

Valdosta State University
Campus Information Security Plan

Date: November 18, 2004

1. Policy Development, Documentation, and Review	6
1.1 Developing Security Policies	6
1.1.2 Obtain support.....	6
1.1.3 Conduct research.....	6
1.1.4 Purpose Statement.....	6
1.1.5 Scope.....	6
1.1.6 Assignment of responsibilities	6
1.1.7 Compliance	6
1.2 Documenting Security Policies	7
1.2.1 Define policies	7
1.2.2 Define standards.....	7
1.2.3 Define guidelines	7
1.2.4 Define enforcement.....	7
1.2.5 Define exceptions.....	7
1.3 Implementing Security Policies	8
1.3.1 Create awareness.....	8
1.3.2 Maintain awareness.....	8
1.4 Reviewing and Evaluating Policies	8
1.4.1 Review by OIIT	8
1.4.2 Institutional review	8
2. Organizational Security.....	9
2.1 Developing an Information Security Infrastructure	9
2.1.1 General.....	9
2.1.2 Manage information security.....	9
2.1.3 Coordinate information security	9
2.1.4 Guideline Description Coordinate information security, cont	10
2.1.5 Allocate responsibilities	10
2.1.6 Authorize information processing facilities	10
2.1.7 Assess third-parties	10
2.2 Managing Risks from Third-Party Access.....	11
2.2.1 Create security awareness	11
2.2.2 Control access	11
2.2.3 Control on-site access	11
2.2.4 Control remote access	11
2.3 Contracting with Third-Party Entities.....	12
2.3.1 Control access	12
2.3.2 Protect assets.....	12
2.3.3 Manage services	12

2.3.4	Manage liabilities	13
2.3.5	Ensure compliance	13
2.3.6	Secure equipment	13
2.3.7	Manage personnel	13
3.	Asset Classification and Control.....	14
3.1	Classifying Assets	14
3.1.1	Organize assets.....	14
3.1.2	Review relevant information.....	14
3.1.3	Interview personnel.....	14
3.1.4	Conduct surveys	14
3.1.5	Identify interdependencies	15
3.1.6	Classify assets	15
3.2	Developing and Maintaining an Asset Inventory	15
3.3	Analyzing and Assessing Risk	15
3.3.1	Define areas of control.....	15
3.3.2	Identify critical asset elements	16
3.3.3	Define areas of potential compromise	17
3.4	Risk Assessment	17
4.	Personnel Security.....	18
4.1	Hiring New Personnel.....	18
4.1.1	Screen potential employees.....	18
4.1.2	Outline employee responsibilities	18
4.1.3	Evaluate the duties of new employees	19
4.2	Ensuring Acceptable Use of Technology.....	19
4.2.1	Identify inappropriate use	20
4.2.2	Develop appropriate use policies	20
4.2.3	Enforce policies.....	20
4.3	Training Users.....	21
4.3.1	Establish information access	21
4.3.2	Establish acceptable use of software.....	21
4.3.3	Establish acceptable use of systems.....	21
4.4	Reporting and Handling Security Incidents	21
4.4.1	Report incidents	22
4.4.2	Report incidents	22
4.4.3	Manage incidents	22
4.4.4	Collecting and sharing information	23
4.5	Reporting Security Weaknesses.....	23
4.5.1	Develop user awareness	23
4.5.2	Define user responsibilities	23
4.6	Developing a Disciplinary Process	24
4.6.1	Develop a disciplinary process	24
4.6.2	Develop a disciplinary process for third-parties	24
5.	Physical and Environmental Security.....	25
5.1	Securing the Physical Perimeter and Facilities	25
5.1.1	Secure information processing equipment	25
5.1.2	Secure the perimeter and facilities.....	25

5.2 Securing Physical Entry to Restricted Areas	26
5.2.1 Issue institution identification badges.....	26
5.2.2 Restrict physical access.....	27
5.2.3 Secure sensitive information.....	27
5.2.4 Inspect luggage and packages.....	27
5.3 Securing Equipment Sites	27
5.3.1 Secure production systems.....	28
5.3.2 Assure continual service	28
5.4 Securing Power Supplies	28
5.4.1 Assess risk.....	29
5.4.2 Provide limited power alternatives	29
5.4.3 Provide long-term power alternatives.....	29
5.4.4 Prepare for emergencies.....	29
5.4.5 Protect against lightning	30
5.5 Securing Equipment Re-Use or Disposal	30
5.5.1 Delete sensitive information	30
5.5.2 Destroy media	30
6. Operations Management	31
6.1 Securing Operational Change	31
6.2 Developing Network Controls	31
6.3 Separating Development and Operation Facilities	32
6.4 Securing External Facilities Management	32
7. System and Software Management.....	33
7.1 Developing Information and Software Exchange Agreements	33
7.2 Developing Electronic Mail Security.....	33
7.3 Securing Publicly Available Systems	34
7.3.1 Disseminate Institutional information classified as public	34
7.3.2 Secure electronic commerce transactions	34
7.4 Maintaining Adequate System Capacity.....	35
7.5 Ensuring System Acceptance.....	35
7.6 Protecting Against Malicious Software	36
8. Information Management	37
8.1 Handling Information.....	37
8.2 Disposing of Media	37
8.2.1 Identify sensitive media	38
8.2.2 Dispose of paper media.....	38
8.2.3 Cleanse magnetic or optical media	38
8.2.4 Develop disposal procedures	38
9. Back-Up Procedures	39
9.1 Developing Back-Up Procedures.....	39
9.1.1 Develop back-up procedures.....	39
9.1.2 Test the procedures	39
9.2 Maintaining Activity Logs	39
9.2.1 Develop activity logging procedures	39
9.2.2 Use automated logs	40
9.3 Maintaining Fault Logs	40

