

---

# **Information Technology Security Guidelines**

**Office of Information and  
Instructional Technology**

April 03



**SENSITIVITY NOTICE**

University System of Georgia (USG) - Sensitive

This security report is classified as USG sensitive. It contains sensitive system security information relating to the security services, processes, and operations of the USG enterprise information network. Unrestricted public disclosure of this information would assist unauthorized persons to breach the USG educational network systems and place 'privacy' and other sensitive categories of information at risk.



# Table of Contents

<b>CHAPTER 1: OVERVIEW.....</b>	<b>1-1</b>
DEVELOPING SECURITY POLICIES .....	1-1
<i>Definition of an IT Policy</i> .....	1-1
<i>Types of IT Policies</i> .....	1-2
DEVELOPING A SECURITY PLAN .....	1-2
<i>Purpose</i> .....	1-2
<i>Risk Analysis</i> .....	1-3
USING THIS DOCUMENT .....	1-3
<i>Terms</i> .....	1-4
<i>Document Organization</i> .....	1-4
<b>CHAPTER 2: POLICY DEVELOPMENT, DOCUMENTATION, AND REVIEW .....</b>	<b>2-1</b>
DEVELOPING SECURITY POLICIES .....	2-1
<i>Program Policy</i> .....	2-1
<i>System-Specific Policy</i> .....	2-2
<i>Issue-Specific Policy</i> .....	2-4
<i>Principle</i> .....	2-4
<i>Guidelines</i> .....	2-4
DOCUMENTING SECURITY POLICIES .....	2-5
<i>Principle</i> .....	2-5
<i>Guidelines</i> .....	2-5
IMPLEMENTING SECURITY POLICIES.....	2-6
<i>Principle</i> .....	2-6
<i>Guidelines</i> .....	2-7
REVIEWING AND EVALUATING POLICIES .....	2-7
<i>Principle</i> .....	2-7
<i>Guidelines</i> .....	2-8
<b>CHAPTER 3: ORGANIZATIONAL SECURITY .....</b>	<b>3-1</b>
DEVELOPING AN INFORMATION SECURITY INFRASTRUCTURE.....	3-1
<i>Principle</i> .....	3-1
<i>Guidelines</i> .....	3-2
MANAGING RISKS FROM THIRD-PARTY ACCESS .....	3-4
<i>Principle</i> .....	3-4
<i>Guidelines</i> .....	3-4
CONTRACTING WITH THIRD-PARTY ENTITIES .....	3-5
<i>Principle</i> .....	3-5
<i>Guidelines</i> .....	3-6
DEFINING SECURITY REQUIREMENTS FOR OUTSOURCING CONTRACTS.....	3-7
<i>Principle</i> .....	3-7
<i>Guidelines</i> .....	3-8
<b>CHAPTER 4: ASSET CLASSIFICATION AND CONTROL.....</b>	<b>4-1</b>
CLASSIFYING ASSETS .....	4-1
<i>Principle</i> .....	4-1
<i>Guidelines</i> .....	4-1
DEVELOPING AND MAINTAINING AN ASSET INVENTORY .....	4-2
<i>Principle</i> .....	4-2

<i>Guidelines</i> .....	4-2
ANALYZING AND ASSESSING RISK .....	4-3
<i>Principle</i> .....	4-3
<i>Guidelines</i> .....	4-3
<b>CHAPTER 5: PERSONNEL SECURITY .....</b>	<b>5-1</b>
HIRING NEW PERSONNEL .....	5-1
<i>Principle</i> .....	5-1
<i>Guidelines</i> .....	5-2
ENSURING ACCEPTABLE USE OF TECHNOLOGY .....	5-3
<i>Principle</i> .....	5-3
<i>Guidelines</i> .....	5-4
TRAINING USERS .....	5-5
<i>Principle</i> .....	5-5
<i>Guidelines</i> .....	5-5
REPORTING AND HANDLING SECURITY INCIDENTS .....	5-5
<i>Principle</i> .....	5-6
<i>Guidelines</i> .....	5-6
REPORTING SECURITY WEAKNESSES .....	5-7
<i>Principle</i> .....	5-8
<i>Guidelines</i> .....	5-8
DEVELOPING A DISCIPLINARY PROCESS .....	5-8
<i>Principle</i> .....	5-8
<i>Guidelines</i> .....	5-9
<b>CHAPTER 6: PHYSICAL AND ENVIRONMENTAL SECURITY .....</b>	<b>6-1</b>
SECURING THE PHYSICAL PERIMETER AND FACILITIES .....	6-1
<i>Principle</i> .....	6-1
<i>Guidelines</i> .....	6-1
SECURING PHYSICAL ENTRY TO RESTRICTED AREAS.....	6-2
<i>Principle</i> .....	6-2
<i>Guidelines</i> .....	6-3
SECURING EQUIPMENT SITES .....	6-4
<i>Principle</i> .....	6-4
<i>Guidelines</i> .....	6-4
SECURING POWER SUPPLIES .....	6-5
<i>Principle</i> .....	6-5
<i>Guidelines</i> .....	6-5
SECURING EQUIPMENT RE-USE OR DISPOSAL .....	6-6
<i>Principle</i> .....	6-6
<i>Guidelines</i> .....	6-7
<b>CHAPTER 7: OPERATIONS MANAGEMENT .....</b>	<b>7-1</b>
SECURING OPERATIONAL CHANGE.....	7-1
<i>Principle</i> .....	7-1
<i>Guidelines</i> .....	7-1
DEVELOPING NETWORK CONTROLS .....	7-1
<i>Principle</i> .....	7-2
<i>Guidelines</i> .....	7-2
SEPARATING DEVELOPMENT AND OPERATION FACILITIES .....	7-2
<i>Principle</i> .....	7-2
<i>Guidelines</i> .....	7-2
SECURING EXTERNAL FACILITIES MANAGEMENT .....	7-3
<i>Principle</i> .....	7-3
<i>Guidelines</i> .....	7-3

<b>CHAPTER 8: SYSTEM AND SOFTWARE MANAGEMENT.....</b>	<b>8-1</b>
DEVELOPING INFORMATION AND SOFTWARE EXCHANGE AGREEMENTS.....	8-1
<i>Principle</i> .....	8-1
<i>Guidelines</i> .....	8-1
DEVELOPING ELECTRONIC MAIL SECURITY.....	8-2
<i>Principle</i> .....	8-2
<i>Guidelines</i> .....	8-2
SECURING PUBLICLY AVAILABLE SYSTEMS.....	8-2
<i>Principle</i> .....	8-2
<i>Guidelines</i> .....	8-3
MAINTAINING ADEQUATE SYSTEM CAPACITY.....	8-4
<i>Principle</i> .....	8-4
<i>Guidelines</i> .....	8-5
ENSURING SYSTEM ACCEPTANCE.....	8-5
<i>Principle</i> .....	8-5
<i>Guidelines</i> .....	8-5
PROTECTING AGAINST MALICIOUS SOFTWARE.....	8-6
<i>Principle</i> .....	8-6
<i>Guidelines</i> .....	8-6
<b>CHAPTER 9: INFORMATION MANAGEMENT.....</b>	<b>9-1</b>
HANDLING INFORMATION.....	9-1
<i>Principle</i> .....	9-1
<i>Guidelines</i> .....	9-1
DISPOSING OF MEDIA.....	9-2
<i>Principle</i> .....	9-2
<i>Guidelines</i> .....	9-2
<b>CHAPTER 10: BACK-UP PROCEDURES.....</b>	<b>10-1</b>
DEVELOPING BACK-UP PROCEDURES.....	10-1
<i>Principle</i> .....	10-1
<i>Guidelines</i> .....	10-1
MAINTAINING ACTIVITY LOGS.....	10-2
<i>Principle</i> .....	10-2
<i>Guidelines</i> .....	10-2
MAINTAINING FAULT LOGS.....	10-3
<i>Principle</i> .....	10-3
<i>Guidelines</i> .....	10-3
DEVELOPING DISASTER RECOVERY AND BUSINESS CONTINUITY.....	10-4
<i>Principle</i> .....	10-4
<i>Guidelines</i> .....	10-4
<b>CHAPTER 11: DOCUMENTATION.....</b>	<b>11-1</b>
DOCUMENTING SECURITY POLICIES, PROCEDURES, PLANS, GUIDELINES, AND STANDARDS.....	11-1
<i>Principle</i> .....	11-1
<i>Guidelines</i> .....	11-1
DOCUMENTING OPERATING PROCEDURES.....	11-1
<i>Principle</i> .....	11-1
<i>Guidelines</i> .....	11-2
SECURING OPERATIONS SYSTEM DOCUMENTATION.....	11-2
<i>Principle</i> .....	11-2
<i>Guidelines</i> .....	11-3
<b>CHAPTER 12: ACCESS CONTROL.....</b>	<b>12-1</b>
DEVELOPING AN ACCESS CONTROL POLICY.....	12-1

<i>Principle</i> .....	12-1
<i>Guidelines</i> .....	12-1
MANAGING PASSWORDS .....	12-3
<i>Principle</i> .....	12-3
<i>Guidelines</i> .....	12-4
CONTROLLING ACCESS TO NETWORKS AND SYSTEMS .....	12-5
<i>Principle</i> .....	12-5
<i>Guidelines</i> .....	12-5
CONTROLLING NETWORK CONNECTION TIMES .....	12-8
<i>Principle</i> .....	12-8
<i>Guidelines</i> .....	12-9
MONITORING SYSTEM ACCESS .....	12-9
<i>Principle</i> .....	12-9
<i>Guidelines</i> .....	12-10
MANAGING REMOTE ACCESS .....	12-11
<i>Principle</i> .....	12-11
<i>Guidelines</i> .....	12-12
<b>CHAPTER 13: SYSTEMS DEVELOPMENT AND MAINTENANCE.....</b>	<b>13-1</b>
ADHERING TO EXISTING SECURITY REQUIREMENTS .....	13-1
<i>Principle</i> .....	13-1
<i>Guidelines</i> .....	13-1
IMPLEMENTING CRYPTOGRAPHIC TECHNIQUES.....	13-4
<i>Principle</i> .....	13-4
<i>Guidelines</i> .....	13-5
DEVELOPING CHANGE CONTROL PROCEDURES.....	13-6
<i>Principle</i> .....	13-6
<i>Guidelines</i> .....	13-7
<b>CHAPTER 14: COMPLIANCE.....</b>	<b>14-1</b>
COMPLYING WITH LEGAL REQUIREMENTS .....	14-1
<i>Principle</i> .....	14-1
<i>Guidelines</i> .....	14-1
REVIEWING SECURITY POLICIES AND TECHNICAL COMPLIANCE.....	14-2
<i>Principle</i> .....	14-2
<i>Guidelines</i> .....	14-2
<b>INDEX .....</b>	<b>INDEX-1</b>
<b>APPENDIX A: BOARD OF REGENTS RELATED POLICIES .....</b>	<b>A-1</b>
DEVELOPING GENERAL POLICIES .....	A-1
<i>Computer Security Policy</i> .....	A-1
<i>Home or Off-Campus Use of Equipment for Business Purposes</i> .....	A-2
HANDLING DISRUPTIVE BEHAVIOR .....	A-3
<b>APPENDIX B: ADDITIONAL RESOURCES .....</b>	<b>B-1</b>
<i>Student and Exchange Visitor Information System (SEVIS)</i> .....	B-1
<i>The Digital Millennium Copyright Act (DMCA)</i> .....	B-1
<i>Health Insurance Portability and Accountability Act of 1996 (HIPAA)</i> .....	B-1
<i>USA Patriot Act of 2001</i> .....	B-2
<i>National Strategy for Defending Cyberspace</i> .....	B-2
<b>APPENDIX C: GLOSSARY .....</b>	<b>C-1</b>

# Overview

The Office of Information and Instructional Technology (OIIT) presents the following policies and guidelines for minimum information technology (IT) security. Each institution within the University System of Georgia (USG) is responsible for developing procedures to implement and enforce a security plan that includes these policies as well as any additional policies necessary to maintain the security of IT resources. Security personnel should develop a comprehensive security plan using, at a minimum, the policies and guidelines set forth in this document. The security plan should:

- Reflect the standards and goals of the institution
- Conform to existing government policies and regulations
- Address the problems of global networking and other new technologies

## *Developing Security Policies*

Although this document does not provide actual security policies, we recommend that you use the principles presented here to develop formally documented IT security policies. It is important to address each major security need with a policy. You can then begin developing a security plan to enforce those policies.

---

### Definition of an IT Policy

In IT security the word *policy* has two meanings:

- Senior management's directives to create an information resources security program, establish its goals, and assign responsibilities
- Specific security rules for particular systems or specific managerial decisions, such as establishing an organization's electronic mail (e-mail) privacy policy or fax security policy

---

## Types of IT Policies

IT security policies are typically of one of the following three types:

Policy	Description
<b>Program</b>	Policies used by management to create an organization's security program. These are typically high-level, comprehensive policies that do not require frequent updates.
<b>System-specific</b>	Body of rules and practices used to protect a particular information system. These policies are limited to the specific system(s) and may require updates to addresses changes to the system, functionality, or vulnerabilities.
<b>Issue-specific</b>	Policies that address current issues and concerns of the agency. These policies are typically limited, particular, and change rapidly. They are typically created in response to a specific IT security incident.

**Note:** The types of policies are explained in more detail in **Chapter 2: Policy Documentation, Review, and Evaluation.**

## Developing a Security Plan

The goal of an official security plan is to define the acceptable use of IT resources and outline procedures to prevent or respond to security incidents. The plan should protect the security of USG IT resources without interfering with the responsibility of the institution to provide resources or data to staff, students, or the public.

---

## Purpose

The purpose of a security plan is to protect the integrity of USG IT resources by addressing the following issues:

Issue	Description
<b>Technology</b>	Acquire, configure, and audit computer systems and networks to minimize vulnerabilities.
<b>Personnel</b>	Inform users at all levels of their responsibility to protect campus technology and information.

## Risk Analysis

A risk analysis examines all potential risks to an institution's IT resources and ranks those risks by severity. OIIT recommends that each USG institution conduct a risk analysis of its IT resources and use the results to guide the development of the security plan. The main goal of a risk analysis is to identify the following elements:

Element	Definition
<b>Assets</b>	Identify all assets of the institution's IT resources and rank them by sensitivity. The basic security goal for each asset is availability, confidentiality, and integrity.
<b>Risks</b>	Identify the corresponding risks to each asset and rank each risk by its severity.

## Using This Document

OIIT has identified a set of IT security principles that are defined in this document. You can use these principles as a guide in the development of institutional IT security policies and the procedures to implement and enforce the security policies. The principles presented here are based on thirteen major security topics, or areas of concern. Each principle has corresponding guidelines for developing procedures for that principle.

Effective procedures will encompass the needs of individual systems and may require more than the principles and guidelines in this document. Individual facilities may need to develop additional policies and procedures based on the specific needs and sensitivity of their systems. Refer to the following appendices for more information:

Appendix	Subject	Content
<b>A</b>	Board of Regents related policies	Lists the Board of Regents policies that are relevant to USG IT security.
<b>B</b>	Additional Resources	Lists of additional IT security resources and legal requirements.
<b>C</b>	Glossary	Defines terms used in this document.

---

## Terms

This document uses the following terminology:

Term	Definition
<b>Principle</b>	A statement that addresses a major issue or concern in campus IT security. The principles can be used to develop campus policies.
<b>Procedure</b>	A course of action or series of steps to implement and enforce policies.
<b>Guidelines</b>	An indication of the scope and direction of policies and procedures.

