Introduction

This document describes the universe of best practices for controlling information technology. The first section deals with general controls and measures that should be in place to ensure the IT environment is able to support data and process integrity through the proper use of security controls. The second section deals with controls that are specific to applications run, and data analyzed and stored in a specific department, school, or college.

General Controls

General controls are designed to manage and monitor the information technology environment and affect all information system-related activities. They are pertinent to all applications. General controls ensure the proper development and implementation of applications, the integrity of program and data files, and the integrity computer operations.

Each of the following sections provides lists of best practices for specific areas of information technology. These practices affect the overall IT environment including the acquisition, implementation, delivery, and support of IS systems and services and influence the implementation of software packages, system security parameters, disaster recovery planning, data input validation, exception report production, locking of user accounts after invalid attempts to access them, and other essential IT processes.

Organization and Operations Controls

1. Segregate key functions of computer programmer, systems analyst, and computer operations within the IT department.
2. Prohibit the IT group from initiating or authorizing transactions.
3. Create an IT steering committee for the organization.

Administrative Controls

1. Create an overall security policy to establish guidelines and standards for accessing the organizations information and application systems.
2. Create an acceptable use policy that details acceptable behavior by the organization's employees whilst they are utilizing the organizations IT equipment and information.
3. Create policy and standards on record retention, protection and destruction, online storage, audit trails, and integration with an enterprise repository.
4. Address data ownership, confidentiality of information, and use of passwords in a data security policy.
5. Prepare a policy documenting the organization's response to IT incidents.

Documentation Controls

1. Create and maintain a current organization chart.
2. Create and update a Security Plan (in compliance with IIA guidance).
3. Create and maintain a complete server inventory.
    a. Designate appropriate servers as "mission critical."
4. Create a network diagram of the organization's system and its interfaces to the UM backbone.
5. Prepare documented descriptions of systems software and hardware.
6. Create a documented disaster recovery plan and share it with IT staff.
7. Create and test a documented backup strategy.

   a. Ensure that critical data is backed up at least once a day.
   b. Verify that backup media is kept in a secure locked storage to prevent theft or tampering with stored data.
   c. Test backup media and replace it as required.
8. Create a contingency plan for any critical system in the event the system becomes unavailable.
9. Keep user manuals from vendors for pre-built systems or develop documentation for systems developed in house.
10. Maintain a software license catalog of system software and applications.
11. Retain risk and security assessments for system.

Environmental and Physical Controls

1. Confirm that no flammable materials are stored on the floors immediately above or below the data center.
2. Restrict physical access to the data center, computer room, and the telecommunications room.
   a. Ensure that data center doors effectively restrict access.
   b. Require visitors to sign in when visiting the data center.
3. Ensure that the temperature and humidity in the room where hardware is housed is appropriate for the equipment.
4. Require the following environmental controls in the data center:
   a. Fire suppression equipment (preferably dry lines)
   b. An uninterrupted power source (UPS) system
   c. Emergency power sources (EPS); i.e., generators are installed
   d. Smoke and water detectors
   e. Emergency lighting
5. Test environmental controls periodically.
6. Verify that maintenance contracts exist for environmental controls.
7. Require regular maintenance on the environmental control system equipment.
8. Confirm that devices are attached to an Uninterruptible Power Supply Device (UPS) and/or surge protector.
9. Make certain server consoles are not left logged in at any point of time.
10. Require that servers be configured with a "time out" feature on the console system.
11. Lock the system administrator console when unattended.

Physical Access and Security Controls

1. Limit access to hardware to only those with a defined need to have such access.
2. Require key locks or card-key access for computer rooms.
3. Store servers in locked racks.
4. Restrict entry and exit to equipment and wiring closets to only authorized personnel.

Logical Access Controls

1. Assign unique user ids to all users.
2. Automatically log off unattended computes after 30 minutes of inactivity.
3. Use lengthy, smart passwords for network, application, and privileged host access.
   a. Enforce a minimum length password by the operating system or application.

   b. Never store password as plain text.
   c. Configure a password-aging feature on the networks and hosts.
      i. At a minimum, the last ten passwords should not be able to be reused.
4. Force users to change their passwords at least annually.
5. Mask passwords everywhere in the system.
6. Grant access based upon the least privilege required to get the job done.
7. Require all user access requests be properly authorized.
8. Eliminate user IDs and passwords from the system in the shortest time possible when authorized users leave the organization.
9. Monitor activity of users with privileged access.
10. Use event logs to record security-related events and review them on a regular basis.

Network Security

1. Document normal values for network statistics (i.e., metrics).
2. Monitor the network for malicious and/or abnormal activity.
3. Ensure that patches are subject to a change management process with adequate testing and approvals.
4. Encrypt system transmissions that contain sensitive and/or confidential information.
5. Regularly monitor logs from network devices such as VPN, routers, IDS, IPS, and firewalls for suspicious activity.
6. Ensure regular reviews for suspicious activity in the log files by the administrator.
7. Use a log analyzer to systematically analyze the logs.
8. Use an intrusion detection system and regularly update signatures.
9. Set strong passwords (minimum eight characters, includes mixed case and special characters) and make sure passwords are regularly changed on routers.
10. Remove default passwords from all networking devices.
11. Remove all unnecessary services from network devices.
12. Use more secure protocols (e.g. using SSH instead of telnet) on security network devices.
13. Perform a vulnerability scan at least annually on network devices such as routers and firewall.