9.3.1 Use manual fault logging	40
9.3.2 Use automated fault logging	40
9.4 Developing Disaster Recovery and Business Continuity	41
9.4.1 Assess the risks and impacts of an emergency or disaster	41
9.4.2 Develop business continuity	41
10. Documentation.....	42
10.1 Documenting Security Policies, Procedures, Plans, Guidelines, and Standards ..	42
10.2 Documenting Operating Procedures	42
10.2.1 Document operation functions	42
10.2.2 Document system maintenance.....	42
10.3 Securing Operations System Documentation	43
11. Access Control.....	44
11.1 Developing an Access Control Policy	44
11.1.1 Develop privilege management	44
11.1.2 Develop access authorization.....	44
11.1.3 Restrict information access	45
11.2 Managing Passwords	46
11.2.1 Develop unique password and authentication policies	46
11.2.2 Develop password change and review policies	47
11.3 Controlling Access to Networks and Systems	47
11.3.1 Control use of network services.....	47
11.3.2 Control the network connection.....	48
11.3.3 Develop security measures for service providers	49
11.3.4 Develop wireless network access policies	49
11.4 Secure system utilities.....	49
11.5 Controlling Network Connection Times.....	50
11.5.1 Limit connection times	50
11.5.2 Establish session time-outs	50
11.6 Monitoring System Access	51
11.6.1 Assess the risk of unauthorized use	51
11.6.2 Monitor system use	51
11.6.3 Monitor events	52
11.7 Managing Remote Access.....	52
11.7.1 Assess the risk of remote access	52
11.7.2 Assess the benefits of telecommuting	53
11.7.3 Train users.....	53
12. Systems Development and Maintenance	54
12.1 Adhering to Existing Security Requirements	54
12.1.1 Develop business requirements.....	54
12.1.2 Control access to data	54
12.1.3 Control access to program source libraries	55
12.1.4 Control operational software.....	55
12.1.5 Avoid malicious code	56
12.2 Implementing Cryptographic Techniques.....	57
12.2.1 Assess the need for cryptographic techniques	57
12.2.2 Develop key management	57

12.3 Developing Change Control Procedures.....	58
12.3.1 Develop change control for data communications infrastructure	58
12.3.2 Develop change control for software development	58
12.3.3 Develop change control for third-party software	59
12.3.4 Develop change control for operating systems	60
13. Compliance	61
13.1 Complying with Legal Requirements	61
13.1.1 Comply with state and federal regulations	61
13.1.2 Develop acceptable usage policies.....	61
13.1.3 Develop security awareness.....	61
13.2 Reviewing Security Policies and Technical Compliance	62
13.2.1 Develop compliance audits	62
13.2.2 Develop technical compliance audits.....	62

1. Policy Development, Documentation, and Review

1.1 Developing Security Policies

1.1.2 Obtain support

Information Security will obtain a commitment from senior management to enforce security policies. Information Security will establish working relationships between departments, such as Human Resources, Internal Audit, Plant Operations, Budget and Finance, Information Technology and, Legal Affairs. Information Security will establish an approval process to include legal, technology, regulatory specialists, human resources specialists, and policy and procedure experts.

1.1.3 Conduct research

Information Security will communicate with other institution security groups to share successful practices, experiences, and ideas. Each policy will include:

1.1.4 Purpose Statement

Explaining why the program is being established and what information security goals it will address.

1.1.5 Scope

Defining which technology resources are addressed by the program, such as hardware, software, data, personnel, facilities, and peripheral equipment.

1.1.6 Assignment of responsibilities

Defining responsibility for information security program management. Also defines supporting responsibilities for executives, managers, data owners, custodians, and users.

1.1.7 Compliance

Describing how the campus will develop and enforce the program. Also establishes any disciplinary process for breaches of the program policy.