---

## Document Organization

The IT security principles identified in this document are divided into thirteen categories. Each category is defined in the table below:

Category	Description
<b>Policy Development, Documentation, and Review</b>	Contains guidelines for developing and documenting security policies and procedures, reviewing and evaluating those policies, and securing resources to put policies into practice.
<b>Organizational security</b>	Contains guidelines to secure the information infrastructure and provides guidelines for defining security requirements for third-party and outsourcing contracts.
<b>Asset classification and control</b>	Contains guidelines for creating accountability for assets and classifying data.
<b>Personnel security</b>	Contains guidelines for personnel security, such as screening new personnel, training users, creating procedures for users to report security incidences and weaknesses, and creating disciplinary processes.
<b>Physical and environmental security</b>	Contains guidelines for securing the physical locations of sensitive computer equipments.
<b>Operation management</b>	Contains guidelines for securing operation facilities.
<b>System and software management</b>	Contains guidelines for securing software, e-mail systems, and publicly available systems such as the Internet. Also includes guidelines for protecting against malicious software.

Category	Description
<b>Information management</b>	Contains guidelines for the secure handling of electronically stored information and proper disposal of media.
<b>Back-up procedures</b>	Contains guidelines for developing back-up procedures in case of system failure or disaster, maintaining activity and fault logs, and developing disaster recovery and business continuity procedures.
<b>Documentation</b>	Contains guidelines for documenting operating procedures and system security.
<b>Access control</b>	Contains guidelines for controlling access to sensitive systems and system information. Includes guidelines for password management, monitoring system access, and managing remote access.
<b>System development and maintenance</b>	Contains guidelines for adhering to existing security requirements during the development of new systems or upgrades.
<b>Compliance</b>	Contains guidelines to ensure campus policies and procedures are compliant with state and federal information requirements.



## Policy Development, Documentation, and Review

This section contains guidelines for the following policies:

- **Developing security policies**
- **Documenting security policies**
- **Implementing security policies**
- **Reviewing and evaluating security policies**

### *Developing Security Policies*

IT security policies are the rules and practices an institution uses to manage and protect its information resources. Typically, these rules and practices are classified as follows:

- Program policies
- System-specific policies
- Issue-specific policies

---

### **Program Policy**

Program policies address overall IT security goals and typically apply to all IT resources within an institution. The institution president or an appointed representative should direct policy development to ensure the policies address the IT security goals for all systems operating within the institution. For instance, program policies can address confidentiality, system integrity, and service availability. All program policies should meet the following criteria:

- Comply with existing laws, regulations, and state and federal policies
- Support and enforce the institution's mission statement and organizational structure

The components of an adequate program policy are defined in the following table:

Component	Description
<b>Purpose Statement</b>	Explains why the program is being established and what IT security goals it will address.
<b>Scope</b>	Defines which IT resources are addressed by the program, such as hardware, software, data, personnel, facilities, and peripheral equipment.
<b>Assignment of responsibilities</b>	Defines responsibility for IT security program management. Also defines supporting responsibilities for executives, line managers, owners, custodians, and users.
<b>Compliance</b>	Describes how the campus will develop and enforce the program. Also establishes any disciplinary process for breaches of the program policy.

---

## System-Specific Policy

System-specific policies address the IT security issues and goals of a particular system. Large facilities may have multiple sets of system-specific policies that address all levels of security from the very general (access control rules) to the particular (system permissions that reflect the segregation of duties among a group of employees).

We recommend the following two-step process to analyze existing policies and develop new policies when necessary:

Step	Subject	Description
1	Security objectives	<p>Define security objectives based on IT security goals and system requirements. Each objective should be an achievable action statement.</p> <p>Example: Ensure ninety-nine percent or better of network availability during the fiscal year.</p> <p>Example: Reduce the incidents of unauthorized access to fewer than three per year.</p>
2	Rules to achieve security objectives	<p>Document rules to achieve each security objective. Rules should be as specific and formal as necessary to enforce the objective. Some rules can be implemented by setting automated system controls however; they should be supplemented with written statements.</p>

---

## Issue-Specific Policy

Issue-specific policies address particular IT security issues such as, Internet access, installation of unauthorized software or equipment, and sending/receiving e-mail attachments. Once you have identified the IT security issues you need to address, develop issue-specific policies using the components defined in the table below:

Component	Description
<b>Issue statement</b>	Identify the terms, definitions, and conditions pertinent to the issue. For instance, how do you define unauthorized software or acceptable Internet use? Include the rationale or justification for the policy.
<b>Statement of the institution's position</b>	Reflects management's decision on the policy. Example: The use of unauthorized software is prohibited.
<b>Applicability</b>	Specifies where, how, when, to whom, and to what the policy applies.
<b>Compliance</b>	Defines who is responsible for enforcing the policy.
<b>Points of contact</b>	Identifies resources for information and guidance.

---

## Principle

Each USG institution should develop policies that are appropriate to its organization and mission.

---

## Guidelines

Guidelines for developing security policies are:

Guideline	Description
<b>Obtain support</b>	Obtain a commitment from senior management to enforce security policies.
	Establish working relationships between departments, such as human resources, internal audit, facilities management, and budget and policy analysis.
	Establish an approval process to include legal and regulatory specialists, human resources specialists, and policy and procedure experts. Allow enough time for the review and respond to all comments whether you accept them or not.

Guideline	Description
<b>Conduct research</b>	Communicate with other institution security groups to share successful practices, experiences, and ideas. <b>Note:</b> Don't work in isolation.
<b>Establish maintenance procedures</b>	Schedule an annual review of security policies to determine if current rules and practices are adequate.
	Anticipate the need for updates due to changes in technology, planned acquisitions, and similar event. This particularly applies to system-specific and issue-specific policies.

## Documenting Security Policies

Once an institution has developed its IT security policies, all policies and procedures should be documented. Separate policy and procedure documents can be developed for different systems and audiences as needed.

---

### Principle

Each USG institution should protect its networks, critical information systems, and sensitive information from unauthorized disclosure, modification, or destruction. Information security policies and procedures must be documented to ensure the integrity; confidentiality, accountability, and availability of information are not compromised.

---

### Guidelines

The security policy document should define the following:

Guideline	Description
<b>Define policies</b>	Define policies by documenting the following information: <ul style="list-style-type: none"> <li>• Identify general areas of risk</li> <li>• State generally how to address the risk</li> <li>• Provide a basis for verifying compliance through audits</li> <li>• Outline implementation and enforcement plans</li> <li>• Balance protection with productivity</li> </ul>

Guideline	Description
<b>Define standards</b>	Define IT security standards by documenting the following information: <ul style="list-style-type: none"> <li>• Define minimum requirements designed to address certain risks</li> <li>• Define specific requirements that ensure compliance with policies</li> <li>• Provide a basis for verifying compliance through audits</li> <li>• Outline implementation and enforcements plans</li> <li>• Balance protection with productivity</li> </ul>
<b>Define guidelines</b>	Define IT security guidelines by documenting the following information: <ul style="list-style-type: none"> <li>• Identify best practices to facilitate compliance</li> <li>• Provide additional background or other relevant information</li> </ul>
<b>Define enforcement</b>	Define how policies will be enforced by documenting the following information: <ul style="list-style-type: none"> <li>• Identify personnel who are authorized to review and investigate breaches of policy</li> <li>• Identify the means to enforce policies</li> </ul>
<b>Define exceptions</b>	Define the possible exceptions to the IT security policies.

## Implementing Security Policies

Successful implementation of IT security policies requires security awareness at all levels of the organization. You can create awareness through widely disseminated documentation, e-mail or other notifications about security issues, a web site, newsletters, and training programs.

---

### Principle

Each USG institution is responsible for developing and implementing policies that are appropriate to its organization and mission.

---

## Guidelines

The guidelines for implementing IT security policies are:

Guideline	Description
<b>Create awareness</b>	Create user awareness using the following methods: <ul style="list-style-type: none"> <li>• Notify employees about the new security polices</li> <li>• Update employees on the progress of new security policies</li> <li>• Publish policy documentation electronically and on paper</li> <li>• Develop descriptive security documentation for users</li> <li>• Develop user training sessions</li> <li>• Require new users to sign a security acknowledgement</li> </ul>
<b>Maintain awareness</b>	Maintain user awareness of ongoing and new security issues using the following methods: <ul style="list-style-type: none"> <li>• Web site</li> <li>• Posters</li> <li>• Newsletters</li> <li>• E-mail for comments, questions, and suggestions</li> </ul>

## Reviewing and Evaluating Policies

Official policies and procedures should undergo two types of review:

- **Initial review by OIIT:** The initial policy document should be reviewed by the OIIT security team as stated in the Board of Regents policy, section 712.
- **Routine reviews within the institution:** Institutions should review their security policies periodically to ensure they continue to fulfill the institutions security needs.

---

## Principle

Each USG institution should ensure that their IT security policies are submitted to OIIT for review. Each institution is also responsible for reviewing and evaluating the effectiveness of their policies and the accompanying procedures.

## Guidelines

This section explains the guidelines for reviewing and evaluating IT security policies.

### ***Initial Review by OIIT***

After an institution has developed IT security policies the OIIT security team will evaluate the policies and provide feedback.

How do you want them to submit this information?

### ***Policy Review within the Institution***

Each institution should develop a plan to review and evaluate their IT security policies once they are in place. The guidelines are:

- Assign responsibility for reviewing policies and procedures
- Implement a reporting plan in which campus agencies report security incidents to designated security personnel
- Implement regular reviews to evaluate the following:
  - Nature, number, and impact of recorded security incidents
  - Cost and impact of controls on business efficiency, including third-party vendor compliance
  - Effects of changes to organizations or technology

## Organizational Security

This section contains guidelines for the following policies:

- **Developing an information security infrastructure**
- **Identifying risks from third-party access**
- **Defining security requirements for third-party access**
- **Defining security requirements for outsourcing contracts**

### *Developing an Information Security Infrastructure*

An information security infrastructure protects an institution's information assets by defining assets and the necessary resources to protect them, and assigning responsibility for assets.

---

#### **Principle**

Each USG institution that develops, uses, or maintains information systems will also develop and maintain an internal information security infrastructure. This infrastructure must consist of information security organizations and programs that ensure the confidentiality, availability, accountability, and integrity of information assets.

## Guidelines

The guidelines for security the information infrastructure are:

Guideline	Description
<b>General</b>	Create an information security organization to take responsibility for all IT security issues as described by ISO 17799.
<b>Manage information security</b>	<p>Outline clear responsibilities and define organizational roles for information security. These responsibilities and roles should include:</p> <ul style="list-style-type: none"> <li>• Forming, reviewing, and approving campus information security</li> <li>• Maintaining threat assessments for internal information</li> <li>• Overseeing investigations of security-related incidents</li> <li>• Overseeing business issues regarding new security initiatives</li> </ul>
	Appoint, designate, or hire an information security officer for the campus and individual departments with particularly sensitive IT security issues. Depending on the size of the campus and its departments, these roles may require full-time positions.
<b>Coordinate information security</b>	Establish an information security officer to interface with law enforcement or any legal personnel.
	<p>Establish a security counsel to manage security incidents. The counsel should include representatives from the following groups:</p> <ul style="list-style-type: none"> <li>• Facilities</li> <li>• Human resources</li> <li>• Safety office</li> <li>• Upper management</li> </ul>

Guideline	Description
<b>Coordinate information security, cont</b>	<p>Determine if the campus requires multiple sub-groups to maintain information security functions for specific departments. Policies and procedures for a multi-level security organization should:</p> <ul style="list-style-type: none"> <li>• Define the roles and responsibilities of each group</li> <li>• Establish methods, procedures, processes, risk assessment, and information classification guidelines.</li> <li>• Provide information security user education and interface</li> <li>• Provide security-related technical architecture to plan and develop groups</li> <li>• Designate security incident investigation responsibility</li> <li>• Provide identification of an architectural interface to the business management groups</li> </ul>
<b>Allocate responsibilities</b>	<p>Clarify responsibilities for security-related issues. For each area of security responsibility address the following issues:</p> <ul style="list-style-type: none"> <li>• Document access procedures for each individual information system</li> <li>• Define the owner of each security asset and the access procedures to that asset</li> <li>• Define authorization levels for access to assets</li> </ul>
<b>Authorize information processing facilities</b>	<p>Define the responsibilities of the managers of information processing facilities regardless of the size or complexity of the institution. When approving new information process facilities address the following issues:</p> <ul style="list-style-type: none"> <li>• Assess the ability of the new institution to conform to existing security policies, including any state and federal requirements</li> <li>• Evaluate hardware and software compatibility of the new facilities with existing facilities</li> <li>• Evaluate the need for additional security measures and the impact of personal computing systems</li> </ul>
<b>Assess third-parties</b>	<p>Use internal (or external, if necessary) information security specialists to guide the information security infrastructure to maintain awareness of new security-related threats and other issues.</p> <p><b>Note:</b> In cases of security-related investigations, external resources may be required.</p>

Guideline	Description
<b>Cooperate with other organizations</b>	Maintain contact lists of both internal and external organizations and service vendors.
	Define the managers authorized to make decisions regarding security-related events.
	Encourage membership in security-related organizations, which can provide valuable insight in security administration. <b>Note:</b> Members of security-related organizations should not release information about an institute’s security events and issues unless approved by the appropriate business management and security personnel.

## Managing Risks from Third-Party Access

Any institution that allows third-party access to its IT resources should analyze the risks and develop security procedures to control access. The most significant risk in third-party access to USG IT resources is network-to-network connections that allow multiple users or systems from the third-party to interact with USG systems.

---

### Principle

Each USG institution that allows third-party access to its information systems should conduct risk assessments and identify risks as defined by the access control policies before access is granted.

---

### Guidelines

The guidelines for managing the risks of third-party access are:

Guideline	Description
<b>Create security awareness</b>	Each campus must identify and manage the risks before allowing third-party access.
	Provide the third-party with a copy of the campus security policy have them agree to comply. <b>Note:</b> Additionally, campuses may use a security firm to investigate the third-party systems and determine if the present unreasonable risk to institution resources.

Guideline	Description
<b>Control access</b>	Create a user profile for each third-party user that includes the following, minimum criteria: <ul style="list-style-type: none"> <li>• Time of day access</li> <li>• Day of week access</li> <li>• Physical location access</li> <li>• Networked location access</li> <li>• Direct dial in access</li> <li>• User directory permissions</li> <li>• User application access</li> </ul>
	Implement extra safeguards if a third-party user has access to institutional information.
<b>Control on-site access</b>	Educate on-site, third-party users about institutional policies and procedures and have them agree to comply.
	Monitor network connection ports for unknown devices and unauthorized connections.
	Train state employees who work in the same area as a third-party user to be vigilant about logging off sessions, logging out or securing computer access, and keeping paper information discreet.
<b>Control remote access</b>	Implement tight controls on user accounts using remote logical access.
	Monitor remote connections for abnormal activity.

## Contracting with Third-Party Entities

Facilities should develop procedures to ensure third-parties comply with all IT security policies. Ideally, third-parties will sign a contract that clarifies the security responsibilities of third-party users.

---

### Principle

Each USG institution that allows third-party access to its information resources should address the security issues of that access and require the third-party to adhere to all established security policies.

**Guidelines**

Each campus is responsible for addressing all relevant security issues when contracting with third-parties. The guidelines for contracting with third-parties are:

Guideline	Description
<b>Control access</b>	On-site access contracts should address the following: <ul style="list-style-type: none"> <li>• Third-party responsibility for the actions of its members</li> <li>• Third-party responsibility to determine the skills and character of on-site personnel</li> </ul>
	Remote access contracts should address the following: <ul style="list-style-type: none"> <li>• Third-party responsibility for the actions of its members</li> <li>• Third-party responsibility for the security of connected networks, systems, and logins</li> <li>• Third-party responsibility to demonstrate ability to meet or exceed normal institution information security policies</li> </ul>
	Provisions for granting authorized user access.
	Method for managing authorized user lists and access rights across systems.
	<b>Protect assets</b>
Procedures to determine if any compromise of assets has occurred.	
Verifiable procedures for the destruction or return of institutional information assets at the end of the provided service.	
Procedure to verify system integrity and availability.	
Specific restrictions on copying or disclosing institutional information.	
<b>Manage services</b>	Detailed descriptions of each service offered by the third-party.
	Service-level criteria for acceptable and non-acceptable performance.
	Process for escalating service issues, problem resolution, and contingency plans.

