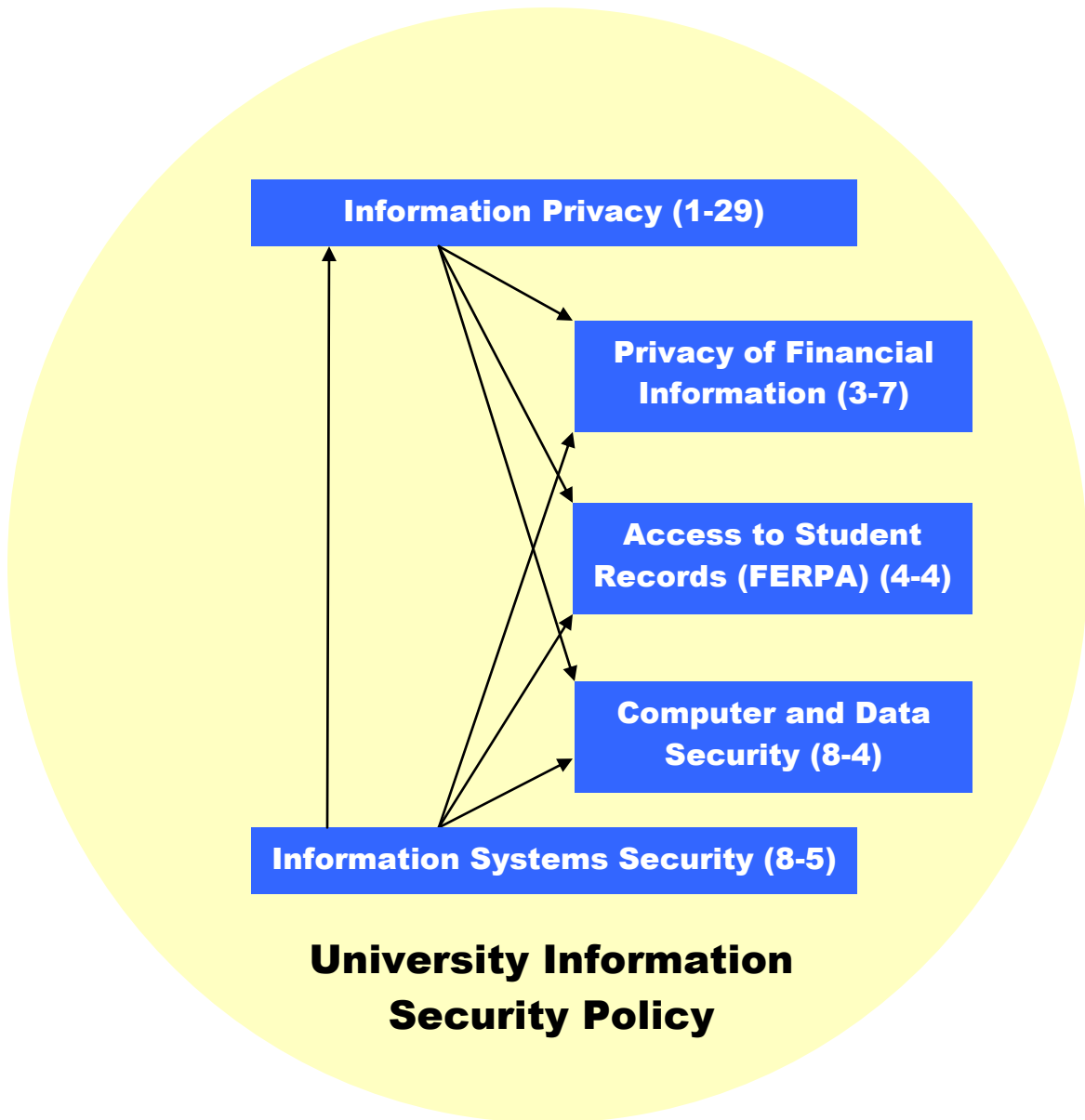
System administrator- a person who is assigned ownership and responsibility for the management of a system or equipment

User- an employee, student, contractor, or guest that uses University electronic information resources (for example, the user of a personal computer on the network)

Username- a computer or system account that allows a user to logon to a computer system; often referred to as a user or network identification (user ID or NetID)

3 University Information Security Policy

The University’s information security policy encompasses several individual policies including this policy as illustrated below. These policies refer to one another and are the authoritative documents that employees should look to for guidance. This policy is based on ISO standard 17799.