Security Policies can include:

- Program Policies
- Systems Specific Policies
- and/or Issue Specific Policies

1.2 Documenting Security Policies

1.2.1 Define policies

Valdosta State University will define policies by documenting the following information:

- Identify general areas of risk
- State generally how to address the risk
- Provide a basis for verifying compliance through audits
- Outline implementation and enforcement plans
- Balance protection with productivity

1.2.2 Define standards

Valdosta State University will define IT security standards by documenting the following information:

- Define minimum requirements designed to address certain risks
- Define specific requirements that ensure compliance with policies
- Provide a basis for verifying compliance through audits
- Outline implementation and enforcements plans
- Balance protection with productivity

1.2.3 Define guidelines

Valdosta State University will define IT security guidelines by documenting the following information:

- Identify best practices to facilitate compliance
- Provide additional background or other relevant information

1.2.4 Define enforcement

Valdosta State University will define how policies will be enforced by documenting the following information:

- Identify personnel who are authorized to review and investigate breaches of policy
- Identify the means to enforce policies

1.2.5 Define exceptions

Valdosta State University will define the possible exceptions to the IT security policies.

1.3 Implementing Security Policies

1.3.1 Create awareness

Valdosta State University will create user awareness using the following methods:

- Notify employees about the new security policies
- Update employees on the progress of new security policies
- Publish policy documentation electronically and on paper
- Develop descriptive security documentation for users
- Develop user training sessions
- Require new users to sign a security acknowledgement

1.3.2 Maintain awareness

Valdosta State University will maintain user awareness of ongoing and new security issues using the following methods:

- Web site
- Posters
- Newsletters
- E-mail for comments, questions, and suggestions

1.4 Reviewing and Evaluating Policies

1.4.1 Review by OIIT

Information Security will submit policies to O.I.I.T. security team for evaluation and feedback

1.4.2 Institutional review

Valdosta State University will 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

2. Organizational Security

2.1 Developing an Information Security Infrastructure

Valdosta State University will protect information assets by defining assets and the necessary resources. The steps for securing the information infrastructure include:

2.1.1 General

Create an information security organization to take responsibility for all information security issues as described by ISO 17799. Outline clear responsibilities and define organizational roles for information security. These responsibilities and roles will include:

- Forming, reviewing, and approving campus information security
- Maintaining threat assessments for internal information
- Overseeing investigations of security-related incidents
- Overseeing business issues regarding new security initiatives

2.1.2 Manage information security

- Appoint, designate or, hire information security officer(s) for the campus who will address particularly sensitive information security issues.
- Establish an information security office to interface with law enforcement or any legal personnel.

2.1.3 Coordinate information security

Valdosta State University will establish a security taskforce to manage security incidents. The taskforce will include representatives from the following groups:

- Facilities
- Information Technology
- Human resources
- Safety office
- Upper management

2.1.4 Guideline Description Coordinate information security, cont

Valdosta State University will determine if the campus requires multiple subgroups to maintain information security functions for specific departments. Policies and procedures for a multi-level security organization should:

- Define the roles and responsibilities of each group
- Establish methods, procedures, processes, risk assessment, and information classification guidelines.
- Provide information security user education and interface
- Provide security-related technical architecture to plan and develop groups
- Designate security incident investigation responsibility
- Provide identification of an architectural interface to the business management groups

2.1.5 Allocate responsibilities

Valdosta State University will clarify responsibilities for information security-related issues. For each area of security responsibility address the following issues:

- Document access procedures for each individual information system
- Define the owner of each security asset and the access procedures to that asset
- Define authorization levels for access to assets

2.1.6 Authorize information processing facilities

Valdosta State University will 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:

- Assess the ability of the new institution to conform to existing security policies, including any state and federal requirements
- Evaluate hardware and software compatibility of the new facilities with existing facilities
- Evaluate the need for additional security measures and the impact of personal computing systems

2.1.7 Assess third-parties

Valdosta State University will 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. Valdosta State University will maintain contact lists of both internal and external organizations and service vendors. Valdosta State University will define the managers authorized to make decisions regarding security-related events.

2.2 Managing Risks from Third-Party Access

2.2.1 Create security awareness

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.

2.2.2 Control access

Create a user profile for each third-party user that includes the following, minimum criteria:

- Time of day access
- Day of week access
- Physical location access
- Networked location access
- Direct dial in access
- User directory permissions
- User application access

Valdosta State University will implement extra safeguards if a third-party user has access to institutional information.

2.2.3 Control on-site access

- 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.

2.2.4 Control remote access

- Implement tight controls on user accounts using remote logical access.
- Monitor remote connections for abnormal activity.