Guideline	Description
<b>Manage liabilities</b>	Statement of liabilities for the institution and the third-party.
	Delegated responsibilities in legal issues involving third-parties.
	Provisions for distribution of intellectual property rights and collaborative work.
<b>Ensure compliance</b>	Performance criteria with monitors and verifiable definitions.
	Provisions to manage user access and monitor user activity.
	Provisions to monitor contractual compliance.
	Statement of the institution’s right to use third-parties to establish contractual compliance.
	Procedure for reporting and investigating security related issues.
<b>Secure equipment</b>	Third-party responsibilities regarding hardware and software installation and maintenance.
	Plan for control of malicious software.
<b>Manage personnel</b>	Provision for transfer of staff as required.
	Reporting structure and specific reporting formats and expected content.
	Plan for change management procedures.
	Process for educating users and administrators about methods, procedures, and security.

## Defining Security Requirements for Outsourcing Contracts

Outsourcing agreements should address all IT security issues identified for the particular resources included in the contract.

---

### Principle

Each USG institution that enters outsourcing agreements should develop security provisions specifically tailored to the particular outsourcing initiative.

## **Guidelines**

Outsourcing contracts should include the guidelines outlined in **Contracting with Third-Party Entities** in this document.

CHAPTER  
**4**

# Asset Classification and Control

This section contains guidelines for the following policies:

- **Classifying assets**
- **Developing and maintaining an asset inventory**
- **Analyzing and assessing risk**

## *Classifying Assets*

Once you have developed an IT security plan it is important to classify the information assets to determine which information systems, data, facilities, equipment, and personnel constitute the critical information infrastructure of the institution.

---

### Principle

Each USG institution should classify its assets to determine which assets constitute the critical information infrastructure of the institution.

---

### Guidelines

The guidelines for classifying IT assets are:

Guideline	Description
<b>Organize assets</b>	Organize assets into basic categories, such as: <ul style="list-style-type: none"> <li>• Data</li> <li>• Equipment</li> <li>• Hardware/software</li> <li>• Personnel</li> <li>• Facilities</li> <li>• Operations</li> </ul>
<b>Review relevant information</b>	Review reports, databases, and documents with information about personnel, information and equipment.
<b>Interview personnel</b>	Interview personnel, such as managers, customers, suppliers, users, and others to as necessary to help determine critical assets.

Guideline	Description
<b>Conduct surveys</b>	Develop survey questions to identify critical assets, such as: <ul style="list-style-type: none"><li>• What are the mission critical or sensitive activities and/or operations?</li><li>• Where is critical or sensitive information stored or processed?</li><li>• Where are the mission critical or high value equipment or material located (onsite or off)?</li><li>• What kind of physical security, access control, and other protective measures are in place in these locations?</li><li>• What impact would a lost or damaged asset have on critical mission functions, operations, and customers?</li></ul>
<b>Identify interdependencies</b>	Identify interdependencies among the components of individual systems and the overall infrastructure.
<b>Classify assets</b>	Classify assets based on your findings. Typically, the more goals an asset supports the more important it is.

## *Developing and Maintaining an Asset Inventory*

An important component of IT security is establishing accountability for all IT resources. A documented asset inventory helps identify and assign responsibility for all resources.

---

### Principle

Each USG institution that operates hardware and software resources should maintain a documented inventory of those resources in compliance with all applicable asset management policies, including the following article from the Official Code of Georgia, annotated: Article 6 of **Chapter 9: Georgia Computer Systems Protection Act**, Title 16.

---

### Guidelines

Asset inventories allow each campus and its separate departments to account for all hardware and software purchased with public funds. As items become out of date or no longer in use they should be removed from the inventory lists in accordance with institutional asset management procedures.

## Analyzing and Assessing Risk

Once you have identified the critical IT assets a risk analysis and assessment can help you identify the vulnerabilities and risks associated with those assets.

---

### Principle

Each USG institution should identify and document the vulnerabilities and risks associated with its critical assets.

---

### Guidelines

This section provides guidelines for analyzing and assessing risk to critical assets.

#### **Risk Analysis**

A risk analysis is used to analyze the risk to critical IT assets by finding and documenting the vulnerabilities. A thorough analysis requires the assistance of experts in the hardware and software used at the institution. A risk analysis should analyze areas of control, critical asset elements, and areas of potential compromise. The guidelines for analyzing risk to critical IT assets are:

Guideline	Category	Description
<b>Define areas of control</b>	General	Define the policies, procedures, practices, and organizational structures designed to ensure business objectives are achieved and undesired events are detected and prevented.

Guideline	Category	Description
<p><b>Define areas of control, cont.</b></p>	<p>Institution-wide security</p>	<p>Define a security framework and continuing cycle of activity to achieve the following:</p> <ul style="list-style-type: none"> <li>• Manage risk</li> <li>• Develop security policies</li> <li>• Assign responsibilities</li> <li>• Evaluate physical and information controls</li> </ul>
		<p>Develop program policies to achieve institution-wide security by accomplishing the following:</p> <ul style="list-style-type: none"> <li>• Assess risk</li> <li>• Develop and implement effective security procedures</li> <li>• Evaluate the effectiveness of procedures</li> </ul>
	<p>Access controls</p>	<p>Define procedures and controls that limit or detect access to critical IT assets. Access controls include the following:</p> <ul style="list-style-type: none"> <li>• Physical controls – limit physical access to critical equipment</li> <li>• Technical controls – security measures, such as security software programs, designed to detect and prevent unauthorized access to critical IT assets</li> </ul>
	<p>Segregation of duties</p>	<p>Develop policies, procedures, and a segregated organizational structure to ensure no single individual controls all key aspects of IT operations.</p>
	<p>Continuity of service</p>	<p>Develop a comprehensive contingency plan to ensure the following:</p> <ul style="list-style-type: none"> <li>• Availability of critical services and operations.</li> <li>• Protection of sensitive data</li> </ul>
	<p>Change control and life cycle management</p>	<p>Develop policies and controls to prevent users from implementing unauthorized programs or modifying existing programs.</p>
		<p>Develop policies and controls to ensure that authorized changes will not interrupt critical services and operations.</p>

Guideline	Category	Description
<b>Define areas of control, cont.</b>	System software controls	<p>Develop policies and controls to limit and monitor access to the programs and sensitive files that control computer hardware and secure applications. A thorough risk analysis requires assessing the following:</p> <ul style="list-style-type: none"> <li>• System software access control</li> <li>• Monitor procedures</li> <li>• Change control procedures</li> </ul>
<b>Identify critical asset elements</b>	Personnel	Identify the staff, management, and executive personnel necessary to plan, organize, acquire, deliver, support, and monitor critical IT assets. Also include any pertinent off-site groups or individuals.
	Automated information and control systems	Identify the electronic and telecommunication equipment, hardware, and software safeguards that support critical IT assets.
	Non-automated information and control systems	<p>Identify the non-automated systems, internal and external, that support critical IT assets, such as:</p> <ul style="list-style-type: none"> <li>• Paper archives</li> <li>• Personnel</li> <li>• Accounting procedures</li> </ul>
	Data	<p>Identify all data, in electronic and printed form, that support critical assets. These include numbers, characters, images, and any other means or sorting information that can be:</p> <ul style="list-style-type: none"> <li>• Assessed by personnel</li> <li>• Stored in or processed by a computer</li> <li>• Transmitted digitally</li> </ul>
	Facilities and equipment	Identify the facilities and equipment that support and house critical IT assets.
<b>Define areas of potential compromise</b>	NA	Review actions, devices, policies, procedures, techniques, and other factors that pose a potential risk to critical IT assets.
		Compile a list of threats and vulnerabilities that can affect the confidentiality, integrity, availability, and accountability or resources essential to critical IT assets.

**Note:** A risk requires both a threat and a vulnerability (threat + vulnerability = security risk).

### **Risk Assessment**

Once you have identified the risks and vulnerabilities through a risk analysis, a risk assessment will help you determine which critical IT assets are most sensitive and at greatest risk. The cost of security enhancements typically exceeds available resources and the objective is to minimize the known vulnerabilities associated with the most critical IT assets. A risk assessment will help you prioritize IT security needs.

A thorough risk assessment should include the following questions:

- Can a vulnerability be better minimized with physical or IT measures?
- How much would it cost to minimize the risk posed by the vulnerability?
- Are the security enhancement costs commensurate with the asset's overall importance?
- What is the countermeasure's function: deter, detect, delay, or destroy?
- Is the effectiveness of the countermeasure related to time or events?
- Is the countermeasure effective institution-wide or for a specific area only?
- Do projected plans or anticipated developments suggest that the vulnerability is likely to become irrelevant in the near future?
- How long will it take to fully implement the proposed security enhancement?
- Will a proposed security enhancement be defeated by IT advances in the near future?

**Note:** Remember that every countermeasure has its own vulnerability.

## Personnel Security

This section contains guidelines for the following policies:

- **Hiring new personnel**
- **Ensuring appropriate use of technology**
- **Training users**
- **Reporting security incidents**
- **Reporting security weaknesses**
- **Developing a disciplinary process**

### *Hiring New Personnel*

When hiring new personnel, IT departments should 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.

---

#### **Principle**

Each USG institution should screen, educate, and train prospective employees who will be granted access to USG information systems.

## Guidelines

The guidelines for screening personnel are:

Guideline	Description
<p><b>Screen potential employees</b></p>	<p>Conduct verification and background checks as part of the initial employment/engagement process for full and part-time employees. Checks should include the following, as applicable:</p> <ul style="list-style-type: none"> <li>• Character references (business and personal)</li> <li>• Training background</li> <li>• Academic and professional experience</li> <li>• Identity and background checks</li> <li>• Credit checks</li> </ul>
	<p>Conduct a re-screening if there is cause for doubt or concern.</p>
	<p>Repeat these checks in cases of job change, role change, and promotion.</p>
<p><b>Outline employee responsibilities</b></p>	<p>Identify the degree of access to institution information systems, processes, and data in job descriptions.</p>
	<p>Define the following for new employees:</p> <ul style="list-style-type: none"> <li>• Official Code of Georgia Annotated Computer Security Act</li> <li>• Applicable state and federal regulations</li> <li>• Terms of confidentiality</li> <li>• Security conditions of employment</li> <li>• Normal administrative processes</li> </ul>
	<p>Define the security issues that are part of the terms and conditions of employment.</p>
	<p>Implement annual security training for all employees that includes:</p> <ul style="list-style-type: none"> <li>• Security awareness</li> <li>• Security policies and procedures updates</li> <li>• Reporting procedures for security incidents and vulnerabilities</li> </ul>
	<p>Create confidentiality and non-disclosure agreements to be signed by new employees who will be accessing sensitive information.</p>
	<p>Educate all employees of the disciplinary action or criminal charges that may result if security policies are violated.</p>

Guideline	Description
<b>Evaluate the duties of new employees</b>	Implement procedures for managers and supervisors to evaluate the duties of inexperienced personnel who access sensitive information. These procedures should be reviewed and updated as necessary.

## *Ensuring Acceptable Use of Technology*

USG facilities provide IT resources to authorized users to facilitate the efficient and effective performance to their duties. Authorization imposes certain responsibilities and obligations on users and is subject to state government policies and applicable state and federal laws. Users at all levels should be trained in the appropriate use of IT resources.

---

### **Principle**

Each USG institution should ensure the appropriate use of its IT resources by users at all levels.

## Guidelines

The guidelines for ensuring appropriate use of IT resources are:

Guideline	Description
<p><b>Identify inappropriate use</b></p>	<p>Identify inappropriate use of IT resources. Inappropriate use includes, but is not limited to, the following:</p> <ul style="list-style-type: none"> <li>• Private or personal for-profit activities, such as personal business transactions or advertising</li> <li>• Unauthorized, not-for-profit business activities</li> <li>• Illegal activities as defined by federal, state, and local laws and regulations</li> <li>• Creation, accession, or transmission of pornographic or obscene material</li> <li>• Creation, accession, or transmission of material that could be considered discriminatory, offensive, threatening, harassing, or intimidating</li> <li>• Creation, accession, or participation in online gambling</li> <li>• Infringement of any copyright, trademark, patent, or other intellectual property rights</li> <li>• Activity that could cause the loss, corruption of, or prevention of rightful access to data or the degradation of IT performance</li> <li>• Activity or solicitation for political or religious causes</li> <li>• Unauthorized use of another employee's access</li> <li>• Modifying or removing computer equipment, software, or peripherals without proper authorization</li> <li>• Creation, accession, or transmission of material to libel or otherwise defame any person</li> </ul>
<p><b>Develop appropriate use policies</b></p>	<p>Define appropriate use of all institutional systems and equipment.</p> <hr/> <p>Implement policies in the following ways:</p> <ul style="list-style-type: none"> <li>• Restrict access to unauthorized users</li> <li>• Train users in appropriate use</li> </ul>
<p><b>Enforce policies</b></p>	<p>Develop procedures to pursue disciplinary action, termination, or criminal prosecution in cases of violation.</p>

## Training Users

Users of IT resources should be aware of potential security concerns and understand their responsibility to report security incidents or vulnerabilities.

---

### Principle

Each USG institution should provide security training to its employees, faculty, and students. Training should be developed with input from human resources and the legal department. Completed training should be documented.

---

### Guidelines

The guidelines for training users are:

Guideline	Description
<b>Establish information access</b>	Establish information access rules and regulations with input from human resources and the legal department.
	Train all users about accessing and using communication systems. Training should teach users about: <ul style="list-style-type: none"> <li>• Acceptable and unacceptable access</li> <li>• Access controls and legal responsibilities</li> <li>• Vigilance of fraudulent activities</li> <li>• Procedures to report security incidents or vulnerabilities</li> </ul>
<b>Establish acceptable use of software</b>	Train all users on the acceptable use of software used for communication with other systems and personnel.
	Create a login process for all applications with secure password protection.
<b>Establish acceptable use of systems</b>	Train all users on the acceptable use of new systems.

## Reporting and Handling Security Incidents

Users of IT resources should have established and clear steps for reporting and handling security incidents.

---

## Principle

Each USG institution should implement procedures for reporting and handling security incidents. All users should be trained to report incidents in accordance with policy.

---

## Guidelines

Each campus should designate a specific administrator to oversee information security. Larger campuses may require more than one, or departmental, security administrators. The administrator(s) should develop and document policies and procedures for reporting and managing incidents that include the following:

Guideline	Description
<b>Report incidents</b>	Develop a process for users to report breaches of security and other incidents to the appropriate personnel. The report should include the following: <ul style="list-style-type: none"> <li>• Incident type</li> <li>• Severity level</li> <li>• Access details</li> <li>• Involvement</li> </ul>
	Develop user training to address the following: <ul style="list-style-type: none"> <li>• Incident reporting process</li> <li>• Awareness of historical incidents in order to avoid future occurrences</li> </ul>
	Provide users who have reported an incident with a receipt or other acknowledgement. The user should also receive updates throughout the investigation.
	Provide confidentiality, and protection if necessary, to users who report a breach of security.
	Develop a feedback process to inform users who report a breach of security when the incident is closed.

Guideline	Description
<b>Manage incidents</b>	Develop a method of logging and tracking the needs to be addressed for specific types of incidents.
	Develop escalation procedures to quickly inform appropriate personnel, such as: <ul style="list-style-type: none"> <li>• System administrators</li> <li>• Management</li> <li>• All parties responsible for security</li> </ul>
	Develop escalation procedures that include multiple escalation points, depending on the severity of the incident, so that evidence can be collected and the damage or restoration can be completed as quickly as possible.
	Develop procedures to report incidents to outside agencies, such a regulatory bodies and law enforcement, if necessary.
<b>Collecting and sharing information</b>	Develop a method of incident data collection to track all incidents. For instance, all data could be kept in an historical database. Information collected should include: <ul style="list-style-type: none"> <li>• Type of incident</li> <li>• Severity level</li> <li>• Cost of incident</li> <li>• Scope of incident</li> <li>• Resolution</li> </ul>
	Develop a method of analyzing the collected information to identify vulnerabilities.
	Develop procedures to regularly analyze incident logs.
	Develop a method for sharing information across campus departments for training and policy development.