4 Risk Management

A risk assessment will be performed yearly or prior to the implementation of a new or extensively changed information system or process. Management will determine to what degree risks will be avoided and mitigated. The process of risk assessment and treatment will be used periodically as a means for continuous improvement.

5 Information Security Policy

Senior and executive management will approve, implement, support, and enforce a suitable information security policy. This policy will be communicated to employees and users of campus electronic data resources to increase security awareness. Information security policy will be updated annually to ensure its continuing effectiveness.

6 Organization of Information Security

6.1 Management of Information Security within the University

Cross-functional input for information security activities will come from the Information Technology department, the Privacy Committee, and the Information Security Committee, which provide diverse representation from across the campus. The Information Security Officer will be responsible for the overall orchestration of information systems security as aligned with the mission of the University. Each department must assess its own unique security needs and inform its users of their responsibilities toward information security. Ultimately each individual person is responsible for the security of the assets under their control.

The addition of new information processing facilities, hardware, or software and also the use of privately owned equipment must be approved by Information Technology in order to ensure consistency, compatibility, and security. An independent review is to be performed on the organization's overall information security processes to ensure they are adequate, complete, fit-for-purpose, and enforced. This will be done as deemed necessary by administration or when significant changes occur.

6.2 External Parties

Arrangements with external parties to outsource information processing and agreements to send them information must be approved by Information Technology. Risks to the organization involved with such activities will be identified and appropriate controls implemented before granting access. An independent review is to be performed on the organization's overall information security processes to ensure they are adequate, complete, fit-for-purpose, and enforced. This will be done as deemed necessary by administration or when significant changes occur. Data stewards must approve of any information given to third parties (see the *Data Stewardship* (8-1) policy), taking care not to violate any provision of FERPA. An agreement with the third party specifying all relevant security requirements may be required and all identified security requirements will be addressed before giving external parties access to the University's information assets.

External parties with whom there is no formal contract to do work on campus must be escorted when entering information processing facilities and may be given confidential information only after a nondisclosure agreement has been signed by both parties.

7 Information Asset Management

7.1 Responsibility for Information Assets

Information assets including data, software, hardware, and services will be inventoried and assigned an owner. The owners will estimate the value of the assets, assess risks to the assets, mitigate risks commensurate to their importance and/or value, and define the classification and acceptable use of the assets.

7.2 Information Classification

Data stewards will manage and classify data resources and assets according to their value, legal and policy requirements, sensitivity, and criticality to the organization as follows:

- Confidential information (such as grades, health records, credit card numbers, social security numbers, etc.) is protected by law, policies, contracts, or regulations and can be disclosed only to individuals authorized as defined by the data owner (see *Data Stewardship* (8-1) policy).
- Proprietary information, usually for internal use, is guarded due to sensitive, ethical, or privacy considerations (such as salaries, memos, plans, budgets, etc.) and can be disclosed upon the discretion of the creator of the information, which may be a department or individual.
- Public information (such as directory information) is generally available to anyone; however, official announcements to the public must be coordinated through University Relations.

Information, based on its classification, will be made available only to the appropriate and authorized audience. This includes all forms of communication, such as conversations, printed material, e-mail, instant messages, web pages, software applications, and faxes. Such information will be protected as needed by lock, encryption, software controls, firewall, etc. Persons requesting confidential information will be identified and authorized before they receive it.

8 Human Resources Security

8.1 Prior to Employment

The terms and conditions of employment are to include requirements for compliance with information security. Information security roles and responsibilities will be explained to potential employees and contractors before they are hired. Background verification checks will be performed commensurate with business requirements, perceived risks, and the classification of information accessed. Potential employees who will have access to lists or databases of credit card data will have a credit- and criminal-record check.

8.2 During Employment

Employees and contractors will be briefed on their information security roles and responsibilities prior to being granted access to sensitive information or systems and will sign an agreement to protect the confidentiality of information and abide by information security policy. Employees and users of campus electronic data resources will receive appropriate awareness training and regular updates of organizational policies and procedures relevant to their job function. All users of campus electronic data resources must comply with the information security policies of the organization. Non-compliance or any information security incidents resulting from non-compliance may result in disciplinary action up to and including dismissal.