2.3 Contracting with Third-Party Entities

Valdosta State University will address the following issues regarding third party entities:

2.3.1 Control access

- On-site access contracts will address the following:
 - Third-party responsibility for the actions of its members
 - Third-party responsibility to determine the skills and character of on-site personnel
- Remote access contracts will address the following:
 - Third-party responsibility for the actions of its members
 - Third-party responsibility for the security of connected networks, systems, and logins
- Third-party responsibility to demonstrate ability to meet or exceed normal institution information security policies
- Provisions for granting authorized user access.
- Method for managing authorized user lists and access rights across systems

2.3.2 Protect assets

- Procedures to protect both hard and soft assets.
- 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.

2.3.3 Manage services

- 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.

2.3.4 Manage liabilities

- 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.

2.3.5 Ensure compliance

- 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.

2.3.6 Secure equipment

- Third-party responsibilities regarding hardware and software installation and maintenance.
- Plan for control of malicious software.

2.3.7 Manage personnel

- 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.

3. Asset Classification and Control

3.1 Classifying Assets

Valdosta State University will classify the information assets to determine which information systems, data, facilities, equipment, and personnel constitute the critical information infrastructure of the institution.

3.1.1 Organize assets

Valdosta State University will organize assets into basic categories, such as:

- Data
- Equipment
- Hardware/software
- Personnel
- Facilities
- Operations

3.1.2 Review relevant information

Valdosta State University will review reports, databases, and documents with information about personnel, information and equipment.

3.1.3 Interview personnel

Valdosta State University will interview personnel, such as managers, customers, suppliers, users, and others to as necessary to help determine critical assets.

3.1.4 Conduct surveys

Valdosta State University will develop survey questions to identify critical assets, such as:

- What are the mission critical or sensitive activities and/or operations?
- Where is critical or sensitive information stored or processed?
- Where are the mission critical or high value equipment or material located (onsite or off)?
- What kind of physical security, access control, and other protective measures are in place in these locations?
- What impact would a lost or damaged asset have on critical mission functions, operations, and customers?

3.1.5 Identify interdependencies

Valdosta State University will identify interdependencies among the components of individual systems and the overall infrastructure.

3.1.6 Classify assets

Valdosta State University will classify assets based on findings. Typically, the more goals an asset supports the more important it is.

3.2 Developing and Maintaining an Asset Inventory

VSU will 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. Asset inventories will allow the 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 will be removed from the inventory lists in accordance with institutional asset management procedures.

3.3 Analyzing and Assessing Risk

Valdosta State University will identify and document the vulnerabilities and risks associated with its critical assets. The guidelines for analyzing risk to critical IT assets are:

3.3.1 Define areas of control

- General Define the policies, procedures, practices, and organizational structures designed to ensure business objectives are achieved and undesired events are detected and prevented.
- Campus wide security
- Define a security framework and continuing cycle of activity to achieve the following:
 - Manage risk
 - Develop security policies
 - Assign responsibilities
 - Evaluate physical and information controls

- Develop program policies to achieve campus-wide security by accomplishing the following:
 - Assess risk
 - Develop and implement effective security procedures
 - Evaluate the effectiveness of procedures
- Define procedures and controls that limit or detect access to critical IT assets. Access controls include the following:
 - Physical controls – limit physical access to critical equipment
 - Technical controls – security measures, such as security software programs, designed to detect and prevent unauthorized access to critical IT assets
- Develop policies, procedures, and a segregated organizational structure to ensure no single individual controls all key aspects of IT operations.
- Develop a comprehensive contingency plan to ensure the following:
 - Availability of critical services and operations.
 - Protection of sensitive data
- Develop policies and controls to prevent users from implementing unauthorized programs or modifying existing programs.
- Develop policies and controls to ensure that authorized changes will not interrupt critical services and operations.
- 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:
 - System software access control
 - Monitor procedures
 - Change control procedures

3.3.2 Identify critical asset elements

- 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.
- Identify the electronic and telecommunication equipment, hardware, and software safeguards that support critical IT assets.

- Identify the non-automated systems, internal and external, that support critical IT assets, such as:
 - Paper archives
 - Personnel
 - Accounting procedures
- 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:
 - Accessed by personnel
 - Stored in or processed by a computer
 - Transmitted digitally
- Identify the facilities and equipment that support and house critical IT assets.

3.3.3 Define areas of potential compromise

- 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 of resources essential to critical IT assets.

3.4 Risk Assessment

Valdosta State University will develop and perform a Risk Assessment that addresses the following criteria:

- Can vulnerability in question be better minimized with physical or technology 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 technology advances in the near future?