Server Operating System Security

1. Install the most current version of the operating system unless there is valid justification for not installing the most current version.
2. Install all known operating system fixes unless valid justification exists for not installing certain fixes.
3. Ensure that procedures are in place to inform system administration personnel of available operating system fixes in a timely manner.
4. Develop guidelines and standards for creating a secure configuration of operating systems and document them.

Host-Based Security Controls

1. Perform a security assessment (RECON) on the system.
2. Perform vulnerability scans periodically and address all high-risk vulnerabilities or verify them to be false positives.

3. Install host-based security tools such as Intrusion Detection and File Integrity Checkers on servers that contain mission critical data and/or confidential data.
4. Disable all unnecessary services on system.
5. Provide services using the “Deny first, then allow" principle.
6. Close all unused TCP/UDP ports.
7. Define normal values of system statistics such as CPU load, number of interrupts, memory scan rates, and other statistics so determining an unusual value will be possible.
8. Backup the entire systems when making systemic changes, such as system upgrades or major application upgrades.
9. Backup individual files when making minor changes.

Firewall Controls

A firewall is a key network control device. It helps administrators govern the network traffic to and from their internal network, and serves as a primary line of defense against external threats.

1. Actively monitor firewall and network traffic.
2. Include a ‘deny all’ rule at the end of the firewall rules.
3. Subject changes made to the firewall configuration to a rigorous change management process.

Anti-Virus Protection

Anti-virus software is available to University faculty, staff, and students at no cost. It is important to develop appropriate virus detection and eliminate the threat for servers. Automatic updates to anti-virus software are essential to ensure that new viruses are detected in a timely, systematic fashion. It is a systems administrator's responsibility to ensure anti-virus definitions are up to date.

1. Use anti-virus software on workstation, servers, and firewall machines.
2. Update anti-virus definitions on a timely basis.
3. Scan the systems for virus, worm, and Trojan activity on a regular basis.

Spyware and Adware Protection

Spyware and adware pose security, privacy and productivity risks. It is important to keep critical systems protected from such malicious programs.

1. Use appropriate anti-spyware and adware tools on critical systems.

Data Security Controls

1. Classify information created and stored in the department, school, or college as to sensitivity.
2. Establish appropriate access control for sensitive datasets.

Sensitive Data Security Controls

1. Classify information created and stored in the area as to sensitivity.
2. Perform risk assessment on information systems that house or process sensitive information to establish a risk-based methodology for selecting and justifying safeguards.
3. Maintain a list of roles or security levels that merit access to sensitive data.
4. Keep a list of all users (including students, temps, and contractors) with access to sensitive information documenting their access rights, privileges, and reasons they were granted.
5. Review users’ rights to sensitive data at least annually.

6. Automatically terminate access rights to sensitive information for users who are not 'regular' employees after a fixed period of time.
7. Log activity in information systems that contain sensitive data and review the logs on a regular basis.
8. Systemically monitor systems and the network and address any intrusions.
9. Create procedures to address the security of storage media and how well electronic documents are protected for both current and future use.

Database Security

1. Perform a security assessment (RECON) on the system that contains the database containing critical information.
2. Encrypt critical information stored in the database.
3. Use the auditing and logging features on the system to capture pertinent information pertaining to all user activities.

Systems Development and Maintenance Controls

1. Address the following procedures in the written change control procedures:
    a. Proper approval to implement program changes
    b. Documentation describing nature and logic of proposed change
    c. Methodology for testing changes
    d. A log of all changes
2. Document user participation and testing of system changes.
3. Users should assign priority to outstanding change requests.
4. Implement changes to production by personnel not responsible for making those changes.
5. Create a test environment to develop, make changes, and test applications systems prior to their implementation.
6. Document emergency change procedures.
7. Migrate emergency changes through segregated libraries to enable review and approval by management.
8. Maintain complete records of modifications made to system or application software.

Backup/Recovery Controls

1. Ensure that all files, including system files, are backed up on a regular, systematic basis and include full and incremental backups.
2. Backup the entire system when making systemic changes, such as system upgrades or major application upgrades.
3. Backup individual files when making minor changes.
4. Rotate offsite backup copies of system, program, and data files on a scheduled basis.
5. Ensure that backups have the same controls and level of security as the equivalent production files.
6. Make sure the offsite backup location is secure and environmentally sound.

Contingency Planning / Disaster Recovery Controls

1. Develop a continuity of operations plan.

2. Test the continuity of operations plan on a regular basis.
3. Prepare and test an IT disaster recovery plan.

Application Controls:

Application controls are designed to ensure the completeness and accuracy of the records and the validity of the processing. Application controls must be specific to the transactions and data within individual programs as each program may have unique requirements.

Application Access Controls

1. Authenticate all users are authenticated when they are granted access.

Application Support Controls

2. Ensure that not only operating systems but also applications are patched regularly and kept up-to-date.
3. Develop a standard process for applying software patches to all software programs on the critical systems on a timely basis.
4. Subject all application patches to the change management process.
5. Develop a test environment for proof of concept work, and a quality assurance environment practice for production procedures.

Spreadsheet Controls

1. Maintain inventory and risk-rank spreadsheets related to critical financial risks.
    a. Perform a risk-based analysis to identify spreadsheet logic errors. Automated tools exist for this purpose.
    b. Ensure the spreadsheet calculations are functioning as intended (i.e., "baseline" them).
    c. Ensure changes to key calculations are properly approved.

Records Management Controls

1. Define a records management program for paper, electronic, and transactional communications, which includes emails, instant messages, and spreadsheets.
2. Create a retention life cycle addressing records management practices, audit trails, and the accessibility and control of the retained content.