8.3 Termination or Change of Employment

Employees will return all of the organization's assets upon termination or retirement. The rights of all users of campus electronic data resources to access information and information processing facilities will be removed upon termination of their employment or student status. Some services may continue for retirees and alumni, but at restricted levels of access to systems and confidential information. Access rights of employees undergoing a change of assignment will be reviewed and changed as appropriate.

9 Physical and Environmental Security

9.1 Secure Areas

Information processing facilities will be alarmed, monitored, and physically secured against unauthorized access, environmental hazards, and natural disasters commensurate with a risk assessment of the facility. Eating and drinking is not allowed in such facilities. Access to data and telecommunication centers is restricted to identified and authorized personnel. Employees authorized for regular access will be entered in biometric readers, given access codes, etc. Other employees, contractors, and visitors must be authorized, logged, and wear provided identifying badges. Employees are expected to notice unidentified visitors and see to their removal from such facilities. Areas housing systems that store and process confidential information will have video surveillance with the ability to review the last three months of activities.

9.2 Equipment Security

Based upon risk assessment, information processing equipment will be protected from environmental threats and hazards, theft, and unauthorized access. They will be protected from power and air conditioning failures, and fire and water damage. Water-based fire suppression systems will have the power cut off prior to deployment. Power cables, cables carrying data, and supporting infrastructure will be protected from interruption, interception, or damage. Telecommunication rooms, patch panels, and manholes will be locked to prevent unauthorized access. The cable plant will be maintained by the IT Infrastructure department. Users will not run their own cable or in any way alter or add to existing cable. Information processing equipment will be properly maintained to ensure

its continued availability and integrity. Redundancy of equipment, components, services, and routes will be done in accordance with needs identified by risk assessment.

All items of equipment containing storage media will be checked to ensure that any confidential data, system configurations, and licensed software has been removed, reset to factory defaults, or securely overwritten prior to disposal, surplus, or reuse.

University owned equipment, information, or software will not be taken off-site without prior authorization. Employees traveling on business or otherwise taking equipment off campus, such as a laptop, removable disk drive, USB drive, and so on, are responsible for the security of equipment as well as the information contained thereon. Confidential data residing on the equipment must be encrypted.

10 Communications and Operations Management

10.1 Operational Procedures and Responsibilities

Operational procedures will be documented, maintained, and made available to all users who need them. Changes to information processing facilities and systems will be subject to change management control. Projects approved by management will include risk and security assessment as part of the project management life-cycle.

Duties and areas of responsibility will be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of assets when the degree of risk justifies such action. Development, test, and operational facilities will be separated to reduce the risks of system or security failure and unauthorized access or changes to the operational system.

10.2 Third Party Service Delivery Management

Information Technology will regularly review third party services to ensure security controls and service levels are implemented, operated, and maintained by the third party. When third parties provide services in connection with credit card processing they must certify their compliance with the *Payment Card Industry Data Security Standard* (PCI DSS). Accounts used by vendors for remote maintenance will be enabled only during the time needed.

10.3 System Planning and Acceptance

System resources will be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance.

Acceptance criteria for new information systems, new versions, and upgrades will be established. A suitable test of such criteria will be carried out during development and prior to acceptance.

10.4 Protection against Malicious and Mobile Code

System owners and operators will implement detection, prevention, and recovery controls to protect against malicious code and malicious mobile code. Servers and workstations will have anti-virus software that is automatically kept up-to-date and patches that

increase security will be applied. E-mail messages will be scanned for viruses, spam, and malicious code, which will be blocked. E-mail attachments received from unknown senders should be deleted without being opened. Personal computer (PC) users will use anti-virus software that is automatically updated and will use a personal firewall.

10.5 Backup

Personal computer (PC) and laptop users will regularly backup the information they create that is not on a network drive in order to restore the information should it become corrupted or lost. Owners of information and system administrators will ensure backup copies of their information and system software are taken and tested regularly to assure successful restoration and recovery in the event of a disaster or media failure.