## Reporting Security Weaknesses

Users of IT resources should have established and clear steps for reporting and handling security weaknesses.

---

## Principle

Each USG institution should develop procedures for users to report vulnerabilities in, or threats to, the security information and communication systems.

---

## Guidelines

Guidelines for reporting security weaknesses are:

Guideline	Description
<b>Develop user awareness</b>	Instill a sense of urgency in users to report security vulnerabilities and potential threats to the designated security administrator.
<b>Define user responsibilities</b>	Train all users of their responsibility to remain vigilant for vulnerabilities and potential threats.
	Train all users to report weaknesses using the appropriate reporting procedures.
	Train all users to report potential weaknesses immediately. Users should <i>not</i> attempt to test a weakness before reporting it.

## Developing a Disciplinary Process

A disciplinary process ensures correct and fair treatment of users who breach security and may also deter users from disregarding security procedures.

---

## Principle

Each USG institution should implement disciplinary procedures for users who breach security.

**Guidelines**

Guidelines for developing disciplinary policies are:

Guideline	Description
<b>Develop a disciplinary process</b>	Develop specific disciplinary actions for the following: <ul style="list-style-type: none"><li>• State employees</li><li>• Contractors</li><li>• Vendors</li></ul>
	Develop policies that ensure correct and fair treatment of users suspected of committing security breaches.
	Develop a procedure to involve local law enforcement if necessary.
	Follow the disciplinary process consistently to deter future breaches.
<b>Develop a disciplinary process for third-parties</b>	Inform all third-party personnel of their responsibility to follow security policies and procedures and make them aware of the consequences of security breaches.
	Develop third-party agreements to include written confirmation that the third-party will comply with institutional policies and procedures and discipline their employees who disregard the institute's security procedures.



## Physical and Environmental Security

This section contains guidelines for the following policies:

- **Securing the physical perimeter**
- **Securing physical entry to restricted areas**
- **Securing equipment sites**
- **Securing power supplies**
- **Securing equipment re-use or disposal**

### *Securing the Physical Perimeter and Facilities*

An important component of IT security is the integrity of the physical perimeter and facilities that contain IT resources.

---

#### Principle

Each USG institution should implement procedures and physical security measures to prevent and detect unauthorized access or damage to facilities that contain USG information systems.

---

#### Guidelines

The guidelines for securing the physical perimeter and facilities are described in the following table:

Guideline	Description
<b>Secure information processing equipment</b>	Ensure that the location of information processing facilities is confidential. Important safeguards are: <ul style="list-style-type: none"> <li>• No signs indicating locations</li> <li>• No public access to directories and telephone books that identify locations</li> </ul>
	Place all printers, copiers, and fax machines in secured areas to prevent unauthorized duplication and transmission of sensitive information.

Guideline	Description
<p><b>Secure the perimeter and facilities</b></p>	<p>Identify the perimeter of all information processing facilities and perform a risk analysis of its physical security.</p>
	<p>Ensure that information processing facilities meet local building codes for structural stability, such as:</p> <ul style="list-style-type: none"> <li>• External walls</li> <li>• Internal walls</li> <li>• Ceilings</li> <li>• Doors</li> </ul>
	<p>Ensure that walls surrounding sensitive areas extend from true floor to true ceiling.</p>
	<p>Secure doors by ensuring the following:</p> <ul style="list-style-type: none"> <li>• Doors to sensitive areas should close automatically and trigger an audible alarm when they have been kept open beyond a certain period of time</li> <li>• Fire doors in sensitive areas should trigger an audible alarm when the crash bar is used</li> </ul>
	<p>Install appropriate control mechanisms, such as locks, alarms, and bars.</p>
	<p>Prevent unauthorized personnel from seeing or hearing information processing equipment.</p>
	<p>Equip all sensitive areas with fire, water, and physical intrusion alarm systems that automatically alert the appropriate personnel.</p>
	<p>Provide additional security for the most sensitive areas of information processing facilities.</p>

**Securing Physical Entry to Restricted Areas**

Buildings that house IT resources should be physically secure. Access to specific areas and rooms that contain IT equipment should be restricted.

**Principle**

Each USG institution should restrict access to areas within facilities that house sensitive or critical USG information systems.

**Guidelines**

The guidelines for screening physical entry to restricted areas are:

Guideline	Description
<p><b>Issue institution identification badges</b></p>	<p>Implement a badge system for sensitive areas. Badges should contain identifying information such as:</p> <ul style="list-style-type: none"> <li>• Name</li> <li>• Photograph</li> <li>• Job title</li> <li>• Level of building access</li> </ul>
	<p>Implement an entry system that requires a badge check prior to entry. Checks can be performed by the following:</p> <ul style="list-style-type: none"> <li>• Receptionists</li> <li>• Desk attendants</li> <li>• Security guards</li> <li>• Electronic card readers</li> </ul>
	<p>Maintain entry logs.</p>
	<p>Train users to challenge anyone in a restricted area who is not wearing a badge.</p>
	<p>Review and update access rights to restricted areas regularly.</p>
<p><b>Restrict physical access</b></p>	<p>Implement appropriate physical access control. The security administration should consult with the managers responsible for staff in restricted areas to determine the appropriate method, such as:</p> <ul style="list-style-type: none"> <li>• Receptionists</li> <li>• Metal key locks</li> <li>• Magnetic card door locks</li> </ul>
<p><b>Secure sensitive information</b></p>	<p>Secure sensitive information, either in paper or electronic format, from unauthorized access and disclosure as follows:</p> <ul style="list-style-type: none"> <li>• Paper – in unattended locations should be locked in safes, file cabinets, or other appropriate containers. Desks should be clear during non-working hours.</li> <li>• Electronic – electronic information should be secured through passwords and physical security of areas where it resides.</li> </ul>
<p><b>Inspect luggage and packages</b></p>	<p>Inspect user’s luggage and packages as necessary to safeguard and deter theft of sensitive equipment and information.</p>

## Securing Equipment Sites

Access to specific equipment sites should be restricted. Equipment sites also need protection from environmental threats.

---

### Principle

Each USG institution should protect critical USG computer and communications equipment from physical and environmental threats.

---

### Guidelines

Guidelines for securing equipment are:

Guideline	Description
<b>Secure production systems</b>	Place production systems in a physically secured area. Production systems include the following: <ul style="list-style-type: none"> <li>• Servers</li> <li>• Hubs</li> <li>• Routers</li> <li>• Voicemail systems</li> </ul>
	Train users about their responsibility to protect equipment by avoiding the following behaviors in workstation areas: <ul style="list-style-type: none"> <li>• Eating</li> <li>• Drinking</li> <li>• Smoking</li> </ul>
<b>Assure continual service</b>	Provide security controls that alert, monitor, and log the following threats: <ul style="list-style-type: none"> <li>• Intrusions</li> <li>• Fires</li> <li>• Explosives</li> <li>• Smoke</li> <li>• Water</li> <li>• Dust</li> <li>• Vibrations</li> <li>• Chemical and electrical effects</li> <li>• Electrical supply interferences</li> <li>• Electromagnetic radiation</li> </ul>

## Securing Power Supplies

USG facilities that provide critical IT resources are responsible for ensuring continuous service through alternative means. Critical systems should be analyzed to determine the necessary power alternatives.

---

### Principle

Each USG institution should provide continuous power to maintain the availability of critical equipment and information systems.

---

### Guidelines

Guidelines for securing power supplies are:

Guideline	Description
<b>Assess risk</b>	Perform a risk assessment of power supplies that affect all information processing systems to determine the type of protection required. Consider the following questions for each system: <ul style="list-style-type: none"> <li>• How critical is this system to public safety?</li> <li>• How critical is this system to regular campus operations?</li> <li>• How critical is this system to information security?</li> <li>• Is it necessary that this system continue to operate in the event of a power failure?</li> <li>• Can this system be shut down until power is restored without affecting any major or critical campus operations?</li> </ul>
<b>Provide limited power alternatives</b>	Use uninterruptible power supply (UPS) systems for brief power interruptions or to allow time for the orderly shutdown of systems for prolonged power outages. Note: Due to cost, UPS systems are normally used for business critical operations only.
	Implement a procedure to test UPS equipment regularly to ensure that it is functioning and has adequate capacity.
	Develop contingency plans in case UPS systems fail.

Guideline	Description
<b>Provide long-term power alternatives</b>	Use back-up generators if the risk assessment results indicate that a system must continue to operate in the event of a prolonged power failure.
	Implement a procedure to test generators regularly as directed by the manufacturers' instructions.
	Ensure that sufficient fuel is available.
<b>Prepare for emergencies</b>	Install emergency power switches near emergency exits in equipment rooms for rapid power-down.
	Install emergency lights in critical areas in case of a main power failure.
<b>Protect against lightning</b>	Provide lightning protections to all critical facilities.
	Provide lightning protection filters to all external communications lines.

## ***Securing Equipment Re-Use or Disposal***

To ensure the security of USG information, facilities should develop procedures to render information unrecoverable before equipment is disposed of or re-used.

---

### **Principle**

Each USG institution should clean equipment containing storage media prior to re-use or disposal to prevent unauthorized exposure to data. Disposal of equipment should be done in accordance with all applicable surplus property and environmental disposal laws, regulation, or policies.

---

## Guidelines

The guidelines for re-using or disposing of equipment are:

Guideline	Description
<b>Delete sensitive information</b>	Implement procedures to render the institutions information unrecoverable before allowing the re-use or disposal of equipment. <b>Note:</b> The delete feature on most software packages is not sufficient to cleanse equipment. Deleted information may still be recoverable.
<b>Destroy media</b>	Implement procedures to destroy defective or damaged media containing sensitive information before allowing the re-use or disposal of equipment. Media may include: <ul style="list-style-type: none"> <li>• Floppy disks</li> <li>• Compact disks</li> <li>• Tapes</li> </ul> Implement procedures to shred hard copies of sensitive information.



## Operations Management

This section contains guidelines for the following policies:

- **Securing operational change**
- **Developing network controls**
- **Separating development and operational facilities**
- **Securing external facilities management**

### *Securing Operational Change*

USG facilities should assign change management responsibilities as necessary to implement a formal change management process to maintain system security.

---

#### Principle

Each USG institution should control all changes to information processing facilities, systems, software, and procedures.

---

#### Guidelines

Guidelines for securing operational change are:

- Identify and record significant changes in an audit log
- Assess the potential impact of changes
- Implement formal approval procedures for changes
- Communicate details of change to all relevant personnel
- Implement procedures for aborting and recovering from unsuccessful changes
- Build awareness of the importance of change management into system life-cycles
- Integrate operational and application change control procedures as necessary

### *Developing Network Controls*

Network controls ensure the security of USG information and connected services.

---

## Principle

Each USG institution should establish controls to ensure the security of the networks they operate.

---

## Guidelines

To achieve and maintain security on computer networks a range of controls must be utilized. The common objective of these controls should be to protect all information and all connected service from unauthorized access. Security management of networks may span organizational boundaries and may involve protecting sensitive data passing over public networks. Guidelines for network security are:

- Separated operational responsibilities for networks and computer operations where appropriate
- Establish remote equipment management
- Establish special controls to protect data passing over public networks and connected systems
- Use network management tools and procedures to ensure controls are consistently applied and services are optimized

## *Separating Development and Operation Facilities*

Separation of development, operation, and test systems reduces the risk of unauthorized changes or access. To operate properly, each type of computing system requires a known and stable environment.

---

## Principle

Each USG institution should separate operation computing environments from development and test computing environments to reduce the risk of one environment adversely affecting another.

---

## Guidelines

Guidelines for separating facilities are:

- Operate development and operational software on different computer processors, in different domains, or in different directories

- Separate development and testing activities from production activities
- Prevent the access of software development utilities from operational systems, unless required.
- Avoid using the same log-on procedures, passwords, and display menus for both operational and test systems to reduce the risk of accidental log-on and other errors
- Implement controls to ensure that administrative passwords for operational systems are closely monitored and controlled
- Define and document the procedures for transferring software from development to operational status. Such transfers should require management approval

## ***Securing External Facilities Management***

External facilities management introduces additional security risks that require special precautions. Specific risks should be identified in advance and appropriate controls should be agreed upon with the contractor.

---

### **Principle**

Each USG institution should establish contractual controls to reduce security risks from external contractors that manage information processing facilities.

---

### **Guidelines**

Guidelines for securing external facilities management are:

- Identify sensitive or critical applications that should be retained in-house
- Obtain approval of business application owners to utilize external facilities
- Consider business continuity plan implications
- Specify security standards and compliance measurement processes
- Implement procedures to effectively monitor all relevant security activities
- Perform background checks and other techniques to screen vendor personnel and require confirmation that background checks have been successfully completed
- Define responsibilities and procedures for reporting and handling security incidents

- Define the security parameters for communications and data to the external site

## System and Software Management

This section contains guidelines for the following policies:

- **Developing information and software exchange agreements**
- **Developing electronic mail security**
- **Securing publicly available systems**
- **Maintaining adequate system capacity**
- **Ensuring system acceptance**
- **Protecting against malicious software**

### *Developing Information and Software Exchange Agreements*

Exchange of information with other organizations should be based on a formal agreement that specifies the conditions for handling the information, such as non-disclosure agreements. The agreement should exist whether the information is in electronic or physical form. The content of the agreement will vary depending on the reason for the exchange.

---

#### Principle

Each USG institution should implement agreements for the exchange of information with external organizations.

---

#### Guidelines

Guidelines for exchange agreements are:

- Assign responsibilities for transmission, dispatch, and receipt
- Notify senders of a transmission, dispatch, and receipt
- Implement minimum technical standards for packaging and transmission
- Implement courier identification standards
- Assign responsibilities and liabilities in the event of lost data
- Implement a labeling system for critical or sensitive data to ensure recognition and protection
- Assign responsibilities for software data protection, copyright compliance, and similar considerations
- Implement extra controls for sensitive items as necessary

## ***Developing Electronic Mail Security***

Electronic mail (e-mail) creates additional security concerns that should be addressed in procedures developed for users at all levels.

---

### **Principle**

Each USG institution should develop an acceptable use policy for their IT resources and actively monitor the network for compliance with state and federal regulations.

---

### **Guidelines**

Guidelines for securing e-mail are:

- Implement user identification and defensive systems against e-mail attacks, such as viruses
- Implement techniques to protect e-mail attachments, such as filtering, stripping, or store and forward
- Implement restrictions on defamatory, harassing, or other forms of illegal or injurious e-mail
- Implement cryptographic techniques to protect the confidentiality and integrity of electronic messages
- Implement techniques to for message retention
- Implement proper handling of messages so that the sender cannot be authenticated
- Implement signed agreements for state employees for acceptable use and inspection of emails without the expectation of privacy

## ***Securing Publicly Available Systems***

Publicly available systems create additional security concerns that should be addressed in procedures developed for users at all levels.

---

### **Principle**

Each USG institution should provide public access to USG electronic information resources in accordance with the safeguards used to protect USG resources.

---

## Guidelines

Guidelines for securing publicly available systems are:

Guideline	Description
<b>Disseminate institutional information classified as public</b>	Disseminated information should be classified in compliance with data protection legislation.
	Implement procedures to protect public information from unauthorized modification and denial of service attacks.
	Ensure that information input to and processed by public systems, such as request forms, comment forms, and questionnaires, are processed in a timely manner.
	Implement procedures to protect sensitive information during the collection process.
	Ensure that users are not allowed unauthorized access to networks connected to sensitive institutional information.
	Ensure that information made available to authorized users, such as certain state employees, is protected from unauthorized access.