4. Personnel Security

4.1 Hiring New Personnel

When hiring new personnel, Valdosta State University Information Security will coordinate with other Valdosta State University departments to implement security procedures to minimize the risks of human error, fraud, and misuse of resources. Security concerns will be addressed as early as the recruitment stage. Valdosta State University will screen, educate, and train prospective employees who will be granted access to Valdosta State University information systems by using the following guidelines:

4.1.1 Screen potential employees

- 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:
 - Character references (business and personal)
 - Training background
 - Academic and professional experience
 - Identity and background checks
 - Credit checks
- Conduct a re-screening if there is cause for doubt or concern.
- Repeat these checks in cases of job change, role change, and promotion.

4.1.2 Outline employee responsibilities

- Identify the degree of access to institution information systems, processes, and data in job descriptions.
- Define the following for new employees:
 - Official Code of Georgia Annotated Computer Security Act
 - Applicable state and federal regulations
 - Terms of confidentiality
 - Security conditions of employment
 - Normal administrative processes
- Define the security issues that are part of the terms and conditions of employment.

- Implement annual security training for all employees that includes:
 - Security awareness
 - Security policies and procedures updates
 - Reporting procedures for security incidents and vulnerabilities

- Create confidentiality and non-disclosure agreements to be signed by new employees who will be accessing sensitive information.

- Educate all employees of the disciplinary action or criminal charges that may result if security policies are violated.

4.1.3 Evaluate the duties of new employees

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.

4.2 Ensuring Acceptable Use of Technology

Valdosta State University will insure the appropriate use of its technology resources utilizing the following guidelines:

4.2.1 Identify inappropriate use

Identify inappropriate use of IT resources. Inappropriate use includes, but is not limited to, the following:

- Private or personal for-profit activities, such as personal business transactions or advertising
- Unauthorized, not-for-profit business activities
- Illegal activities as defined by federal, state, and local laws and regulations
- Creation, accession, or transmission of pornographic or obscene material
- Creation, accession, or transmission of material that could be considered discriminatory, offensive, threatening, harassing, or intimidating
- Creation, accession, or participation in online gambling
- Infringement of any copyright, trademark, patent, or other intellectual property rights
- Activity that could cause the loss, corruption of, or prevention of rightful access to data or the degradation of IT performance
- Activity or solicitation for political or religious causes
- Unauthorized use of another employee's access
- Modifying or removing computer equipment, software, or peripherals without proper authorization
- Creation, accession, or transmission of material to libel or otherwise defame any person

4.2.2 Develop appropriate use policies

- Define appropriate use of all institutional systems and equipment.
- Implement policies in the following ways:
 - Restrict access to authorized users
 - Train users in appropriate use

4.2.3 Enforce policies

Develop procedures to pursue disciplinary action, termination, or criminal prosecution in cases of violation.

4.3 Training Users

Valdosta State University will provide information security training to its employees, faculty, and students. Training will be developed with input from Human Resources and the Legal Affairs department. Completed training will be documented. Suggested guidelines are:

4.3.1 Establish information access

- 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:
 - Acceptable and unacceptable access
 - Access controls and legal responsibilities
 - Vigilance of fraudulent activities
 - Procedures to report security incidents or vulnerabilities

4.3.2 Establish acceptable use of software

- 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.

4.3.3 Establish acceptable use of systems

Train all users on the acceptable use of new systems.

4.4 Reporting and Handling Security Incidents

Valdosta State University will implement procedures for reporting and handling information security incidents. All users will be trained to report incidents in accordance with policy.

4.4.1 Report incidents

- Develop a process for users to report breaches of security and other incidents to the appropriate personnel. The report should include the following:
 - Incident type
 - Severity level
 - Access details
 - Involvement
- Develop user training to address the following:
 - Incident reporting process
 - Awareness of historical incidents in order to avoid future occurrences
- 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.

4.4.2 Report incidents

Develop a feedback process to inform users who report a breach of security when the incident is closed.

4.4.3 Manage incidents

- 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:
 - System administrators
 - Management
 - All parties responsible for security
- Develop escalation procedures that include multiple escalation points, depending on the severity of the incident, so that evidence can be collected and the correction 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.

4.4.4 Collecting and sharing information

- 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:
 - Type of incident
 - Severity level
 - Cost of incident
 - Scope of incident
 - Resolution
- 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.

4.5 Reporting Security Weaknesses

Valdosta State University will develop procedures for users to report vulnerabilities in, or threats to, the information and communication systems.

4.5.1 Develop user awareness

Instill a sense of urgency in users to report security vulnerabilities and potential threats to the designated security administrator.

4.5.2 Define user responsibilities

- 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 not attempt to test a weakness before reporting it.

4.6 Developing a Disciplinary Process

Valdosta State University will implement disciplinary procedures for users who intentionally breach security.

4.6.1 Develop a disciplinary process

- Develop specific disciplinary actions for the following:
 - State employees
 - Students
 - Contractors
 - Vendors
- 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.

4.6.2 Develop a disciplinary process for third-parties

- 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 institution's security procedures.