Backups of production systems and institutional information will be stored at a remote location that has the appropriate level of physical and environmental protection consistent with the standards applied at the main site. An inventory log of all media will be maintained. The security of the remote location and the media inventory will be reviewed annually. Media no longer needed that contains confidential information will be destroyed.

10.6 Network Security Management

Information Technology (IT) will protect network equipment from threats. Equipment will be secured according to best practices, receive security patches, and will be accessed over encrypted transmission with password protection and audit logs. Only IT is allowed to provision wireless access to the campus network, which will be encrypted and authenticated at least to the level of Wi-Fi Protected Access (WPA). The network architecture, including a network diagram, will be documented and kept up-to-date.

10.7 Media Handling

Removable media will not be used for the storage of confidential information unless it is encrypted or kept locked when not in use. Media with confidential data will be destroyed or securely erased when no longer required.

10.8 Exchange of Information

Information that is sent to or received from an external organization that contains confidential information will be protected using secure transport methods, such as encryption, and privacy will be enhanced through a mutually written agreement. Permission to send information is subject to approval from the data steward.

10.9 Electronic Commerce Services

Any campus entity that processes credit card information will comply with the *Payment Card Industry Data Security Standard* (PCI DSS). This includes software purchased, developed in house, or vendor services that process credit card information. Any such transactions will be encrypted end-to-end, including web transactions.

The integrity of information being made available on public web servers will be protected to prevent unauthorized modification. Information put on web servers will be subject to the *Web Pages* (8-3) policy.

10.10 Monitoring

Audit logs recording user activities, exceptions, faults, security events, and administrator and operator activities will be produced for production systems and kept for at least one year, with a minimum of three months immediately available to assist with possible investigations. Provisions will be made to keep logs for the duration of an active investigation. Audit logs, intrusion prevention logs, event correlation logs, and so on, will be monitored daily to detect unauthorized information processing activities. Logging facilities and log information will be protected against tampering and unauthorized access. The clocks of all production information processing systems will be synchronized with a reliable and accurate central time server. The University respects the privacy of users, however it reserves the right to access all information transmitted and stored on University systems and to monitor all communications and examine data on systems and networks owned by the University.

11 Access Control

11.1 Business Requirements for Access Control

Access to information or information processing facilities will be restricted to authorized persons on a “need to know” or “need to enter” basis and will require department management and IT approval. Access to information by a system or program will be granted upon approval of the department that owns the system or program and the data steward. Access requests will not be allowed without approval of the line management of the requestor. Access rights will be reviewed when an individual’s job or student status changes and will be removed when an individual leaves the University.

11.2 User Access Management

Employees receive a user account when they are employed. Students receive a user account after they have been accepted. Each user will receive a unique user account and a unique password. They will be granted privileges on an as-needed basis. Employees must change and students are recommended to change their password at least once a year. Employees who handle credit card transactions must change their password at least every 90 days. Employees and students should change their password immediately if it has been potentially exposed to others. Employee accounts and access will be removed immediately upon termination of employment. A terminated employee’s home directory and e-mail will be deleted in thirty days, allowing time for their supervisor to retrieve business critical information. Retiree and alumni accounts will remain with only the minimum privileges required.

A guest, contractor, or other person may receive a user account if there is a justifiable business reason and department sponsorship. The department will define how long the account will remain active. Such accounts will expire if the password has not changed within ninety days or there has not been any use within thirty days. Such accounts will be

deleted upon expiration of the department defined period or after expiration of the account. All user accounts will be reviewed at least once a year to find malicious, out-of-date, or unidentified accounts, which will be deleted.

As support personnel fulfill requests, the possibility of social engineering attempts will be considered, and care and caution used to make sure only authorized changes are made. When requests are received in person, over the phone, via email, etc., the identity of the requestor may need to be verified before fulfilling the request. For example, further verification may be needed when a person requests to enter a restricted area, calls on the phone for a password change, sends an email (seemingly from a system administrator) to reboot a system, etc. Examples of verification include calling the requestor's supervisor, presentation of student identification, or talking to an e-mail requestor in person.