Guideline	Description
<b>Secure electronic-commerce transactions</b>	Implement periodic penetration testing or other security assessment to ensure that security has not been compromised.
	Implement third-party analysis of e-commerce web servers to test the following: <ul style="list-style-type: none"><li>• Internal/External system</li><li>• Security policy</li><li>• Hypertext link integrity</li><li>• CGI</li><li>• Server identification</li><li>• Responding ports on the server IP address</li><li>• Know subversions based on server technology</li><li>• Observable IP networks from the Internet</li><li>• Memory bounding and exception handling</li><li>• Change controls</li><li>• User accounts</li><li>• Backup and recovery</li><li>• Intrusion detection</li><li>• Unauthorized changes</li><li>• DMZ penetration</li></ul>

## ***Maintaining Adequate System Capacity***

USG facilities are responsible for providing adequate system capacity for future information system requirements.

---

### **Principle**

Each USG institution should monitor current and future system capacity requirements to ensure continuous and adequate power, bandwidth, and storage.

---

## Guidelines

Guidelines for maintaining adequate system capacity are:

- Monitor changing demands for:
  - Processing power
  - Bandwidth
  - Storage
- Project future requirements by assessing key system resources, such as:
  - Processors
  - Main storage
  - File storage
  - Printers
  - Communications systems
- Identify usage trends and changes to specific applications or systems

## *Ensuring System Acceptance*

Procedures to ensure system acceptance will reduce the risk of systems failure due to inadequate testing and validation acceptance of new or upgraded information systems.

---

## Principle

Each USG institution should define, document, and utilize the necessary system acceptance criteria for all new information systems and system upgrades to avoid system failure.

---

## Guidelines

Before installing or upgrading information systems, clearly define, document, and test acceptance controls that include the following:

- Authorized security controls
- Business continuity preparations
- Error recovery, restart, and contingency plans and procedures
- Manual operating procedures
- Operation training for new or upgraded systems
- Penetration testing
- Projected performance and capacity requirements

- Standardized routine operating procedures
- User verification of proper operational performance
- Verification of the non-profit of the new system on existing systems and on overall organizational security

## ***Protecting Against Malicious Software***

Securing systems against malicious software requires user awareness, change management policies, and system controls. Malicious software can include the following:

- Computer viruses
- Network worms
- Trojan horses
- Logic bombs

---

### **Principle**

Each USG institution should use prevention and detection controls and create security awareness among state employees to protect information systems and services against malicious software.

---

### **Guidelines**

Guidelines for protecting institutional systems are:

- Comply with software licenses
- Prohibit use of unauthorized software
- Avoid software files from external sources
- Install, update, and consistently use anti-virus software on personal computers and network file servers
- Review critical system data for unauthorized files
- Review files from unknown sources before use
- Review e-mail attachments and file downloads before use
- Train system managers to establish methods for virus protection, incident reporting, and attack recovery
- Establish business continuity and attack recovery plans
- Ensure malicious software warnings and bulletins are accurate and informative

## Information Management

This section contains guidelines for the following policies:

- **Handling information**
- **Disposing of media**

### *Handling Information*

Electronically-stored USG information should be protected from unauthorized access or misuse.

---

#### Principle

Each USG institution should establish internal procedures for the secure handling and storage of its electronically-stored information to prevent unauthorized access or misuse.

---

#### Guidelines

Guidelines for handling electronically-stored information are:

- Develop procedures to invoice and manage the following:
  - Documents
  - Computing systems
  - Networks
  - Mobile users
  - Postal services
  - E-mail
  - Voice mail
  - Voice communications
  - Fax machines
  - Multi-media
  - Other sensitive items
- Develop methods for handling and storing media
- Develop access restrictions to identify unauthorized users
- Maintain formal records of the recipients of data
- Store media in accordance with manufacturer's specifications
- Restrict distribution of information
- Indicate the authorized recipient of all copies of data

- Review distribution lists and verify authorized recipients at regular intervals

## Disposing of Media

To ensure the security of USG information, facilities should develop procedures to render information unrecoverable before disposing of media.

---

### Principle

Each USG institution should develop a media disposal process based on the sensitivity of the data as determined by law and the data owners.

---

### Guidelines

Guidelines for disposing of media are:

Guideline	Description
<b>Identify sensitive media</b>	Sensitive media that require secure disposal include any media that contains sensitive institution information, such as: <ul style="list-style-type: none"><li>• Paper documents</li><li>• Output reports</li><li>• System documentation</li><li>• Program listings</li><li>• Removable disks or cassettes</li><li>• Recordings</li><li>• Magnetic tapes</li><li>• Optical storage media</li><li>• Test data</li></ul>
<b>Dispose of paper media</b>	Develop procedures to incinerate or shred sensitive paper media.
<b>Cleanse magnetic or optical media</b>	Develop procedures to cleanse magnetic or optical media before re-use. Consider using software designed to securely erase and reformat the media.

<b>Guideline</b>	<b>Description</b>
<b>Develop disposal procedures</b>	Consider hiring a media disposal contractor to ensure adequate security control.
	Maintain a log of the disposal of sensitive items to provide an audit trail.
	Avoid collecting large quantities of media to be disposed at one time. This makes it more difficult to keep a record of disposed media.



# 10 Back-Up Procedures

This section contains guidelines for the following policies:

- **Developing back-up procedures**
- **Maintaining activity logs**
- **Maintaining fault logs**
- **Developing disaster recovery and business continuity**

## *Developing Back-Up Procedures*

A back-up plan is necessary to ensure essential, electronically-stored business data can be recovered in the event of a system failure or disaster.

---

### Principle

Each USG institution should develop back-up procedures for all essential, electronically-stored business data.

---

### Guidelines

Guidelines for information back-up are:

Guideline	Description
<b>Develop back-up procedures</b>	Determine which data is essential and how often it should be backed-up.
	Implement procedures to back-up data on a regular basis.
	Determine if back-ups should be retained temporarily or permanently archived.
	Maintain 3 cycles of back-ups for critical business applications.
	Store back-ups at a secure, remote location. Apply the same standards to back-ups that apply to media on the main site.

Guideline	Description
<b>Test the procedures</b>	Test system facilities to ensure that essential business data can be recovered following a system failure or disaster.
	Test back-up media regularly to ensure that it can be restored.
	Test the restoration procedure regularly to ensure the procedures are appropriate, restoration systems are adequate, and the restoration process can be completed within the time allotted in the recovery procedures. <b>Example:</b> Once a week, delete a file and recover it from the backup tapes. All tape drives should be tested to ensure they are adequately backing up data.

**Note:** It is very important to test backup procedures to ensure that data restoration in case of an emergency or system failure.

## Maintaining Activity Logs

Maintaining activity logs is an important component of system back-up. Logs can be used to trace system activity and errors.

---

### Principle

Each USG institution should maintain appropriate activity logs for critical information systems.

---

### Guidelines

Guidelines for maintaining activity logs are:

Guideline	Description
<b>Develop activity logging procedures</b>	Create activity logs which include the following: <ul style="list-style-type: none"> <li>• Start and finish date and time for system activity</li> <li>• System errors and corrective action taken</li> <li>• Confirmation of proper handling of media</li> <li>• Name of the person making the log entry</li> </ul>
	Store logs in a secure place.
	Develop procedures to review the logs regularly.

Guideline	Description
Use automated logs	Implement automated logging whenever possible.
	Configure automatic logs to record the following: <ul style="list-style-type: none"> <li>• System utilization</li> <li>• System errors and corrective actions taken (especially automated error recovery)</li> <li>• Communication session statistics</li> <li>• Successful and unsuccessful logins</li> </ul>

## Maintaining Fault Logs

Maintaining fault logs is an important component of system back-up. Logs can be used to trace system activity and errors.

---

### Principle

Each USG institution should maintain fault logs for information systems and services.

---

### Guidelines

Guidelines for maintaining activity logs are:

Guideline	Description
Use manual fault logging	Develop procedures for personnel who monitor system operations to maintain a fault log.
	Create logging procedures to include: <ul style="list-style-type: none"> <li>• Date and time of log entry</li> <li>• Description of fault and corrective actions taken</li> <li>• Name of the person making the log entry</li> <li>• Review and confirmation of proper handling of fault</li> <li>• Review and corrective measures to ensure that controls have not been compromised</li> </ul>
Use automated fault logging	Implement automated logging whenever possible.
	Configure automatic logs to record the following: <ul style="list-style-type: none"> <li>• System utilization</li> <li>• System errors and corrective actions taken (especially automated error recovery)</li> <li>• Communication session statistics</li> <li>• Successful and unsuccessful logins</li> </ul>

## Developing Disaster Recovery and Business Continuity

USG facilities must ensure their departments continue to deliver essential business functions despite damage, loss, or disruption of information systems due to an emergency or disaster.

---

### Principle

Each USG institution should develop, test, and maintain disaster recovery and business continuity plans to ensure essential services and communications remain available in the event of an emergency or disaster.

---

### Guidelines

Guidelines for developing disaster recovery and business continuity are:

Guideline	Description
<b>Assess the risks and impacts of an emergency or disaster</b>	Assess the possibility of an emergency or disaster to all relevant systems. Analyze the likelihood of each risk and determine the priority of the risks based on the importance and sensitivity of the system.
	Assess the impact of an emergency or disaster through an impact analysis. Consider long and short-term interruptions and the different impacts of minor and major incidents.
<b>Develop business continuity</b>	Create business continuity plans to support the organizations objectives and priorities.
	Develop a process to regularly test the business continuity plan to determine if it is effective. Ensure that the plan is updated when the business process changes.

## Documentation

This section contains guidelines for the following policies:

- **Documenting security policies, procedures, plans, guidelines, and standards**
- **Documenting operating procedures**
- **Documenting operations system security**

### *Documenting Security Policies, Procedures, Plans, Guidelines, and Standards*

Once an institution has agreed upon a set of security policies, those policies should be documented. The procedures, plans, guidelines, and standards used to enforce the policies should also be documented and disseminated.

---

#### Principle

Each USG facility should document its IT security policies, procedures, plans, guidelines, and standards.

---

#### Guidelines

Each institution should document its IT security policies. In addition, all procedures, plans, guidelines, and standards that support those policies should be documented and disseminated to the appropriate managers and users.

### *Documenting Operating Procedures*

Operating procedures should be documented and maintained to ensure secure operation of USG information processing facilities.

---

#### Principle

Each USG institution should document operating responsibilities and procedures for USG information processing facilities.

---

## Guidelines

Guidelines for documenting operational procedures are:

Guideline	Description
<b>Document operation functions</b>	Document specific instructions for operation functions, such as: <ul style="list-style-type: none"><li>• Handling and processing information</li><li>• Scheduling requirements (include definitions, start/stop times, interdependencies)</li><li>• Handling exceptions or errors</li><li>• Contacting technical support if necessary</li><li>• Handling data processing output and disposal of output from failed jobs</li><li>• Restart and recovery after a system failure</li><li>• Responding to incidents</li><li>• Recovering from disasters</li><li>• Access approval methods</li></ul>
<b>Document system maintenance</b>	Document the typical system maintenance activities, such as: <ul style="list-style-type: none"><li>• Start/stop procedures</li><li>• System back-up</li><li>• Equipment maintenance procedures and time windows</li><li>• Computer room management and safety</li><li>• Mail handling management and safety</li></ul>

## *Securing Operations System Documentation*

System documentation, such as operations manuals, tables, and access control lists, should be protected from unauthorized disclosure.

---

## Principle

Each USG institution should develop procedures to secure operational system documentation from unauthorized access.

## **Guidelines**

Guidelines for securing operational system documentation are:

- Store system documentation in a manner that is consistent with its classification
- Restrict the access list for system documentation to the minimum authorized by the application owner
- Protect system documentation that resides on or can be accessed from a public network



# 12 Access Control

This section contains guidelines for the following policies:

- **Developing an access control policy**
- **Managing passwords**
- **Controlling access to networks and systems**
- **Controlling network connection times**
- **Monitoring system access**
- **Managing remote access**

**Note:** Refer to **Chapter 6: Physical and Environmental Security** for more information about physical security.

## *Developing an Access Control Policy*

Access control policies should be based on the specific purpose of a system and its applicable security policies.

---

### Principle

Each USG institution should control access to information systems. All sensitive USG information should be protected from improper disclosure, modification, and deletion.

---

### Guidelines

Guidelines for controlling access are:

Guideline	Description
<b>Develop privilege management</b>	Identify the owners of sensitive institution information. These individuals should have sole authority to grant access to the information which they are responsible for.
	Develop a ‘deny-all’ default access privilege that applies to all users until they are granted permission to access specific systems and information.
	Base user permissions on a ‘need to-know’ basis.
	Develop a process to log and review privilege management activities.

Guideline	Description
<p><b>Develop access authorization</b></p>	<p>Appoint supervisors or managers to be responsible for:</p> <ul style="list-style-type: none"> <li>• Granting access to information on a ‘need to know’ criteria of the information owners</li> <li>• Creating user identifications (IDs) and passwords</li> <li>• Deleting user permissions</li> <li>• Changing user permissions</li> </ul>
	<p>Develop a process of written approval by managers and information owners before user IDs are issued to new or transferred employees, or contractors, consultants, and temporary employees.</p>
	<p>Develop a process to deny permissions to users who no longer fit the ‘need to know’ criteria, such as employees who leave or change jobs, or contractors and temporary employees whose contracts have ended.</p>
	<p>Develop user responsibilities that users agree to before receiving user IDs. Users should physically or electronically sign the following agreements:</p> <ul style="list-style-type: none"> <li>• Confidentiality</li> <li>• Information system security</li> </ul>
	<p>Provide all new users with a statement describing their access rights and responsibilities. Users are responsible for all activity performed with their user IDs and should be informed to avoid the following:</p> <ul style="list-style-type: none"> <li>• Allowing others to use their ID</li> <li>• Using someone else’s ID</li> </ul>

Guideline	Description
<b>Restrict information access</b>	Ensure that application access is granted to authorized users, only.
	Assign the following user access rights based on job functions: <ul style="list-style-type: none"> <li>• Read</li> <li>• Write</li> <li>• Execute</li> <li>• Delete</li> </ul>
	Ensure the integrity of information in applications and systems that share resources.
	Secure access to system Help files that contain information about overriding existing system security.
	Ensure that public institutional information in systems that provide resources to the public is segregated from non-public information.
<b>Secure access to software</b>	Develop appropriate access policies for: <ul style="list-style-type: none"> <li>• Custom application software</li> <li>• Software utilities</li> </ul>

## Managing Passwords

Passwords are an important component of controlling access to IT resources. Password procedures should provide security sufficient for the sensitivity of the system.

---

### Principle

Each USG institution should develop password management.

## Guidelines

Guidelines for managing passwords are:

Guideline	Description
<p><b>Develop unique password and authentication policies</b></p>	<p>Develop a user authentication system that links a unique password to each user ID. Users should change passwords immediately if they suspect others have discovered the password. Passwords should be assigned to the following:</p> <ul style="list-style-type: none"> <li>• User level accounts</li> <li>• Web accounts</li> <li>• E-mail accounts</li> <li>• Screen saver protection</li> <li>• Voicemail accounts</li> <li>• Local router logins</li> </ul>
	<p>Develop strong password construction as a first line of defense against improper access. Strong passwords typically exhibit the following characteristics:</p> <ul style="list-style-type: none"> <li>• At least 8 alphanumeric characters</li> <li>• Upper and lower case characters</li> <li>• Digits and special characters as well as letters, such as numbers (0-9) and other characters (!@#%&amp;)</li> <li>• No identifiable words in any language, slang, dialect, or jargon</li> <li>• No personal information, such as family names</li> <li>• No null passwords or passwords which are the same as the user ID</li> </ul>
	<p>Ensure that all applications support the following:</p> <ul style="list-style-type: none"> <li>• Authentication of individual users, not groups</li> <li>• Role management that allows one user to take over the functions of another without a password</li> <li>• Password integrity by not storing passwords in clear text or any reversible form</li> </ul>
	<p>Develop a one-time password authentication or a public/private key system with a strong pass phrase for remote access users.</p>

Guideline	Description
<p><b>Develop password change and review policies</b></p>	<p>Develop a policy to change passwords as often as possible without increasing the likelihood that users will write down the password. The following list indicates how often certain types of passwords should be changed at a minimum:</p> <ul style="list-style-type: none"> <li>• System-level passwords - monthly</li> <li>• User-level passwords - every 45 days</li> </ul>
	<p>Develop a procedure to perform periodic, random password audits by attempting to guess passwords or using an automated tool. If a password is determined during a test the use should change it immediately.</p>

## Controlling Access to Networks and Systems

USG facilities should control access to their networks, systems, and resources based on user authorization and rights.

