Table of Contents:

Introduction

Security Plan

• Administrative Controls

• Operational and Technical Controls
  o Identity and access management
  o Access controls
  o Systems and Application Security
  o Network Security
  o Change Management
  o Audit Logs
  o Encryption

• Physical and Environmental Controls
  o Risk mitigation measure
  o Physical access controls
  o Inventories of devices including their movement
  o Disposition of equipment
  o Portable devices and media
Introduction

Campus organization and departments must utilize appropriate safeguards to protect sensitive and/or protected information resources based upon the sensitivity of data in question, legal requirements, and risks to the university. These safeguards are expressed within a technical information security plan.

Security Plan

The information security plan should include measures to enhance the security of information assets, including administrative, operational, technical, physical and environmental controls. Components of this plan should include the following measures.

- **Administrative Controls**

  Administrative controls include establishing sound authentication and authorization processes and procedures with respect to positions that require access to information resources. The emphasis of these processes and procedures is on security, with an aim to provide information workers guidance as they perform their duties.

  People in the organization should be identified as responsible for determining who has access to what information resources and their level of privilege. Once that is done, procedures should be implemented to:

  - authorize access only for those who need it, with the least permissions necessary
  - change access when task assignments change or when people leave the University
  - initial access authorization, changes, and termination should be recorded and retained
  - follow principles of separation of duties with restricted or essential data
  - review on a regular basis the work of people with privileged access

  Some positions need access to restricted information as part of their duties, and may be deemed critical positions. Such positions should have appropriate background checks as part of the selection process, and procedures should be developed to revoke access in cases of termination or disciplinary action.

  Procedures should be developed for appropriate action if unauthorized access is discovered, including reporting the action (whistleblower policy), and steps to take when it is discovered.

- **Operational and Technical Controls**

  Passwords, network controls, change management and controls to reduce risk from known threats constitute examples of technology and/or operational controls that, if implemented effectively, improve chances of meeting security objectives.

  - **Identity and access management**

    Departments should use identity and access management processes that provide secure, authenticated access to network based services. Control measures should be secure and provide accountability.
Access controls

Access controls typically include login accounts or the use of a campus identifier, should be instantiated in a manner consistent with campus standards, and records of access should be kept in accordance with audit log guidelines.

Appropriate password management should include periodic identification of weak passwords and use of sufficiently strong encryption technologies. The risk of using the same password for multiple applications should be noted, and for critical positions, mitigated in some way, for example with two factor methods. Passwords and other authentication credentials should be considered restricted information and should be protected in transit or at rest. Passwords should be strong and not shared. If circumstances require sharing, a way to determine who accessed Resources should be devised and logged.

Automatic logouts or session timeouts should be in place for all devices with access to restricted resources.

Privileged accounts should only be used for authorized purposes and procedures commensurate with the level of risk, should be in place to prevent abuse.

- privileged users should be informed of their responsibility to keep Resources secure and not divulge information discovered as part of routine duties
- the number of privileged accounts should be few
- privileged users should have non-privileged accounts to perform duties that don't need root
- privileged account use should be logged
- privileged account use should be monitored and reviewed regularly

Systems and application security

The security of applications and systems should be the responsibility of people knowledgeable about information technology. They should be aware of applicable UC, campus and departmental policies. They should develop operational security plans commensurate with the level of risk of each resource via periodic risk assessments, and regularly evaluate resource exposure to potential threats. Backup plans should be devised to include recovery of systems with essential data in the case of disaster, as well as to encrypt restricted data. Personal or desktop computers with restricted or essential data should be included in the backup plan. Retention of backups must comply with UC policy regarding electronic data retention.

Measures should be deployed to protect systems with restricted or essential data from malicious software. These systems should also be kept up to date with respect to security and other important patches.

Application development and maintenance should conform to the specification in BFB IS-10 as well as any local standards, procedures, guidelines and conventions. Developers should conduct an analysis of how personal information should be collected, stored, shared and managed for any application that will be used to process personal information. Internal Audit should be involved early in the application development process.
Network security

All department servers and personal machines should follow local minimum requirements for network connectivity. Firewalls and/or IDS or IPS devices should be used to limit system attacks, with special attention paid to systems with essential and/or restricted data.

Change management

Changes to resources with essential or restricted data should include:

- monitoring and logging of all changes
- steps to detect unauthorized changes
- confirmation of testing
- authorization for moving application programs to production
- tracking movement of hardware and other infrastructure components
- periodic review of logs
- back out plans, and
- user training

Audit logs

Organizations are encouraged to develop a centralized log management infrastructure to protect logs on systems of record and to provide forensics and problem debug capabilities.

Encryption

Strong encryption must be used for restricted information in transit and at rest. Other information at rest may need timely or continual availability. Some information is subject to the California Public Records act, and an authoritative copy should be stored in a known location in unencrypted form.

Key management is an important part of any encryption strategy, since the risk exists of information becoming unavailable. An encryption key management plan shall:

- ensure keys are backed up
- specify procedures if keys are compromised or suspected to be compromised
- specify a method to determine if keys have been compromised
- regular review of encryption keys strength
- include user training on cryptographic key best practices

Physical and Environmental Controls

Policies and procedures should be developed for the physical protection of Resources supporting restricted and or essential data. The following guidelines may help:
Risk mitigation measures

Preparation should be made for emergency conditions such as earthquakes, fire, flooding and environmental conditions exceeding limits. Controls should also be in place to protect from theft.

Physical access controls

Controls should be in place limiting and logging physical access to restricted or essential Resources.

Inventories of devices including their movement

Procedure should be in place to track inventory; when it is installed, when it is moved, and when it is decommissioned.

Disposition of equipment

Procedures should ensure complete removal of restricted or sensitive data for final disposition of hardware and electronic media.

Portable devices and media

Procedures should be in place to guide users on the physical security of portable devices and media.