11.3 User Responsibilities

Users can be the weakest link in the information security chain and must receive continual training and reminders to increase their awareness. Users need to read and understand the policies listed below. Employees need to sign the *Employee Information Usage Agreement* and complete the *Information Privacy and Compliance Training* on the BYU-Idaho web site.

- *Information Privacy* (1-29)
- *Computer and Data Security* (8-4)
- *Electronic Communications* (2-10)

11.4 Network Access Control

Network connections, including wireless, are provisioned by Information Technology (IT) and will be granted after approval of the requesting department and IT management. Authorized employees and students are allowed network access, which will be granted upon authentication. Guests may be allowed temporary access by a sponsoring department; guests will have accounts and passwords that identify them for accountability purposes and access will be granted upon authentication. Authorized users will be granted access only to services that are required for them to do their job or school work. IT management is authorized to disable network accounts, services, or connections when policy is violated, a security incident is being mitigated, an asset is being protected, or it is deemed in the best interest of the University.

Access to a live network jack will be physically restricted (ie. locked) or logically controlled (ie. network access control) in order to prevent unauthorized use of the network.

Under no circumstances will anyone, except with the approval of IT management, install a server or otherwise provide network services for others on the network. Nor will anyone, except IT, connect separate networks together or extend or multiply network connections through any means including, but not limited to, a router, bridge, gateway, hub, switch, wireless access point, server, personal computer, or modem. A system with a dial-up modem and a provisioned telephone (analog) connection will not be allowed on the network unless there is department and IT management approval and special security

enabled to ensure the system does not become a back door entry point into the network. Such systems must be tracked and audited at least yearly to ensure security is adequate.

Physical and logical access, including remote access, to diagnostic and configuration ports will be disabled or adequately controlled to prevent unauthorized access. Groups of information services, users, and systems will be segregated, segmented, or compartmentalized on networks to add a level of access control and security.

Servers publicly reachable through the Internet will reside in the DMZ (demilitarization zone) and will be separated from the internal network by a firewall. Servers containing confidential information should be segmented from the rest of the network for extra access protection. Systems communicating from the Internet to internal systems will be restricted to use only authorized communication ports. Firewall filters will block all ports and public systems will not be allowed direct access to internal systems, except to allow specific ports for business reasons approved by management and IT. Approval of exceptions will be documented and exceptions reviewed twice a year to make sure they are still needed.

All users will be automatically blocked from accessing Internet sites identified as inappropriate by the University. Users will not tamper with or bypass the blocking software. Exceptions to firewall, filtering, and such management practices may be requested through the IT department.

11.5 Operating System Access Control

Operating system default security settings (WPA keys, SSID, SNMP community strings, etc.) will be changed before taking the system into production. Default accounts will be disabled or passwords changed. Services, ports, and protocols that are not needed will be removed or disabled.

Passwords will not be transmitted between computers or stored in clear text. Generic user accounts accessed by many users should be avoided. User accounts should have an identified purpose and traceable to an individual person, for accountability purposes.

Administrators must have the ability to increase and decrease their privileges as needed or maintain separate accounts and use the more privileged account only when necessary. Administrator accounts will be reviewed quarterly, removing administrator privileges when no longer required.

Access to operating systems will be controlled by a secure logon procedure including:

- Display a warning notice that unauthorized access is prohibited (for example, “This is a private BYU-Idaho system. Do not attempt to login unless you are an authorized user. Any authorized or unauthorized access and use may be monitored and can result in criminal or civil prosecution or disciplinary action under applicable law or policy.”)
- Display no system information (such as operating system and version) that would help facilitate an attack or compromise until after the authorized users has successfully logged on

- Upon a logon failure event, indication that the username or password does not exist or is incorrect should be done in a manner that does not allow an attacker to guess and discover valid usernames
- The number of unsuccessful logon attempts to the enterprise domain, production servers, and network equipment, will be limited to no more than six with at least a thirty minute time delay before further attempts are allowed
- Log unsuccessful and successful logon attempts
- For production servers, send an alarm to the monitoring system when maximum number of logon attempts is reached
- Upon successful logon of production servers and network equipment, display the date and time of the previous successful logon and details of any unsuccessful logon attempts since the last successful logon
- Display no password being entered and transmit no password in clear text
- If a session has been idle more than 15 minutes, require the user to re-enter their password to reactivate the terminal

Systems for managing passwords will ensure privacy and password quality through the following precautions:

- Enforcement of the use of individual user accounts and passwords to maintain accountability
- Allowing users to select and change their own passwords
- Enforce minimum password length of eight characters using at least two character sets (upper and lower case alphabet, numbers, special characters)
- Forcing users to change temporary passwords at the first logon
- Prevent the re-use of at least the past ten passwords.

