

Internal Use Only

BRIGHAM YOUNG
UNIVERSITY

IDAHO

Information Technology

Information Security Plan

Draft 1

- 1. **Executive Summary**..... 3
- 2. **Terms** 3
- 3. **Introduction** 3
- 4. **Risk Management**..... 4
- 5. **Information Security Policy** 5
- 6. **Organization of Information Security**..... 6
- 7. **Information Asset Management**..... 6
- 8. **Human Resources Security**..... 7
- 9. **Physical and Environmental Security** 7
- 10. **Communications and Operations Management** 8
- 11. **Access Control**..... 10
- 12. **Systems Acquisition, Development, and Maintenance** 12
- 13. **Information Security Incident Management**..... 13
- 14. **Business Continuity Management**..... 14
- 15. **Compliance**..... 14

1. Executive Summary

Information security is based on making sure information is available only by those who should have access to it (confidentiality), is modified only by those who are authorized to do so (integrity), and is available when and where it is needed (availability). Balancing this triad of confidentiality, integrity, and availability is based upon risk management. Risk management is all about assessing the threats and vulnerabilities in the system, process, and people, and implementing ways to mitigate or reduce those risks to an acceptable level. This too is a balancing act, because there is not enough time or money to totally eliminate all risks. This information security plan is based on the international standard ISO 17799:2005, which is a risk-based best practices approach to information systems security. It is a description of the current information security program with comments on next steps that need to be taken. The completion and regular updating of the plan will lead to continuous improvement in information security at BYU-Idaho. Such improvements contribute to the ability of Information Technology (IT) to ultimately help enable the mission of the University.

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

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

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

PCI DSS- Payment Card Industry Data Security Standard, which must be complied with by any campus department that processes credit cards

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 eliminate risk or reduce it to an acceptable level

3. 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. This information security plan is a means achieving the right balance, reviewing, and continually improving security programs and processes.