---

### Principle

Each USG institution should control access to its networks, systems, and resources to ensure only authorized users gain access based on their level of authorization.

---

### Guidelines

Guidelines for controlling access to networks and systems are:

Guideline	Description
<p><b>Control use of network services</b></p>	<p>Control the use of the institution's network services by developing procedures to:</p> <ul style="list-style-type: none"> <li>• Verify user identity through institution issued user IDs linked to a confidential password</li> <li>• Develop an authentication system for internal networks that store sensitive institution information</li> <li>• Protect in-bound connections to networks with a dynamic password access control system</li> </ul>

Guideline	Description
<p><b>Control use of network services, cont</b></p>	<p>Control third-party and public access to institutional network services by developing procedures to:</p> <ul style="list-style-type: none"> <li>• Gain approval of security and access administration before granting third-party access</li> <li>• Protect institutional networks connected to the Internet with an access control system</li> <li>• Protect outbound connections initiated from institution offices by routing them through systems expressly established to provide secure network access</li> <li>• Encrypt all links that allow access to sensitive institution information outside the network</li> <li>• Avoid shared file systems between internal and external systems</li> <li>• Install and enable anti-virus programs on all web servers, LAN servers, mail servers, and networked PCs</li> <li>• Develop session time-outs for systems accepting remote connections from public networks, such as dial-up phone network or the Internet</li> <li>• Use login banners on all networks and computers that are directly accessible through external networks</li> <li>• Maintain system logs on all networks and computers which interface with external networks. Logs should indicate time, date, identity, and activity</li> <li>• Implement control mechanisms on all networks connected to external networks</li> <li>• Apply authentication to host systems that accept automatic connections from remote computers, such as Virtual Private Networks (VPN) and remote access services</li> <li>• Use remote diagnostic port protection</li> </ul> <p>Segregate large networks that cross organizational boundaries with separate logical domains, each protected with suitable security perimeters and access controls.</p> <p>Use an intrusion detection system on key communications segments to intercept and analyze traffic. These systems should be monitored and updated routinely for current patches and signatures for intrusion detection.</p>

Guideline	Description
<p><b>Control the network connection</b></p>	<p>Develop additional access control for in-bound connections to internal institution networks and systems through external sources.</p>
	<p>Use firewalls to protect system and networks with web access and inbound applets containing active content, such as Sun's Java, Microsoft's Active X, Microsoft's Visual Basic scripts, and Macromedia Shockwave files.</p>
	<p>Run all firewalls, routers, and access control devices used to protect internal networks on separate dedicated computers. These computers should not be used for any other purpose, such as web servers.</p>
	<p>Train employees and managers to follow established policies for configuration and use of firewall, router, and access control devices. These policies should not be changed without permission of the appropriate security administrator.</p>
	<p>Apply proper access control lists to communication devices such as firewalls, routers, and servers to prevent unauthorized access.</p>
	<p>Disable unused ports.</p>
<p><b>Develop security measures for service providers</b></p>	<p>Review all documentation for a system prior to using service providers to avoid disclosing confidential information. <b>Note:</b> Service providers acting as common carriers assume no responsibility for institutional information.</p>
	<p>Sign security agreements with potential service providers who will handle institutional information.</p>
<p><b>Develop wireless network access policies</b></p>	<p>Develop operating system hardening to include the following:</p> <ul style="list-style-type: none"> <li>• Removal of default shares, such as C\$</li> <li>• Strong administrator passwords</li> <li>• No unnecessary services/applications running on machines</li> </ul>
	<p>Employ Frequency Hopping Spread Spectrum instead of Direct Sequence Spread Spectrum to secure transmissions and less interference of transmissions.</p>

Guideline	Description
<b>Secure system utilities</b>	Develop polices to secure system utilities that: <ul style="list-style-type: none"> <li>• Employ user authentication of all system level utilities</li> <li>• Segregate utilities from other general user executables</li> <li>• Limit the use of system utilities to a subset of authorized users with specific training and privileged user access</li> <li>• Use system utility logging</li> <li>• Develop documentation to describe system utilities and their purposes</li> <li>• Harden the operation system to remove unnecessary utilities</li> <li>• Place time constraints on the use of system utilities</li> </ul>
	Develop security that is appropriate to the different types of utilities.
	Develop access control policies to prevent unauthorized users from accessing diagnostic, network, change control, and administrative utilities

## Controlling Network Connection Times

Facilities can control access to USG networks by limiting the time and dates when user connections are accepted and to automatically log users off after a period of inactivity.

---

### Principle

Each USG institution should control network connectivity. This includes restricting user utilization, such as bandwidth usage.

---

## Guidelines

Guidelines for controlling connection times are:

Guideline	Description
<b>Limit connection times</b>	Use timed logins to protect critical applications and data that require added security. Timed logins allow specific users to access the system at specific times. Security administrators and business management should be consulted before overriding any timed login.
	Use timed windows on institution systems that receive information from outside computing sources. The timed window should be opened to begin the process and close when the process is complete.
<b>Establish session time-outs</b>	Establish session time-outs that will terminate a connection that has been inactive for a certain period of time. The length of time before time-out should be determined by: <ul style="list-style-type: none"> <li>• Level of risk associated with a logged in session</li> <li>• Sensitivity of data</li> </ul>

## Monitoring System Access

USG systems should be monitored to detect misuse of resources.

---

## Principle

Each USG institution should develop a plan to audit its systems to monitor the activities of system users.

## Guidelines

Guidelines for monitoring system access are:

Guideline	Description
<p><b>Assess the risk of unauthorized use</b></p>	<p>Determine the risk of unauthorized use of a system with a risk assessment. The assessment should consider the following:</p> <p>Authorized access:</p> <ul style="list-style-type: none"> <li>• User ID</li> <li>• Date and time of key events</li> <li>• Types of events</li> <li>• Files or resources accessed</li> <li>• Program, utilities, and applications</li> </ul> <p>Privileged operations:</p> <ul style="list-style-type: none"> <li>• Supervisor account use</li> <li>• System start and stop activity</li> <li>• I/O device attachment/detachment</li> </ul> <p>Unauthorized access attempts:</p> <ul style="list-style-type: none"> <li>• Failed attempts</li> <li>• Access policy violations and notifications network gateways and firewalls</li> <li>• Alerts from proprietary intrusion detection systems</li> </ul> <p>System alerts or failures:</p> <ul style="list-style-type: none"> <li>• Console alerts or messages</li> <li>• System log exceptions</li> <li>• Network management alarms</li> </ul>
<p><b>Monitor system use</b></p>	<p>Develop monitoring procedures based on the findings of the risk assessment. These procedures should facilitate the discovery of attempts at unauthorized use.</p> <hr/> <p>Develop a system to maintain and regularly review log files. Secure log files to prevent unauthorized alterations.</p>

Guideline	Description
<p><b>Monitor events</b></p>	<p>Develop a system to monitor logging events to contain the following, at a minimum:</p> <ul style="list-style-type: none"> <li>• User ID</li> <li>• Dates and times of login and logoff</li> <li>• Login method, location, terminal identity, network address</li> <li>• Records of successful and unsuccessful system access attempts</li> <li>• Records of successful and rejected data access and other resource access attempts</li> </ul>
	<p>Develop a system to maintain and regularly review log files. Determine the length of retention based on availability of resources and the need to track historical information. Logs can be used evidence in future investigations and should be maintained as long as resources allow.</p>
	<p>Develop a system to maintain data access event logs and correlate the information with system access logs.</p>

## Managing Remote Access

Access controls should include remote access users. Remote access policies should adhere to all existing security policies.

---

### Principle

Each USG institution should manage remote access to its networks, systems, and their resources.

## Guidelines

Guidelines for managing remote access are:

Guideline	Description
<b>Assess the risk of remote access</b>	Determine the risks of remote access to internal systems with a risk assessment
	Determine the methods of access most compatible with the required security levels of each system based on the results of the risk assessment.
	Develop requirements for specific connection methods or the use of cryptographic techniques based on the results of the risk assessment.
	Develop document policies for remote access based on the results of the risk assessment.
<b>Assess the benefits of teleworking</b>	Determine if teleworking will benefit an organization by considering the following: <ul style="list-style-type: none"> <li>• Can the teleworking site meet current physical security requirements for internal systems?</li> <li>• Will the proposed teleworking environment promote staff productivity?</li> <li>• Are the networking and communications systems reliable, robust, and secure enough to meet current security requirements for data communications?</li> <li>• Is physical access to the teleworking environment secure enough to ensure no compromise of the computing resources connected to it?</li> <li>• Does the teleworking environment provide sufficient, secure storage space for materials and equipment?</li> <li>• Does the local environment have provisions for securing any unused network connections into the networked infrastructure?</li> <li>• Does the teleworking environment have timely procedures for revoking access to its facilities as needed?</li> </ul>

Guideline	Description
<b>Train users</b>	Train users about their responsibility for the security of remote access connections. Responsibilities include: <ul style="list-style-type: none"><li>• Physical security of a connected laptop</li><li>• Security of the information on a laptop</li><li>• Cryptographic data storage and appropriate uses of cryptographic techniques</li><li>• Awareness of ‘overlooking’, such as a person watching a users logon sequence or seeing proprietary information</li></ul>



# 13 Systems Development and Maintenance

This section contains guidelines for the following policies:

- **Adhering to existing security requirements**
- **Implementing cryptographic techniques**
- **Developing change control procedures**

## *Adhering to Existing Security Requirements*

When USG systems are developed or updated all existing security policies should be observed.

### Principle

Each USG institution should ensure that all system development and maintenance adhere to existing security requirements. Business requirements for system development should specify and define the necessary system controls based on existing policy.

### Guidelines

Guidelines for adhering to existing security policies when developing or updating systems are:

Guideline	Description
<b>Develop business requirements</b>	Develop business requirements that include specifications for security controls before developing new systems or updating existing ones. Specifications should include requirements for the following: <ul style="list-style-type: none"> <li>• Automated controls</li> <li>• Manual controls</li> <li>• ‘Off the shelf’ controls</li> </ul>
	Analyze the security needs of a new or updated system. Business requirements should address the following security concerns: <ul style="list-style-type: none"> <li>• Types of risk associated with the system</li> <li>• Sensitivity of the information handled by the system</li> <li>• Pertinent data security standards that may affect security, such as HIPAA</li> </ul>

Guideline	Description
<p><b>Control access to data</b></p>	<p>Control access to data in new or updated systems based on existing security requirements. Data access requirements should address the following:</p> <ul style="list-style-type: none"> <li>• Ownership of data</li> <li>• Sensitivity of data</li> </ul>
	<p>Control access to test data. Typically, test data is classified as sensitive information and should be handled according to existing security policies for sensitive data until it is disposed of. Additional security measures are:</p> <ul style="list-style-type: none"> <li>• Perform tests on operational data only when required safeguards for that data are in place</li> <li>• Obtain authorization each time operational information is copied to a test application system</li> <li>• Erase operational information from the test application immediately after testing</li> <li>• Log all events that involve copying and using operational information</li> </ul>
<p><b>Control access to program source libraries</b></p>	<p>Remove program source libraries from production systems unless it is required.</p> <p><b>Note:</b> Removed libraries should be archived and labeled with the exact version of the software.</p>
	<p>Control access to program source libraries that remain on the system. Consider the following:</p> <ul style="list-style-type: none"> <li>• Appoint a program source librarian or administrator</li> <li>• Restrict access by IT support staff</li> <li>• Avoid storing programs under development or maintenance in production program source libraries</li> <li>• Obtain authorization from the IT support manager for an application before updating program source libraries or issuing program sources to programmers</li> <li>• Keep program listings in a secure environment</li> <li>• Maintain an audit log for all program source libraries</li> <li>• Avoid multiple updates to production modules between backups</li> <li>• Archive old versions of source programs and label them clearly</li> <li>• Apply strict change control procedures to program source libraries</li> </ul>

Guideline	Description
<p><b>Control operational software</b></p>	<p>Develop business requirements that prohibit the use of unapproved or unlicensed software. Periodically audit the software on desktop systems.</p>
	<p>Develop strict change management processes for production systems. Approvals for change at the operating system level should include security administration.</p>
	<p>Minimize operating system files to only those files required for the purpose for which the system is designed.</p>
	<p>Audit operating system files for authenticity and directory structures before placing the system into change management.</p>
	<p>Develop a regular audit schedule for production systems to monitor changes during operation.</p>
	<p>Audit dynamic data on the production system to ensure their integrity. For instance, the directory structure should contain only the expected files with typical permissions.</p>
	<p>Obtain approval from the application owners before placing static data under change management.</p>
	<p>Establish roll-back plans and event logging for all change control operations.</p>
	<p>Establish controls for production and operational systems that include the following:</p> <ul style="list-style-type: none"> <li>• Operation program libraries should be updated by the designated administrator only after receiving appropriate change management approval</li> <li>• Production systems should only hold operationally relevant code and data</li> <li>• Executable code should not be installed on a production system until it is successfully tested</li> <li>• An audit log should be maintained to record all updates to operational system files</li> <li>• Previous versions of software should be retained as a contingency measure</li> </ul>

Guideline	Description
<p><b>Avoid malicious code</b></p>	<p>Include best practices for avoiding malicious code in the business requirements before developing a new system or updating an existing one. Best practices include the following:</p> <ul style="list-style-type: none"> <li>• Buy programs from reputable sources, only</li> <li>• Buy programs with verifiable source code</li> <li>• Use evaluated, third-party products</li> <li>• Inspect all source code before use</li> <li>• Control access to code once installed</li> <li>• Screen users before allowing them access to key systems</li> <li>• Establish security policies regarding e-mail attachments and e-mail from unknown sources</li> </ul>
	<p>Place detection and protective devices at the logical perimeters of a network environment. This helps to eliminate the threat as it arrives at the first level of communication.</p>
	<p>Train users about their responsibilities to avoid malicious code. Responsibilities should include the following:</p> <ul style="list-style-type: none"> <li>• Use safe practices while connected to the Internet through an institutional network</li> <li>• Avoid 'open-source' software available over the Internet unless approved by management</li> <li>• Avoid opening e-mail attachments from unknown sources unless the it has been screen with anti-virus software</li> </ul>

## Implementing Cryptographic Techniques

If necessary, implement cryptographic techniques for those systems that require added security.

---

### Principle

Each USG institution should implement cryptographic techniques for sensitive systems as needed.