11.6 Application and Information Access Control

Purchased or developed software applications will allow only authorized personnel with legitimate reasons the ability to access, transmit, or display confidential information.

11.7 Mobile Computing and Telecommuting

Access to campus information resources is normally provided by BYU-Idaho web sites via the Internet. More direct access to the campus network by employees, also known as remote access, must be approved by department and IT management and will be encrypted and authenticated. Computers used for remote access should have a firewall, up-to-date antivirus software, and the latest operating system security patches. The user will be responsible for backup of information. The computer may access confidential information through encrypted transmission, but will not store such information on the PC, including portable storage devices, unless it is encrypted.

Telecommuting requires management approval and a suitability assessment. If approved it will be done using campus owned equipment over a campus owned or subsidized connection. The equipment and connectivity to the campus network should only be used by the employee and not others.

12 Systems Acquisition, Development, and Maintenance

12.1 Security Requirements of Information Systems

All security requirements will be identified at the requirements phase of a project and justified, agreed upon, and documented as part of the overall business case for an information system. Information systems include operating systems, infrastructure, business applications, off-the-shelf products, services, and user-developed applications.

12.2 Correct Processing in Applications

Validation checking will be incorporated into applications to ensure data is correct and appropriate and to detect any corruption through processing errors or deliberate acts. Data input errors and attacks, including buffer overflow and code injection, will be eliminated by checking for:

- Out-of-range values or exceeding upper and lower data volume limits
- Invalid characters in data fields, such as command initiation characters
- Missing or incomplete data or unauthorized or inconsistent control data

Data output from an application will be validated to ensure that the processing of stored information is correct and appropriate to the circumstances and may include:

- Plausibility checks to test whether the output data is reasonable
- Reconciliation control counts to ensure processing of all data
- Creating a log of activities in the data output validation process

12.3 Cryptographic Controls

Credit card numbers will be transmitted using at least 128 bit encryption. Credit card numbers should not be stored, but when required to meet a business requirement must be encrypted. Credit card full magnetic stripe data, verification codes, and personal identification numbers (PIN) must never be stored. Manage cryptography keys to insure they:

- Are protected from disclosure and misuse
- Are restricted as few custodians as possible
- Are stored securely in as few locations and forms as possible
- Re-keyed if suspected compromise
- Split knowledge and establishment of dual controls

12.4 Security of System Files

Access to program source code will be restricted and controlled to prevent the introduction of unauthorized functionality and to avoid unintentional changes.

Test data will be selected carefully, protected, and controlled. The use of operational databases containing confidential information for testing purposes should be avoided. If used, the information should be modified beyond recognition before use.

A balance will be maintained between the need to keep vendor supplied software up-to-date (with possible security enhancements) and the need to upgrade only when there is a justifiable business reason (to avoid possible down time). Software patches that remove or reduce security weaknesses will be applied as soon as possible and no later than one month. Installation of software on production systems will:

- Be guided and tracked by a configuration control system
- Be approved only for successfully tested and approved software
- Be performed by trained administrators upon management authorization
- Commence only after a rollback strategy is in place

Physical or logical access should be given to suppliers for support purposes only when necessary and with management approval. The supplier's activities should be monitored.

12.5 Security in Development and Support Processes

Change control procedures will be utilized for all changes to systems. All changes to programs must be properly authorized, strictly controlled, limited to necessary changes, and tested before moving to the live environment. When operating systems are changed, business critical applications will be reviewed and tested to ensure there is no adverse impact on organizational operations or security. Change control procedures should include:

- Documentation of impact
- Management sign-off by appropriate parties
- Testing of operational functionality
- Back-out procedures

The software and application development process will be based on industry best practice, secure coding guidelines, and will include information security throughout the software development life cycle. The development of web applications will be based on secure coding guidelines in order to prevent:

- Cross-site scripting
- Injection flaws
- Malicious file execution
- Insecure direct object references
- Cross-site request forgery
- Information leakage and improper error handling
- Broken authentication and session management
- Insecure cryptographic storage
- Insecure communications
- Failure to restrict URL access

Outsourced software will be developed using tools and methods approved by and under the supervision of Information Technology. Custom code involving payment card processing will be reviewed for vulnerabilities prior to release. The classification of information must be considered before giving, transmitting, interfacing, or storing information to make sure it is not accessible by unauthorized parties.