4. Risk Management

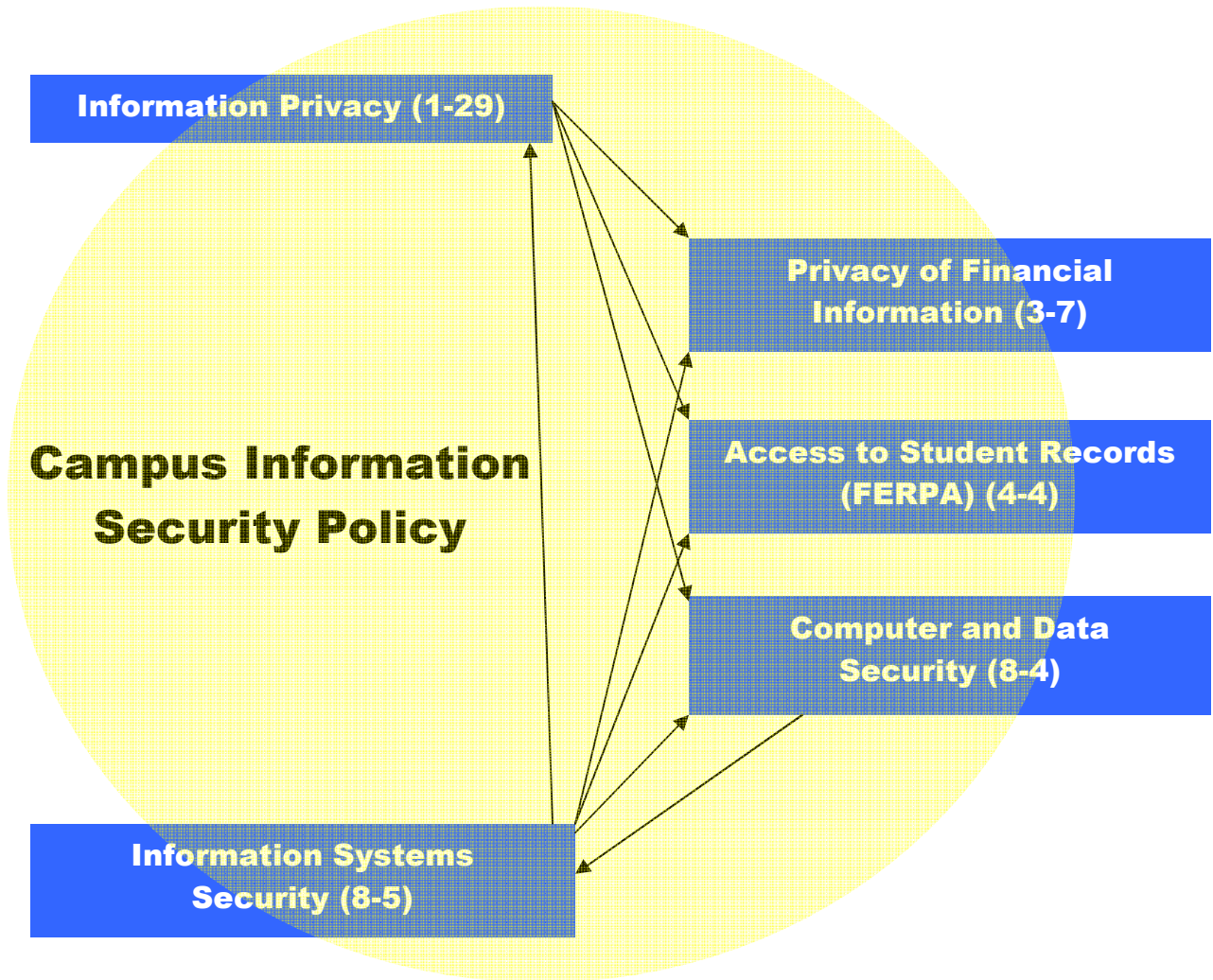
Risk assessments should identify, quantify, and prioritize risks against criteria for risk acceptance and objectives relevant to the organization. The results should guide and determine the appropriate management action and priorities for managing information security risks and for implementing controls selected to protect against these risks. The process of assessing risks and selecting controls may need to be performed a number of times to cover different parts of the organization or individual information systems.

An information security policy was approved in January of 2008 that states, “A risk assessment will be performed 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.” A checklist of items to consider during a risk assessment of new systems, processes, and projects should be compiled and used as a tool to aid in the procurement of more secure systems and processes. Such assessments done upfront will result in better security at a lower cost than doing so after the fact.

A comprehensive risk assessment of Information Technology was completed and a report of audit issued in August of 2007. Of the many risks identified, five were considered most important with a focus to mitigate them. These risks are being tracked by the Information Security Officer. Comprehensive risk assessments are difficult, time consuming, and needed from time to time. However, risk assessments that are ongoing as projects are undertaken and as systems are being procured can be more in-depth and much more meaningful to the overall cause of information security. Imbedding risk assessment into portfolio management and system procurement will require a cultural change in the way IT functions.

5. Information Security Policy

Information security policies provide direction and support for information security in accordance with university requirements and relevant laws and regulations. In January of 2008, two new policies were approved by President’s Council, which combined with existing policy make up the information security policy for the campus. The *Computer and Data Security* and *Information Systems Security* policies are newly approved and combine with the *Information Privacy* and related policies to make up a comprehensive information security policy. All employees are required to sign a statement acknowledging their understanding and acceptance of their responsibilities toward information security. Information security policy will be updated annually to ensure its continuing relevancy.



6. Organization of Information Security

Management recognized the need for an information security program and appointed a full time Information Security Officer (ISO) in late 2006, who reports to the Chief Technology Officer (CTO) and is a peer of the IT directors. The CTO is the head of the IT department, reports to the Vice President of Academics, often meets with the President, and is on the extended President's Council.