**Guidelines**

Guidelines for implementing cryptographic techniques are:

Guideline	Description
<p><b>Assess the need for cryptographic techniques</b></p>	<p>Determine the need for cryptographic techniques by conducting a risk assessment on the system.</p> <hr/> <p>Select a cryptographic technique based on the following:</p> <ul style="list-style-type: none"> <li>• Risks</li> <li>• Type of key management required</li> <li>• Level of data classification</li> <li>• Responsible parties for implementation and key management</li> <li>• Compatibility of existing data storage systems</li> <li>• Import and export laws regarding encryption technology</li> </ul>
<p><b>Develop key management</b></p>	<p>Develop policies to manage the electronic cryptographic keys if necessary. Types of key encryption are:</p> <ul style="list-style-type: none"> <li>• Symmetric</li> <li>• Public</li> <li>• Private</li> </ul> <hr/> <p>Protect keys from modification and destruction. Private keys require protection from unauthorized disclosure.</p> <hr/> <p>Create defined activation and deactivation of keys.</p> <hr/> <p>Develop a process to protect public and private keys through physical identification of the user requesting keys. This process is usually performed by the registration authority and should include due diligence for the identity of the user at the time the key is issued.</p>

Guideline	Description
<b>Develop key management, cont</b>	<p>Ensure that key management is based on existing security standards. Key management policies should include the following:</p> <ul style="list-style-type: none"><li>• Generate keys for different cryptographic systems and different applications</li><li>• Generate and obtain public key certificates</li><li>• Distribute keys to intended users with complete instructions</li><li>• Store keys in secure areas</li><li>• Update the key management rules when keys are changed</li><li>• Develop procedures for handling compromised keys</li><li>• Develop procedures to revoke and deactivate keys when necessary</li><li>• Develop procedures to archive keys when the user terminates employment</li><li>• Develop procedures to recover lost or corrupted keys</li><li>• Develop procedures for key destruction</li><li>• Log and audit key management activities</li></ul>

## Developing Change Control Procedures

Change control procedures reduce security risks and system disruption during the process of changing or upgrading operating systems or software.

---

### Principle

Each USG institution should develop change control procedures before upgrading or changing operating systems and software to avoid security risks and disruption.

**Guidelines**

Guidelines for developing change control are:

Guideline	Description
<p><b>Develop change control for data communications infrastructure</b></p>	<p>Develop a change control process that ensures continued availability of communications resources.</p>
	<p>Document all change control processes and assign staff responsibilities as necessary.</p>
	<p>Develop a review process to determine the quality of change controls.</p>
<p><b>Develop change control for software development</b></p>	<p>Develop a change control process that prevents unauthorized access to software design, code, libraries, and databases.</p>
	<p>Document all change control processes and assign staff responsibilities as necessary.</p>
	<p>Develop a review process to determine the quality of change controls.</p>
	<p>Develop change control for mainframe systems that include the following:</p> <ul style="list-style-type: none"> <li>• Maintain a record of agreed authorization levels</li> <li>• Ensure changes are submitted by authorized users</li> <li>• Review controls and the integrity of procedures to ensure that they will not be compromised by the changes</li> <li>• Identify all computer software, information, database entities, and hardware that will change</li> <li>• Obtain formal approval for detailed proposals before work commences</li> <li>• Ensure the authorized user accepts changes prior to implementation</li> <li>• Ensure the implementation is carried out to minimize disruptions</li> <li>• Update system documentation</li> <li>• Archive old documentation</li> <li>• Maintain version control of all software updates</li> <li>• Maintain an audit trail of all change requests</li> </ul>

Guideline	Description
<p><b>Develop change control for software development, cont</b></p>	<p>Ensure the security of software development for mid-range and small servers by following the same change control procedures for larger systems.</p>
	<p>Document the new mid-range or small server application. Include the following:</p> <ul style="list-style-type: none"> <li>• Function or purpose</li> <li>• Special tuning requirements</li> <li>• User account requirements</li> <li>• File and directory structures</li> <li>• Super user account requirements</li> <li>• Account and file permissions</li> <li>• Network ports</li> <li>• System library requirements and versions</li> <li>• Device file requirements</li> <li>• Data storage requirements</li> <li>• Kernel changes</li> <li>• Scheduled tasks</li> </ul>
	<p>Develop change control for desktop software to include the following:</p> <ul style="list-style-type: none"> <li>• Test the install or upgrade on all types use desktops that will be affected</li> <li>• Notify users and help-desk staff prior to the change to minimize disruption</li> <li>• Develop automated or server-based installs to minimize disruption</li> <li>• Provide extra on-call support during the change</li> <li>• Follow-up with users to ensure that the change was successful</li> </ul>
<p><b>Develop change control for third-party software</b></p>	<p>Develop a change control process for installing or upgrading third-party software. Typically, third-party software should be used as intended by the vendor. Executable code should not be modified unless the vendor supplies patches or upgrades. Avoid ‘open source’ modifications unless they are specifically supported and supplied by the vendor.</p>
	<p>Document all change control processes and assign staff responsibilities as necessary.</p>

Guideline	Description
<p><b>Develop change control for third-party software, cont</b></p>	<p>Develop change control procedures for modifying third-party software if necessary. If it is necessary to modify a software package, consider the following:</p> <ul style="list-style-type: none"> <li>• Risk of built-in controls</li> <li>• Risk to integrity controls</li> <li>• Legality of changes without vendor consent</li> <li>• Responsibility for future maintenance as a result of modification</li> <li>• Undetected security compromises</li> </ul>
<p><b>Develop change control for operating systems</b></p>	<p>Develop a change control process for operating system upgrades, such as the installation of security patches, performance patches, and maintenance upgrades.</p> <p>Document all change control processes and assign staff responsibilities as necessary.</p> <p>Develop a review process to determine the quality of change controls.</p> <p>Develop procedures to test new code prior to installation. The best option is a completely redundant system with identical system load and hardware compatibility. If this is not possible, implement unit testing.</p> <p>Backup the existing system and databases just prior to a new installation or upgrade.</p> <p>Schedule installations and upgrades at times that will have the minimum impact on business operations and notify all affected parties of any downtime.</p> <p>Close all running tasks and applications if the operation will require a re-boot. If the system has a sophisticated database with transactional capabilities or applications that require special handling, include the database and application administrators in the upgrade process.</p>

Guideline	Description
<b>Develop change control for operating systems, cont</b>	Ensure that multiple changes to a system are completed in the proper order. This process should be tested prior to install or upgrade.
	Develop an approval process for any new installation or upgrade. The approval process should include the following: <ul style="list-style-type: none"><li>• Review of application controls and integrity procedures to ensure they have not been compromised by the changes</li><li>• Ensure the annual support plan and budget cover reviews and system testing</li><li>• Notify administrators of changes in time for appropriate reviews before implementation</li><li>• Make appropriate changes to business continuity plans</li></ul>

# 14 Compliance

This section contains guidelines for the following policies:

- **Complying with legal requirements**
- **Reviewing security policies and technical compliance**

## *Complying with Legal Requirements*

USG facilities should ensure they are in compliance with current legal requirements. Refer to **Appendix B: Additional Resources** for more information.

---

### Principle

Each USG institution should comply with state and federal information security regulations and provide awareness and compliance training to all users.

---

### Guidelines

Guidelines for developing compliance policies are:

Guideline	Description
<b>Comply with state and federal regulations</b>	Develop policies for all types of institutional information. These policies should ensure the security of information while allowing the public appropriate access.
	Develop policies that comply with state and federal requirements, such as: <ul style="list-style-type: none"> <li>• HIPAA</li> <li>• FERPA</li> <li>• COPPA</li> <li>• Gramm-Leach Bailey Act</li> <li>• CJIS</li> </ul>
<b>Develop acceptable usage policies</b>	Develop policies that define acceptable use of all types of institutional information.
	Inform all users of their responsibility for the security of the institutional information to which they have access. All users should be required to sign compliance statements.

Guideline	Description
<b>Develop security awareness</b>	Develop security awareness training for all users that is commensurate with their access to the institute's information.

## Reviewing Security Policies and Technical Compliance

Once the security plan is developed and implemented, it should be reviewed periodically to address new and ongoing compliance issues in information security.

---

### Principle

Each USG institution should periodically review documented procedures and operations to ensure compliance with state and federal security requirements.

---

### Guidelines

Guidelines for reviewing compliance procedures are:

Guideline	Description
<b>Develop compliance audits</b>	Develop compliance audits to ensure that campus departments are complying with security policies. Audit frequency should be based on the sensitivity of the system.
<b>Develop technical compliance audits</b>	Develop compliance audits to determine compliance with existing security standards. Technical compliance audits should test system operations and accessibility and examine configurations.
	Develop procedures to control the dissemination and use of the results of the audit.

# Index

## A

- Acceptable use, 5-9, 14-1
  - enforcement, 5-10
  - guidelines, 5-10
  - inappropriate use (defining), 5-10
  - policies, 5-10
  - principle, 5-9
- Access control, 12-1
  - authorization, 12-2
  - guidelines, 12-1
  - information access, 12-3
  - monitoring system access, 12-9
  - network connection times, 12-8
  - networks, 12-5
  - passwords, 12-3
  - principle, 12-1
  - privilege management, 12-1
  - remote access, 12-11
  - software access, 12-3
  - systems, 12-5
- Activity logs, 10-2
  - automated, 10-3
  - guidelines, 10-2
  - logging procedures, 10-2
  - principle, 10-2
- Asset inventory, 4-2
  - guidelines, 4-2
  - principle, 4-2
- Asset risk, 4-3
  - analyzing and assessing, 4-3
  - guidelines, 4-3
  - principle, 4-3
- Assets, 1-3
  - classifying, 4-1
  - inventory, 4-2
- Awareness
  - creating, 2-6
  - maintaining, 2-6

## B

- Back-up, 10-1
  - activity logs, 10-2
  - business continuity, 10-4
  - developing procedures, 10-1
  - disaster recovery, 10-4
  - fault logs, 10-3
  - guidelines, 10-1
  - principle, 10-1
  - testing procedures, 10-2
- Board of Regents. *See* BOR
- BOR policy, A-1

- computer security policy, A-1
- developing general policies, A-1
- disruptive behavior, A-3
- equipment use off-campus, A-2
- general policy, A-1
- institutional responsibilities, A-2
- system level activities, A-2

- Business continuity, 10-4
  - developing, 10-4
  - guidelines, 10-4
  - principle, 10-4

## C

- Change control, 13-6
  - data communications, 13-7
  - guidelines, 13-7
  - operating systems, 13-9
  - principle, 13-6
  - software development, 13-7
  - third-party software, 13-8, 13-9
- CJIS, 14-1
- Classifying assets, 4-1, 4-2
  - guidelines, 4-1
  - interdependencies, 4-2
  - organization of assets, 4-1
  - principle, 4-1
  - review, 4-1
- Compliance, 14-1
- Contracting, 3-6, 3-8
- COPPA, 14-1
- Critical assets
  - automated systems, 4-5
  - data, 4-5
  - equipment, 4-5
  - facilities, 4-5
  - non-automated systems, 4-5
  - personnel, 4-5
- Cryptographic techniques, 13-4
  - assessing risk, 13-5
  - guidelines, 13-5
  - principle, 13-4

## D

- Developing policies, 2-1
  - guidelines, 2-3
  - issue-specific policies, 2-3
  - principle, 2-3
  - program policies, 2-1
  - system-specific policies, 2-2
- Developing support
  - maintenance, 2-4

- research, 2-4
- support, 2-3
- Development/operation facilities, 7-2
  - guidelines, 7-2
  - principle, 7-2
- Disaster recovery, 10-4
  - assessing risk, 10-4
  - guidelines, 10-4
  - principle, 10-4
- Disciplinary process, 5-14
  - developing, 5-15
  - guidelines, 5-15
  - principle, 5-14
  - third-party, 5-15
- DMCA, B-1
- Document organization, 1-4
- Documentation, 11-1
  - enforcement (defining), 2-5
  - exceptions (defining), 2-5
  - guidelines, 11-1
  - guidelines (defining), 2-5
  - IT security policies, 11-1
  - operating procedures, 11-1
  - plans, 11-1
  - policy (defining), 2-4
  - principle, 11-1
  - procedures, 11-1
  - securing operations system documentation, 11-2
  - standards, 11-1
  - standards (defining), 2-5
- Documenting operating procedures, 11-1
  - guidelines, 11-2
  - operation functions, 11-2
  - principle, 11-2
  - system maintenance, 11-2
- Documenting policies, 2-1, 2-4
  - guidelines, 2-4
  - principle, 2-4

## E

- E-commerce
  - securing, 8-4
- EDUCAUSE, B-2
- Electronic commerce. *See* e-commerce
- Electronic mail. *See* e-mail
- Electronically stored information
  - principle, 9-1
- Electronically-stored information, 9-1
  - guidelines, 9-1
- E-mail
  - guidelines, 8-2
  - principle, 8-2
  - security, 8-2
- Equipment re-use/disposal, 6-6
  - guidelines, 6-7
  - principle, 6-6
- Equipment sites, 6-4
  - assuring continual service, 6-4
  - guidelines, 6-4
  - principle, 6-4
  - production systems, 6-4

- Exchange of information, 8-1
- Existing security requirements, 13-1
- External facilities, 7-3
  - guidelines, 7-3
  - principle, 7-3

## F

- Fault logs, 10-3
  - automated, 10-3
  - guidelines, 10-3
  - principle, 10-3
- FERPA, 14-1

## G

- Glossary, C-1
- Government acts, B-1
- Gramm-Leach Bailey Act, 14-1
- Guidelines
  - acceptable use, 5-10
  - access control, 12-1
  - activity logs, 10-2
  - asset inventory, 4-2
  - asset risk, 4-3
  - back-up, 10-1
  - business continuity, 10-4
  - change control, 13-7
  - classifying assets, 4-1
  - cryptographic techniques, 13-5
  - developing policies, 2-3
  - development/operation facilities, 7-2
  - disaster recovery, 10-4
  - disciplinary process, 5-15
  - documentation, 11-1
  - documenting operating procedures, 11-2
  - documenting policies, 2-4
  - electronically-stored information, 9-1
  - e-mail, 8-2
  - equipment re-use/disposal, 6-7
  - equipment sites, 6-4
  - external facilities, 7-3
  - fault logs, 10-3
  - hiring, 5-8
  - implementing policies, 2-6
  - information security infrastructure, 3-2
  - Legal requirements, 14-1
  - malicious software, 8-6
  - media disposal, 9-2
  - monitoring system access, 12-10
  - network connection times, 12-9
  - network controls, 7-2
  - networks/system access, 12-5
  - operational change, 7-1
  - operations system documentation, 11-3
  - outsourcing contracts, 3-9
  - passwords, 12-4
  - power supplies, 6-5
  - publicly available systems, 8-3
  - remote access, 12-12
  - restricted areas, 6-3
  - reviewing and evaluating policies, 2-7

- reviewing policies, 14-2
- securing the physical perimeter, 6-1
- security incidents, 5-12
- security weaknesses, 5-14
- software exchange agreements, 8-1
- system acceptance, 8-5
- system capacity, 8-5
- system development/maintenance, 13-1
- third-party access, 3-4
- third-party contracts, 3-7
- training users, 5-11

## H

- Handling information, 9-1
- HIPAA, B-1, 14-1, B-1
- Hiring practices, 5-7
  - evaluating candidates, 5-9
  - guidelines, 5-8
  - outlining responsibilities, 5-8
  - principle, 5-7
  - screening, 5-8

## I

- Implementing policies, 2-5
  - awareness, 2-6
  - guidelines, 2-6
  - principle, 2-5
- Information management, 9-1
- Information security infrastructure, 3-1
  - coordinating, 3-2
  - facilities, 3-3
  - guidelines, 3-2
  - manageing, 3-2
  - principle, 3-1
  - responsibilities, 3-3
  - third-party, 3-3
- Information technology. *See* IT
- Issue-specific polices, 2-3
- Issue-specific policies
  - applicability, 2-3
  - compliance, 2-3
  - issue-statements, 2-3
  - points of contact, 2-3
  - statement of the institution's position, 2-3
- IT policy
  - definition, 1-1
  - issue specific, 1-2
  - program, 1-2
  - system-specific, 1-2
  - types, 1-2
- IT resources
  - acceptable use, 5-9, 14-1
  - misuse, 12-9
  - reporting and handling security incidents, 5-11
  - reporting security weaknesses, 5-13
  - securing physical entry, 6-2
  - securing the physical perimeter, 6-1
- IT security
  - legislation, B-1
- IT security principles, 1-3, 1-4