12.6 Technical Vulnerability Management

Timely information about technical vulnerabilities of information systems being used will be obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk. System components, processes, and custom software will be tested frequently to ensure security controls are effective, including:

- Test for unauthorized wireless access points at least quarterly
- Internal and external network vulnerability scans at least quarterly
- Internal and external, including network and applications, penetration test at least annually
- Continuously monitor traffic in zones with confidential information with up-to-date intrusion detection systems
- Monitor for file integrity on critical systems at least weekly

13 Information Security Incident Management

13.1 Reporting Information Security Events and Weaknesses

Users of information systems and services should note any observed security weakness, violation of information security policy, or unauthorized access to confidential data and report it as quickly as possible through appropriate management channels or to the Information Security Officer. In cases where confidentiality in reporting is needed or working through management channels is not appropriate, contact the CES Compliance Hotline at 888-238-1062.

13.2 Management of Information Security Incidents

Information security breaches should be reported without delay to the Information Security Officer to speed the identification of damage caused, restoration and repair, and to facilitate the gathering of associated evidence. The Information Security Committee, under the lead of the Information Security Officer, will be responsible for handling information security incidents. This team will draw on others as necessary, collect information and evidence, resolve the crisis, notify users and management, recommend changes in future operations, and evaluate lessons learned from the event. Information security incidents that may lead to criminal or civil legal action will require the collection of evidence in a manner that conforms to the rules for evidence. Assistance from University Security and the Information Security Officer should be sought before collection activities begin. Notification must be made to customers as soon as reasonably possible when their personally private information has been exposed or lost and there is reason to believe the information could be used misused. Personally private information includes but is not limited to the loss of a person's name and one the following: social security number, credit card number, bank account number, or driver's license number.

14 Business Continuity Management

A business continuity and disaster recovery management process will be developed and implemented to maintain or restore critical business processes. Events that can cause interruptions will be identified, along with the probability and impact of such

interruptions and their consequences for information security. Business continuity and disaster recovery plans will be tested and updated regularly to ensure that they are still relevant and effective.

15 Compliance

15.1 Compliance with Legal Requirements

The University and users of campus systems and data will comply with the:

- Family Education Rights and Privacy Act (FERPA) federal statute, which protects the privacy of all records of individual students. See the *Access to Student Records* (4-4) policy.
- Graham-Leach-Bliley Act (GLBA) federal statute, which protects any record containing non-public financial information about a student or any third party who has a relationship with the University. See the *Privacy of Financial Information* (3-7) policy.
- Health Insurance Portability and Accountability Act (HIPAA) federal statute, which protects the privacy of individuals whose medical records, including mental health, are processed or stored by the University.
- Idaho statutes 28-51-104 to 28-51-107, which require the University to notify individuals if their personally identifiable information has leaked and it has been or is likely to be misused.
- Idaho statutes 18-2201 and 18-2202, which prohibits accessing, attempting to access, altering, or damaging a computer, system, or network without authorization. It further prohibits the use of such systems (even by one who has authority) with the intent to commit crime.
- Intellectual property rights and copyright law. See the *University Guidelines for Copying* (1-16) policy.
- Licensing agreements of software applications.

15.2 Compliance with Security Policies/Standards

Managers will ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies, standards, and best practices. Areas that process credit cards must comply with the *Payment Card Industry Data Security Standard* (PCI DSS). Important records should be protected from loss, destruction, and falsification.

15.3 Information Systems Audit Considerations

Audit requirements and activities involving checks on operational systems should be carefully planned and agreed upon to minimize the risk of disruptions to business processes. Access to information systems audit tools should be protected to prevent any possible misuse or compromise.