5. Physical and Environmental Security

5.1 Securing the Physical Perimeter and Facilities

Valdosta State University will implement procedures and physical security measures to prevent and detect unauthorized access or damage to facilities that contain Valdosta State University information systems. Suggested guidelines are:

5.1.1 Secure information processing equipment

Ensure that the location of information processing facilities is confidential. Important safeguards are:

- No signs indicating locations
- No public access to directories and telephone books that identify locations

Place all printers, copiers, and fax machines in secured areas to prevent unauthorized duplication and transmission of sensitive information.

5.1.2 Secure the perimeter and facilities

- Identify the perimeter of all information processing facilities and perform a risk analysis of its physical security.
- Ensure that information processing facilities meet local building codes for structural stability, such as:
 - External walls
 - Internal walls
 - Ceilings
 - Doors
- Ensure that walls surrounding sensitive areas extend from true floor to true ceiling.
- Secure doors by ensuring the following:
 - Doors to sensitive areas should close automatically and trigger an audible alarm when they have been kept open beyond a certain period of time
 - Fire doors in sensitive areas should trigger an audible alarm when the crash bar is used
- Install appropriate control mechanisms, such as locks, alarms, and bars.

- Prevent unauthorized personnel from seeing or hearing information processing equipment.
- Equip all sensitive areas with fire, water, and physical intrusion alarm systems that automatically alert the appropriate personnel.
- Provide additional security for the most sensitive areas of information processing facilities.

5.2 Securing Physical Entry to Restricted Areas

Valdosta State University will restrict access to areas within facilities that house sensitive or critical Valdosta State University information systems.

5.2.1 Issue institution identification badges

- Implement a badge system for sensitive areas. Badges should contain identifying information such as:
 - Name
 - Photograph
 - Job title
 - Level of building access
- Implement an entry system that requires a badge check prior to entry. Checks can be performed by the following:
 - Receptionists
 - Desk attendants
 - Security guards
 - Electronic card readers
- Maintain entry logs.
- Train users to challenge anyone in a restricted area who is not wearing a badge.
- Review and update access rights to restricted areas regularly.

5.2.2 Restrict physical access

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:

- Receptionists
- Metal key locks
- Magnetic card door locks

5.2.3 Secure sensitive information

Secure sensitive information, either in paper or electronic format, from unauthorized access and disclosure as follows:

- Paper in unattended locations should be locked in safes, file cabinets, or other appropriate containers.
- Desks should be clear during non-working hours.
- Electronic information should be secured through passwords and physical security of areas where it resides.

5.2.4 Inspect luggage and packages

Inspect user's luggage and packages as necessary to safeguard and deter theft of sensitive equipment and information.

5.3 Securing Equipment Sites

Information Security will protect critical Valdosta State University computer and communications equipment from physical and environmental threats.

5.3.1 Secure production systems

- Place production systems in a physically secured area. Production systems include the following:
 - Servers
 - Hubs
 - Routers
 - Voicemail systems

- Train users about their responsibility to protect equipment by avoiding the following behaviors in workstation areas:
 - Eating
 - Drinking
 - Smoking

5.3.2 Assure continual service

Provide security controls that alert, monitor, and log the following threats:

- Intrusions
- Fires
- Explosives
- Smoke
- Water
- Dust
- Vibrations
- Chemical and electrical effects
- Electrical supply interferences
- Electromagnetic radiation

5.4 Securing Power Supplies

Valdosta State University will, within practical limitations, provide continuous power to maintain the availability of critical equipment and information systems.

5.4.1 Assess risk

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:

- How critical is this system to public safety?
- How critical is this system to regular campus operations?
- How critical is this system to information security?
- Is it necessary that this system continue to operate in the event of a power failure?
- Can this system be shut down until power is restored without affecting any major or critical campus operations?

5.4.2 Provide limited power alternatives

- Use uninterruptible power supply (UPS) systems for brief power interruptions or to allow time for the orderly shutdown of systems for prolonged power outages.
- 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.

5.4.3 Provide long-term power alternatives

- 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.

5.4.4 Prepare for emergencies

- 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.

5.4.5 Protect against lightning

- Provide lightning protections to all critical facilities.
- Provide lightning protection filters to all external communications lines.

5.5 Securing Equipment Re-Use or Disposal

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

5.5.1 Delete sensitive information

Implement procedures to render the institutions information unrecoverable before allowing the re-use or disposal of equipment.

5.5.2 Destroy media

- Implement procedures to destroy defective or damaged media containing sensitive information before allowing the re-use or disposal of equipment.
Media may include:
 - Floppy disks
 - Compact disks
 - Tapes
 - Hard drives
- Implement procedures to shred hard copies of sensitive information.