Cross-functional input and diverse representation for information security activities will come from the:

- Information Technology staff (directors and direct reports to the CTO)
- Privacy Committee, which is chaired by the Financial Services Director with the Financial Aid and Scholarship Director, Health Services Director, Internal Auditing Director, International Services Coordinator, ISO, Registrar, and a CIS professor as members
- Information Security Committee, which is chaired by the ISO with the Lead Software Engineer, Network Supervisor, Senior System Administrator, Senior Technology Support Specialist, System Supervisor, and CIS and CS professors as members

The ISO will be responsible for the overall orchestration of information security as aligned with the mission of the University. However, for a security program to be successful, everyone must be involved and security must be embedded in processes and procedures throughout the University. Likewise, each department must assess their own unique security needs and inform their users of their responsibilities toward information security. Each individual person is responsible for the security of the assets under their control.

7. Information Asset Management

7.1. Responsibility for Information Assets

Inventories of assets help ensure that effective asset protection takes place. The process of compiling an inventory of assets is an important aspect of risk management. An organization needs to be able to identify its assets and the relative value and importance of these assets. Based on this information an organization can then provide levels of protection commensurate with the value and importance of the assets. The ownership of information assets is defined in the *Data Stewardship* (8-1) policy. The data steward must give permission before information can be used.

7.2. Information Classification

Information maintained by the University needs to be classified and protected accordingly. The classification of information is defined in the *Information Systems Security Policy* (8-5), section 7.2.

8. Human Resources Security

8.1.Prior to Employment

When hiring new personnel, the University must implement security procedures to minimize the risks of human error, fraud, and misuse of resources. Security concerns should be addressed as early as the recruitment stage.

Human Resources were informed of the need to do a credit- and criminal-check on potential new hires who will deal with credit cards. They balked because of the cost of doing this. Upon further research it was determined we could greatly limit the scope of background checks by requiring a credit- and criminal-check only on those who have access to lists or a database of credit card numbers. This is stance is necessary in order to be PCI DSS compliant.

8.2.During Employment

Security awareness training ensures that University computer users are knowledgeable about university policies, guidelines and procedures that they are expected to comply with. User training, whether delivered through formal instructor-led classes or through online classes, brochures and printed materials, is an important means of ensuring that users are familiar with basic information security practices and are able to apply them in protecting information technology resources they maintain.

New employees are required to sign an *Employee Information Usage Agreement*, which refers them to campus information security policies and online information security awareness training. This should be strengthened by:

- Requiring all employees to complete the online training
- Incorporating specific security responsibilities in job descriptions
- Including awareness information in new student orientation and the catalog

8.3.Termination or Change of Employment

The access rights of all employees, students, and third party users of information and information processing facilities should be removed or adjusted when they terminate their association or change their relationship with the University. Upon termination of employment, a user's rights to access information and information processing facilities are removed. There also needs to be a process in place that will review and if necessary change the rights of employees undergoing a change of assignment.

9. Physical and Environmental Security

9.1.Secure Areas

Important business information processing facilities should reside in secure areas with appropriate security barriers and entry controls. The protection provided should be commensurate with identified risks. Moreover, procedures and physical security measures should be developed to prevent and detect unauthorized interference, access, or damage to these facilities. The objectives of this section are to reduce risks of human

error, theft, fraud or misuse of facilities and to ensure that users are aware of information security threats and concerns.

In response to the 2007 risk assessment, IT management has committed to provide more controlled and uniform access to the data center, telecommunication center, and telecommunication rooms. They also committed to improve the physical security of the IT suite of offices, especially during the early morning cleaning hours.

9.2. Equipment Security

Critical computer and communications equipment should be protected from physical and environmental threats. The data center, telecommunication center, and some telecommunication rooms need to be upgraded to provide growth, reliability, and security. These upgrades will happen in 2008 and 2009. The need to lock all campus manholes has been pointed out to Physical Facilities and their plan to correct this needs to be verified.

The secure erasure of confidential information from computers being repurposed or sent to surplus has been formalized. Providing a means for users to likewise shred their confidential information is being formalized. At the same time the means for a user to encrypt confidential information on their local drive, network drive, USB drive, CD, DVD, etc. is also being formalized.