## K

- Key encryption, 13-5

## L

- Legal requirements, 14-1
  - acceptable use, 14-1
  - CJIS, 14-1
  - COPPA, 14-1
  - developing awareness, 14-2
  - DMCA, B-1
  - EDUCAUSE, B-2
  - FERPA, 14-1
  - Gramm-Leach Baily Act, 14-1
  - guidelines, 14-1
  - HIPAA, B-1, 14-1, B-1
  - National Strategy for Defending Cyberspace, B-2
  - Patriot Act, B-2
  - principle, 14-1
  - SEVIS, B-1

## M

- Malicious software, 8-6
  - guidelines, 8-6
  - principle, 8-6
- Media disposal, 9-2
  - guidelines, 9-2
  - magnetic/optical, 9-2
  - paper, 9-2
  - principle, 9-2
  - sensitive, 9-2
- Medial disposal
  - developing procedures, 9-3
- Misuse of resources, 12-9

## N

- National Strategy for Defending Cyberspace, B-2
- Network access, 12-5
- Network connection times, 12-8
  - guidelines, 12-9
  - limits, 12-9
  - principle, 12-8
  - time-outs, 12-9
- Network controls, 7-1
  - guidelines, 7-2
  - principle, 7-2
- Network/system access
  - controlling, 12-5
  - network connection, 12-7
  - network services, 12-5
  - service providers, 12-7
  - system utilities, 12-8
  - wireless networks, 12-7
- Networks/system access
  - guidelines, 12-5
  - principle, 12-5

## O

- Operation facilities, 7-2
- Operational change, 7-1
  - guidelines, 7-1
  - principle, 7-1
- Operations management, 7-1
- Operations system documentation, 11-2
- Organizational security, 3-1
- Outsourcing contracts, 3-8
  - guidelines, 3-9
  - principle, 3-8
- Overview, 1-1

## P

- Passwords, 12-3
  - authentication, 12-4
  - changing, 12-5
  - guidelines, 12-4
  - principle, 12-3
  - reviewing policies, 12-5
  - unique, 12-4
- Patriot Act, B-2
- Personnel
  - acceptable use of technology, 5-9
  - disciplinary process, 5-14
  - new hiring policies, 5-7
  - reporting and handling security incidents, 5-11
  - reporting security weaknesses, 5-13
  - training users, 5-11
- Physical perimeter, 6-1
  - equipment security, 6-1
  - identifying, 6-2
  - principle, 6-1
  - securing, 6-1
- Policy
  - access control, 12-1
  - compliance, 14-1
  - developing, 2-1
  - documentation, 11-1
  - documenting, 2-1, 2-4
  - implementing, 2-5
  - reviewing, 2-1, 14-2
- Power supplies, 6-5
  - assessing risk, 6-5
  - emergencies, 6-6
  - guidelines, 6-5
  - power alternatives, 6-5, 6-6
  - principle, 6-5
  - protecting against lightening, 6-6
- Principle
  - acceptable use, 5-9
  - access control, 12-1
  - activity logs, 10-2
  - asset inventory, 4-2
  - asset risk, 4-3
  - back-up, 10-1
  - business continuity, 10-4
  - change control, 13-6
  - classifying assets, 4-1
  - cryptographic techniques, 13-4

- developing policies, 2-3
  - development/operation facilities, 7-2
  - disaster recovery, 10-4
  - disciplinary process, 5-14
  - documentation, 11-1
  - documenting operating procedures, 11-2
  - documenting policies, 2-4
  - electronically-stored information, 9-1
  - e-mail, 8-2
  - equipment re-use/disposal, 6-6
  - equipment sites, 6-4
  - external facilities, 7-3
  - fault logs, 10-3
  - hiring practices, 5-7
  - implementation, 2-5
  - information security infrastructure, 3-1
  - legal requirements, 14-1
  - malicious software, 8-6
  - media disposal, 9-2
  - network connection times, 12-8
  - network controls, 7-2
  - networks/system access, 12-5
  - operational change, 7-1
  - outsourcing contracts, 3-8
  - passwords, 12-3
  - physical perimeter, 6-1
  - power supplies, 6-5
  - publicly available systems, 8-2
  - remote access, 12-11
  - restricted areas, 6-2
  - review and evaluate policies, 2-6
  - reviewing policies, 14-2
  - securing operations system documentation, 11-2
  - security incidents, 5-12
  - security weaknesses, 5-14
  - software exchange agreements, 8-1
  - system acceptance, 8-5
  - system access, 12-9
  - system capacity, 8-4
  - system development/maintenance, 13-1
  - third-party access, 3-4
  - third-party contracts, 3-6
  - training users, 5-11
- Principles
- defined, 1-4
- Program policies, 2-1
- assignment of responsibilities, 2-2
  - compliance, 2-2
  - purpose statement, 2-1
  - scope, 2-2
- Prurpose of document, 1-2
- Publicly available systems, 8-2
- disseminating public information, 8-3
  - e-commerce, 8-4
  - guidelines, 8-3
  - principle, 8-2

## R

- Remote access, 12-11
  - assessing risk, 12-12
  - guidelines, 12-12

- principle, 12-11
- teleworking, 12-12
- training users, 12-13
- Restricted areas, 6-2
  - guidelines, 6-3
  - identification badges, 6-3
  - inspectin luggage and packages, 6-3
  - physical access, 6-3
  - principle, 6-2
  - sensitive information, 6-3
- Reveiwng policies
  - principle, 14-2
- Reviewing and Evaluating policies, 2-6
  - guidelines, 2-7
  - principle, 2-6
  - two-step process, 2-6, 2-7
- Reviewing policies, 2-1, 14-2
  - compliance audits, 14-2
  - guidelines, 14-2
- Risk analysis, 1-3, 4-3
  - access controls, 4-4
  - areas of control, 4-3
  - change control, 4-4
  - critical assets (defining), 4-5
  - instituion-wide security, 4-4
  - segregation of duties, 4-4
  - service continuity, 4-4
  - system software, 4-5
- Risk assessment, 4-6
  - cryptographic techniques, 13-5
  - disaster recovery, 10-4
  - remote access, 12-12
  - sample questions, 4-6
  - unauthorized system use, 12-10
- Risks, 1-3

## S

- Securing the physical perimeter, 6-1
- Security
  - development/operation facilities, 7-2
  - disruptive behavior (BOR policy), A-3
  - e-mail, 8-2
  - equipment reuse/disposal, 6-6
  - equipment sites, 6-4
  - external facilities, 7-3
  - malicious software, 8-6
  - network, 7-1
  - operational change, 7-1
  - organizational, 3-1
  - physical perimeter, 6-1
  - power supplies, 6-5
  - restricted areas, 6-2
- Security incidents, 5-11
  - collecting information, 5-13
  - guidelines, 5-12
  - managing, 5-13
  - principle, 5-12
  - reporting, 5-12
  - sharing information, 5-13
- Security plan, 1-2
- Security weaknesses, 5-13

- awareness, 5-14
  - guidelines, 5-14
  - principle, 5-14
  - user responsibilities, 5-14
- Sensitivity notice, 3
- SEVIS, B-1
- Software exchange agreements, 8-1
  - guidlines, 8-1
  - principle, 8-1
- Software management, 8-1
- System acceptance, 8-5
  - guidelines, 8-5
  - principle, 8-5
- System access, 12-5
  - guidelines, 12-10
  - monitoring, 12-9, 12-10
  - principle, 12-9
  - unauthorized use, 12-10
- System capacity, 8-4
  - guidelines, 8-5
  - principle, 8-4
- System development, 13-1
- System development/maintenance
  - business requirements, 13-1
  - data access, 13-2
  - guidelines, 13-1
  - malicious code, 13-4
  - operational software, 13-3
  - principle, 13-1
  - program source libraries, 13-2
- System maintenance, 13-1
- System management, 8-1
- System-specific policies, 2-2
  - two-step process, 2-2

## T

- Teleworking, 12-12
- Terms
  - glossary of terms, C-1
  - guidelines, 1-4
  - principle, 1-4
  - procedure, 1-4
- Third-party
  - access control, 3-5, 3-7
  - asset protection, 3-7
  - disciplinary process, 5-15
  - equipment management, 3-8
  - liabilities, 3-8
  - personnel management, 3-8
  - service management, 3-7
- Third-party access
  - guidelines, 3-4
  - principle, 3-4
- Third-party contracts
  - guidelines, 3-7
  - principle, 3-6
- Third-party policies
  - contracting, 3-6
  - managing risks, 3-4
- Training users, 5-11
  - acceptable use of software, 5-11

*Index*

acceptable use of systems, 5-11  
guidelines, 5-11

principle, 5-11

## Board of Regents Related Policies

This section explains the Board of Regents (BOR) policies relevant to USG network security. The policies are taken from the following sections:

- 700 Finance and Business
- 1900 Miscellaneous

### *Developing General Policies*

BOR policy section 700 Finance and Business address the responsibility of OIIT and the presidents of individual institutions to create and maintain network security policies and procedures. It also addresses the off-site use of USG equipment. The sections cited here are:

- 712 Computer security policy:
  - 712.01 General policy
  - 712.02 System level activities
  - 712.03 Institutional responsibilities
- 711.09 Home or off-campus use of equipment for business purposes

---

### Computer Security Policy

BOR policy section 712 Computer Security Policy contains the following policies relevant to USG IT security:

Category	Policies
712.01 General Policy	The Board of Regents recognizes that all computer and computer related resources are valuable institution assets and require some degree of protection. The degree of protection needed is based on the nature of the resource and its intended use. The Board also recognizes that while no security procedures will provide for absolute security, all institutions of the system have the responsibility to minimize risk by enacting a computer security or related policy.

Category	Policies
712.02 System Level Activities	<p>A. The Vice Chancellor for Information Technology shall maintain a security plan and guidelines for inter-institutional computer activities.</p> <p>B. The Vice Chancellor for Information Technology shall maintain a computer security implementation guide which the individual units of the USG may choose to use in their individualized implementation schemes.</p>
712.03 Institutional Responsibilities	<p>A. The president of each institution shall be responsible for ensuring that appropriate and auditable security controls are in place on his/her campus.</p> <p>B. Each institution shall develop, implement and maintain a computer security plan which follows guidelines provided by the Office of Information Technology. Institutions should submit the plan to the Office of Information Technology for review and approval.</p> <p>C. The Board recognizes that user education is a vital part of security. Therefore, each institution shall include in its security plan methods for ensuring that information regarding the applicable laws, regulations, guidelines and policies is distributed and readily available to computer users.</p> <p>D. Clear and documented procedures for reporting and handling security violations shall be distributed on each campus. The method of providing this information shall be included in the formal plan.</p> <p>E. The Regents' Central Office, Skidaway Institute, and any other institutions or institutes added to the USG shall develop computer security plans using the same guidelines provided to the institutions (BR Minutes, 1991 – 92, pp. 391 – 392).</p>

---

### Home or Off-Campus Use of Equipment for Business Purposes

BOR policy section 7.1.1 states: Personal property such as portable personal computers or similar items may be removed from a campus to the home of an employee or an off-campus site when the purpose is for business only. Such use shall be tightly controlled, and documentation as to the location and use shall be available at all times (BR Minutes, 1990-91, pp. 378 – 379).

## ***Handling Disruptive Behavior***

BOR policy section 1902 Disruptive Behavior does not specifically mention computer systems or information however, it is relevant to USG IT security.

The policy states: Any student, faculty member, administrator, or employee, acting individually or in concert with others, who clearly obstructs or disrupts, or attempts to obstruct or disrupt any teaching, research, administrative, disciplinary, or public service activity, or any other activity authorized to be discharged or held on any campus of the University System is considered by the Board to have committed an act of gross irresponsibility and shall be subject to disciplinary procedures, possibly resulting in dismissal or termination of employment (BR Minutes, 1968-69, pp. 166 – 168; 1970-71, p. 98.).



## Additional Resources

This appendix briefly describes government acts and legislation that may affect IT security in certain USG facilities. For more information about these issues contact the government agency or refer to government resources on the Internet.

---

### Student and Exchange Visitor Information System (SEVIS)

SEVIS is an Internet-based software application being developed by the Immigration and Naturalization Service (INS) that will provide tracking and monitoring of non-immigrant students (F and M visas) and exchange visitors (J visa) and their dependents. The interactive portion of SEVIS is available as of July 1, 2002. While development and pilot projects have been underway for some time, the Patriot Act of October 2001 requires that SEVIS be fully implemented by all institutions by January 30, 2003. This dramatic acceleration is affecting higher education IT departments, international student offices, and human resources departments working to meet the implementation deadline.

---

### The Digital Millennium Copyright Act (DMCA)

The 1998 enactment of the DMCA represents the most comprehensive reform of United States copyright law in a generation. The DMCA seeks to update United States copyright law for the digital age in preparation of ratification of the World Intellectual Property Organization (WIPO) treaties. Key among the topics included in the DMCA are provisions concerning the circumvention of copyright protection systems, fair use in a digital environment, and online service provider (OSP) liability, including details of safe harbors, damages, and 'notice and takedown' practices.

---

### Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Facilities affected by HIPAA will be required to develop and maintain training to educate their employees, trading partners, contractors, and agents about HIPAA regulations and compliance. They must also demonstrate their efforts to create awareness of HIPAA regulations. These regulations include, but are not limited to, the following:

- Health care information security
- Virus protection
- Risk management
- Media management
- Chain of trust
- Personnel
- Security management
- Incident reporting
- Configuration change management
- Policies and procedures required to comply with HIPAA rules

---

## USA Patriot Act of 2001

This legislation contains several provisions of interest to higher education facilities including sections on electronic surveillance, student records, and biological agents and toxins. The electronic surveillance section broadens the scope of current law to account for new technologies and different modes of communication, such as the Internet, in intelligence surveillance. It also expands and simplifies government's ability to obtain court orders for electronic surveillance. In addition, it identifies some new circumstances in which ISOs may disclose information about suspicious customers or subscribers. In order to address some concerns of civil libertarians with the scope of this legislation, the section pertaining to electronic surveillance would expire in four years (December 2005), if Congress does not pass legislation to renew it. Personnel responsible for developing IT security should consult their institution's attorneys and other appropriate officials for advice about complying with these new laws and responding to queries by law enforcement.

---

## National Strategy for Defending Cyberspace

This strategy will stress the need for cooperation between the public and private sectors in establishing standards and best practices for security information, systems and networks. EDUCAUSE staff members of the Security Task Force are reviewing the National Strategy and the recommendations for higher education.

## Glossary

This appendix defines the terms used in this document.

**Access control list (ACL)** – a table that tells a system what access rights are granted based on a specific identification parameter, such as user ID, network segment, or host name.

**Change management** – a business process to test system changes prior to implementation to avoid unexpected repercussions.

**Criminal Justice Information System Section (CJIS)** – an agency that manages a series of computerized information systems indexes of crime information relating to state and national information security.

**Health Insurance Portability and Accountability Act (HIPAA)** – an act that regulates and governs the privacy, security, and electronic transactions of health care information.

**Information security** – the preservation of the confidentiality, integrity, and availability of information.

**Information system** – the network or combinations of all computing equipment, telecommunication, or other communication or information processing devices and channels used within an organization.

**Private key** – a small, encrypted file used to identify a user with a pass phrase or password. The successful use of the password or phrase allows the decrypting of information from a matching public key. Private keys are also used to create digital signatures that can be decrypted by anyone with the corresponding public key.

**Public key** – a small, encrypted file that contains information about a specific user. The key is supplied by the owner to anyone who wants to encrypt a document or message so that only the public key owner can decrypt it using their private key. For digital signatures, the public key is used to confirm the message was signed by the owner using a private key.

**Risk assessment** – an analysis of potential threats, impacts, and vulnerabilities of information and information systems.

**Teleworking** – the practice of performing regular work duties from a remote site.

**Trojan horse** – software written to allow access to a computer through some method not intended by the system owners. Trojan code is typically embedded in some other form of software that camouflages its presence.

**Users** – employees, contractors, vendors, students, and any other parties granted access to an institution’s systems or applications.