6. Operations Management

6.1 Securing Operational Change

Valdosta State University will control all changes to information processing facilities, systems, software, and procedures as necessary to implement a formal change management process to maintain system security. Suggested guidelines for securing operational change include:

- 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

6.2 Developing Network Controls

Valdosta State University will establish controls to ensure the security of the networks it operates to ensure the security of Valdosta State University information and connected services. To achieve and maintain security on computer networks a range of controls must be utilized. The common objective of these controls will 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

6.3 Separating Development and Operation Facilities

Valdosta State University will separate operation computing environments from development and test computing environments to help reduce the risk of one environment adversely affecting another. 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 will require management approval

6.4 Securing External Facilities Management

Valdosta State University will work with the Legal Affairs Department to establish contractual controls to reduce security risks from external contractors that manage information processing facilities. Guidelines for securing external facilities management include:

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

7. System and Software Management

7.1 Developing Information and Software Exchange Agreements

Valdosta State University will implement agreements for the exchange of information with external organizations. The agreement will exist whether the information is in electronic or physical form. The content of the agreement(s) will vary depending on the reason for the exchange. Guidelines for exchange agreement(s) 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

7.2 Developing Electronic Mail Security

Valdosta State University will develop an acceptable use policy for their IT resources and actively monitor the network for compliance with state and federal regulations.

Guidelines for securing e-mail are:

- Implement user identification and defensive systems against email 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 as necessary 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 repudiate authentication
- Implement signed agreements by users for acceptable use and inspection of emails without the expectation of privacy

7.3 Securing Publicly Available Systems

Valdosta State University will provide public access to Valdosta State University electronic information resources in accordance with the safeguards used to protect Valdosta State University resources.

7.3.1 Disseminate Institutional information classified as public

- 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.

7.3.2 Secure electronic commerce transactions

- 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:
 - Internal/External system
 - Security policy
 - Hypertext link integrity
 - CGI
 - Server identification
 - Responding ports on the server IP address
 - Know subversions based on server technology
 - Observable IP networks from the Internet
 - Memory bounding and exception handling
 - Change controls
 - User accounts
 - Backup and recovery
 - Intrusion detection
 - Unauthorized changes
 - DMZ penetration

7.4 Maintaining Adequate System Capacity

Valdosta State University will monitor current and future system capacity requirements to ensure continuous and adequate power, bandwidth, and storage providing adequate system capacity for future information system requirements. Guidelines for maintaining adequate system capacity include:

- 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

7.5 Ensuring System Acceptance

Valdosta State University will define, document, and utilize the necessary system acceptance criteria for all new information systems and system upgrades to avoid system failure due to inadequate testing and validation acceptance of new or upgraded information systems. 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

7.6 Protecting Against Malicious Software

Valdosta State University will use prevention and detection controls and create security awareness among its users to protect information systems and services against malicious software such as:

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

Guidelines for protecting institutional systems include:

- 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

8. Information Management

8.1 Handling Information

Valdosta State University will establish internal procedures for the secure handling and storage of its electronically-stored information to prevent unauthorized access or misuse. Guidelines for handling electronically-stored information include:

- 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

8.2 Disposing of Media

Valdosta State University will develop a media disposal process based on the sensitivity of the data as determined by law and the data owners to render information unrecoverable before disposing of media.

8.2.1 Identify sensitive media

Sensitive media that require secure disposal include any media that contains sensitive institution information, such as:

- Paper documents
- Output reports
- System documentation
- Program listings
- Removable disks or cassettes
- Recordings
- Magnetic tapes
- Optical storage media
- Test data

8.2.2 Dispose of paper media

Develop procedures to incinerate or shred sensitive paper media.

8.2.3 Cleanse magnetic or optical media

Develop procedures to cleanse magnetic or optical media before re-use. Consider using software designed to securely erase and reformat the media.

8.2.4 Develop disposal procedures

- 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.

9. Back-Up Procedures

9.1 Developing Back-Up Procedures

Valdosta State University will develop back-up and test procedures for all essential, electronically-stored business data.

9.1.1 Develop back-up procedures

- 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.

9.1.2 Test the procedures

- 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. Example: 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.

9.2 Maintaining Activity Logs

Valdosta State University will maintain appropriate activity logs for critical information systems.

9.2.1 Develop activity logging procedures

- Create activity logs which include the following:
 - Start and finish date and time for system activity
 - System errors and corrective action taken
 - Confirmation of proper handling of media
 - Name of the person making the log entry
- Store logs in a secure place.
- Develop procedures to review the logs regularly.

9.2.2 Use automated logs

- Implement automated logging whenever possible.
- Configure automatic logs to record the following:
 - System utilization
 - System errors and corrective actions taken
 - Communication session statistics
 - Successful and unsuccessful logins

9.3 Maintaining Fault Logs

Valdosta State University will maintain fault logs for information systems and services to be used to trace system activity and errors.