10. Communications and Operations Management

10.1. Operational Procedures and Responsibilities

Policies for the management and operation of all university information processing facilities should be established, codified, and communicated to all employees in order to ensure correct and secure operation. This includes the development of appropriate operating instructions, incident response procedures, and segregation of duties where appropriate.

In general, the operating procedures within IT need to be better documented and maintained. Security specific job responsibilities should be included in job descriptions.

10.2. Third Party Service Delivery Management

The University should embed risk and security assessments with any consideration of third party services. Such assessments can help avoid unpleasant surprises and costly mistakes.

A contract should require PCI DSS compliance of any third party service, product, or software application that will be used to process credit cards. The Bookstore vendor is trying to, but is not yet PCI DSS compliant.

10.3. System Planning and Acceptance

Advanced planning is required to ensure the availability and adequate capacity of University resources. This planning entails projecting future capacity requirements to reduce the risk of system overload. Moreover, the operational requirements of new systems should be established, documented and tested prior to their acceptance and use.

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

10.4. Protection against Malicious and Mobile Code

Controls should be implemented to prevent and detect the introduction of unauthorized or malicious software. University computers are vulnerable to a large number of malicious programs such as computer viruses, network worms, Trojan horses and logic bombs. Users should be made aware of these dangers and managers should, where appropriate, introduce special controls to detect or prevent their introduction.

Improvements in this area should be achieved by the introductions of intrusion prevention technology the network upgrade in 2008 and 2009. In addition, firewalls on personal computers need to be turned on.

10.5. Backup

In order to maintain the integrity and availability of information processing and communication services, procedures should be established for carrying out the agreed back-up strategy.

IT needs to create and follow a backup policy. IT is pursuing live offsite disk storage that will provide another form of offsite backup. Users, in general, need to regularly backup their files that are not on the network drive (which is automatically backed up by IT). IT should encrypt backup data of confidential information.

10.6. Network Security Management

Security management will be implemented to safeguard university networks and supporting infrastructure. Additional controls may also be required to protect sensitive data passing over public networks.

In 2008 and 2009, the network team will be implementing a new network with improved security architecture and systems for monitoring security. The network team will need to add to their duties the responsibility of monitoring network security. This will be done presumably through log file collection and correlation, event management and correlation, and intrusion detection/prevention systems. The network architecture, including a network diagram, needs to be documented and kept up-to-date.

10.7. Media Handling

In order to prevent damage to assets and interruptions to business activities, media should be controlled and physically protected. Appropriate operating procedures should be established to protect documents, computer media (tapes, disks, and cassettes), input/output data and system documentation from damage, theft and unauthorized access.

The loss of confidential information through the surplus or loss of computers, laptops, USB disks, etc. is a concern. We need to make sure server disks are securely erased or destroyed when they are repurposed or sent to surplus. As the storage area network is used more, similar precautions need to be implemented when disks are replaced. *Data Encryption and Shredding Guidelines* is being finalized to instruct users how to encrypt and shred their confidential files.

10.8. Exchange of Information

Procedures and standards to protect information and media in transit should be established to prevent the loss, modification or misuse of exchanged information. Furthermore, exchanges of information and software between organizations should be both controlled and compliant with any relevant legislation.

Awareness needs to be heightened of existing *Data Stewardship* policy that requires permission to use confidential information in programs or data transfers. Exchange of information with a third party also requires a non-disclosure agreement. Awareness also needs to be heightened that e-mail is not a secure way to exchange confidential information. This is spelled out in *Information Privacy* policy and online training.

10.9. Electronic Commerce Services

The university will take steps to ensure the security of electronic commerce services. The security implications associated with using electronic commerce services, including on-line transactions, and the requirements for controls, should be considered.

The University is not in full compliance with PCI DSS. Steps to become compliant have been identified and are being worked on. Some steps will be taken as part of the 2008 network upgrades. However, progress has been slow. Management needs set a goal for compliance and vigorously pursue it.

10.10. Monitoring

University systems should be monitored and information security events should be recorded.

As has been already mentioned, monitoring will be a huge undertaking, mostly borne on the back of the Infrastructure department, and will require changes in equipment, processes, and job responsibilities. This is perhaps the most critical and difficult step that needs to be taken to improve our overall security posture. A major undertaking for the IT department will be to collect and correlate log files, event management, and monitoring. We must develop the ability to know when we are under attack, have lost confidential information, or recognize some other improper event is occurring. Management believes these capabilities must be integrated into the processes and job descriptions of IT personnel rather than assigned to information security personnel. Initiatives to strengthen monitoring capabilities and intrusion detection systems are planned coincide with major network upgrades scheduled to begin the last quarter of 2008.

11. Access Control

11.1. Business Requirements for Access Control

Access to university information and business processes should be controlled on the basis of business and security requirements according to university policies and procedures. Furthermore, this should take into account the policies for information dissemination and authorization.

We need to be able to track who accessed the data center, telecommunication center, and telecommunication rooms and when.

11.2. User Access Management

Formal procedures should be in place to control the allocation of access rights to university information systems and services. The procedures should cover all stages in the life-cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services. Special attention should be given, where appropriate, to the need to control the allocation of privileged access rights, which allow users to override system controls.

In this area, several issues need to be considered:

- We need to have control over password strength, changes, and expiration
- CES is considering changes to the shared NetID and password system and we need to be on top of the proposed changes and in a position to influence them
- The Microsoft active directory needs to be looked at for organizational, procedural, and security issues culminating in a written architecture and procedures
- Generic and shared accounts need to be replaced with better alternatives
- The system of expiration and deletion of accounts needs to be enhanced
- A secure method of handling account and password change requests

11.3. User Responsibilities

Users must be made aware of their responsibilities for maintaining effective access controls, particularly regarding the use of passwords and the security of user equipment. Users can be the weakest link in the information security chain and must receive continual training and reminders to increase their awareness.

An information security policy has been approved, which has been included in the information privacy online training. All employees are required sign the *Employee Information Usage Agreement* and encouraged to complete the *Information Privacy and Compliance Training* on the BYU-Idaho web site.

11.4. Network Access Control

To ensure that users do not compromise the security of university network services, the University is required to control access to both internal and external networked services.

Part of the network upgrade will be to implement the checking of personal computers for viruses and security patches prior to allowing access to the network.

A good security practice we follow on this campus is to not allow anything from the Internet to have direct access to any system inside the campus network. This is being done in all cases except two high profile systems, Alma and Spencer. Alma is the Library catalog server and Spencer is our main IBM databases, including much confidential information. Correcting this problem for Alma will require an additional server put in the DMZ and significant configuration changes. Correcting this problem for Spencer will require replacing old applications that depend on direct access from the Internet.

11.5. Operating System Access Control

In order to prevent unauthorized computer access, operating system configurations should be used to restrict access to computer resources. These settings should be capable

of identifying and verifying the user identity, recording successful and failed system accesses, and providing appropriate means for authentication.

The 2007 vulnerability assessment pointed out that some server ports have unnecessarily been left open. The server group downloaded a tool (Nessus) and have agreed to evaluate the situation.

11.6. Application and Information Access Control

Controls should be used to restrict access within application systems. Logical access to software and information should be restricted to authorized users. The application systems should control user access to information and system functions in accordance with a defined access control policy.

11.7. Mobile Computing and Telecommuting

To ensure information security in a mobile computing environment the university must implement controls that are commensurate with the risks.

Decisions need to be made whether to allow SSL VPN for student and employee use or to continue to make applications available through web applications. Will the existing employee VPN be expanded, maintained, or phased out?

12. Systems Acquisition, Development, and Maintenance

12.1. Security Requirements of Information Systems

During the requirements-gathering phase, security reviews are necessary to ensure that controls and security requirements become a part of the overall design process.

We need to figure out how to embed risk and security assessment into the purchase and development of new information systems.

12.2. Correct Processing in Applications

Appropriate controls should be designed into applications, including user developed applications to ensure correct processing. These controls should include the validation of input data, internal processing and output data.

We need to determine if our programmers understand secure programming techniques and provide training in areas that are lacking. Programmers need to be involved in a group that keeps up with programming security issues such as the Open Web Application Security Project at www.owasp.org.

12.3. Cryptographic Controls

Cryptographic controls are necessary to protect the confidentiality, authenticity, or integrity of confidential information that is at risk and not adequately protected by the institution by other controls.

The privacy committee has had many discussions on the possibility of losing confidential information by losing a laptop or USB drive. The auditing department is going to survey campus employees to see how common it is to have confidential

information on mobile or local devices. *Data Encryption and Shredding Guidelines* is being developed to help shore up this potential problem.

12.4. Security of System Files

Access to system files and program source code should be controlled, and IT projects and support activities conducted in a secure manner. Care should be taken to avoid exposure of sensitive data in test environments.

12.5. Security in Development and Support Processes

Managers responsible for application systems should also be responsible for the security of the project or support environment. They should ensure that all proposed system changes are reviewed to check that they do not compromise the security of either the system or the operating environment.

12.6. Technical Vulnerability Management

Technical vulnerability management should be implemented in an effective, systematic, and repeatable way with measurements taken to confirm its effectiveness. These considerations should include operating systems, and any other applications in use.

IT contracted with Trustwave to perform monthly scans of PCI DSS related systems and we have been passing those tests.

A vulnerability scan was performed on BYU-Idaho Internet-facing web servers and an audit report issued in November 2007. Six general vulnerabilities were identified as needing to be resolved. The progress on these vulnerabilities is being tracked by the Information Security Officer. IT personnel have been assigned to go over reports of vulnerabilities, focusing on high and medium vulnerabilities. Follow-up on identified vulnerabilities has been slow.

A more continual process of vulnerability and penetration testing capability within IT needs to be pursued.

13. Information Security Incident Management

Responsibilities and procedures should be in place to handle information security events and weaknesses effectively once they have been reported. A process of continual improvement should be applied to the response to, monitoring, evaluating, and overall management of information security incidents.

The Information Security Committee, under the lead of the ISO, is 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.

Perhaps there should be an incident response team independent of the Security Committee. It would be hard for members of the committee, especially faculty, to respond to an immediate request to meet and work through an incident. Someone with computer forensic expertise should be identified as available when needed.

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.

A business continuity/disaster recover plan is part of the IT strategic plan and in response to the 2007 risk assessment has been committed to by management to be completed by the end of 2008.

15. Compliance

15.1. Compliance with Legal Requirements

The University and users of campus systems and data will comply with FERPA, GLBA, HIPAA federal statutes, and other state statutes as outlined in information security policy and online training.

An assessment of BYU-Idaho compliance with PCI DSS was performed with a report issued in March 2007. BYU-Idaho is not in complete compliance with the standard. The earliest estimated date of compliance is the last quarter of 2008. Progress toward compliance is being tracked by the ISO.

The Health Center should be audited to verify HIPAA compliance.

15.2. Compliance with Security Policies/Standards

It is necessary to ensure compliance of information technology systems with university information security policies and standards. In order to accurately review security controls that are supposed to be in place, it may be necessary to perform vulnerability assessment or penetration testing.

Now that there is an information security policy, auditing activities should determine to what extent the campus population is aware of and adheres to policies. Furthermore, IT personnel should be audited to determine the extent of compliance. These activities also help increase user awareness and the need to comply.

15.3. Information Systems Audit Considerations

It is desirable to maximize the effectiveness of system audits and to minimize business disruptions due to vulnerability and/or penetration tests performed on university information technology resources. Audit and vulnerability assessment tools must be appropriately utilized by trained staff members to prevent unintentional damage to systems, applications and data.

Audit requirements and activities involving checks on operational systems are carefully planned and agreed upon to minimize the risk of disruptions to business processes. Notice of audits, vulnerability scans, and penetration tests are given in advance of such activities.