9.3.1 Use manual fault logging

- Develop procedures for personnel who monitor system operations to maintain a fault log.
- Create logging procedures to include:
 - Date and time of log entry
 - Description of fault and corrective actions taken
 - Name of the person making the log entry
 - Review and confirmation of proper handling of fault
 - Review and corrective measures to ensure that controls have not been compromised

9.3.2 Use automated fault logging

- Implement automated logging whenever possible.
- Configure automatic logs to record the following:
 - System utilization
 - System errors and corrective actions taken
 - Communication session statistics
 - Successful and unsuccessful logins

9.4 Developing Disaster Recovery and Business Continuity

Valdosta State University will 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.

9.4.1 Assess the risks and impacts of an emergency or disaster

- 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.

9.4.2 Develop business continuity

- 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.

10. Documentation

10.1 Documenting Security Policies, Procedures, Plans, Guidelines, and Standards

Valdosta State University will document its agreed upon Information Security policies, procedures, plans, guidelines, and standards.

The procedures, plans, guidelines, and standards used to enforce Valdosta State University policies will be documented and disseminated to the appropriate managers and users.

10.2 Documenting Operating Procedures

Valdosta State University will document operating responsibilities and procedures for Valdosta State University information processing facilities. Guidelines for documenting operational procedures include:

10.2.1 Document operation functions

Document specific instructions for operation functions, such as:

- Handling and processing information
- Scheduling requirements
- Handling exceptions or errors
- Contacting technical support if necessary
- Handling data processing output and disposal of output from failed jobs
- Restart and recovery after a system failure
- Responding to incidents
- Recovering from disasters
- Access approval methods

10.2.2 Document system maintenance

Document the typical system maintenance activities, such as:

- Start/stop procedures
- System back-up
- Equipment maintenance procedures and time windows
- Computer room management and safety
- Mail handling management and safety

10.3 Securing Operations System Documentation

Valdosta State University will develop procedures to secure operational system documentation from unauthorized access. Guidelines for securing operational system documentation include:

- 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

11. Access Control

11.1 Developing an Access Control Policy

Valdosta State University will control access to information systems. All sensitive Valdosta State University information will be protected from improper disclosure, modification, and deletion.

11.1.1 Develop privilege management

- 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.

11.1.2 Develop access authorization

- Appoint supervisors or managers to be responsible for:
 - Granting access to information on a 'need to know' criteria of the information owners
 - Creating user identifications (IDs) and passwords
 - Deleting user permissions
 - Changing user permissions
- 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.
- 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.
- Develop user responsibilities that users agree to before receiving user IDs. Users should physically or electronically sign the following agreements:
 - Confidentiality
 - Information system security

- 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:
 - Allowing others to use their ID
 - Using someone else's ID

11.1.3 Restrict information access

- Ensure that application access is granted to authorized users, only.
- Assign the following user access rights based on job functions:
 - Read
 - Write
 - Execute
 - Delete
- 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.
- Develop appropriate access policies for:
 - Custom application software
 - Software utilities

11.2 Managing Passwords

Valdosta State University will develop password management to control access to information resources. Guidelines for password management include:

11.2.1 Develop unique password and authentication policies

- 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:
 - User level accounts
 - Web accounts
 - E-mail accounts
 - Screen saver protection
 - Voicemail accounts
 - Local router logins
- Develop strong password construction as a first line of defense against improper access. Strong passwords typically exhibit the following characteristics:
 - At least 8 alphanumeric characters
 - Upper and lower case characters
 - Digits and special characters as well as letters, such as numbers (0-9) and other characters (!@#%&)
 - No identifiable words in any language, slang, dialect, or jargon
 - No personal information, such as family names
 - No null passwords or passwords which are the same as the user ID
- Ensure that all applications support the following:
 - Authentication of individual users, not groups
 - Role management that allows one user to take over the functions of another without a password
 - Password integrity by not storing passwords in clear text or any reversible form
- Develop a one-time password authentication or a public/private key system with a strong pass phrase for remote access users.

11.2.2 Develop password change and review policies

- 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:
 - System-level passwords - monthly
 - User-level passwords - every 45 days
- 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 user should change it immediately.

11.3 Controlling Access to Networks and Systems

Valdosta State University will control access to its networks, systems, and resources to ensure only authorized users gain access based on their level of authorization. Strategies for access control include:

11.3.1 Control use of network services

- Control the use of the institution's network services by developing procedures to:
 - Verify user identity through institution issued user IDs linked to a confidential password
 - Develop an authentication system for internal networks that store sensitive institution information
 - Protect in-bound connections to networks with a dynamic password access control system
- Control third-party and public access to institutional network services by developing procedures to:
 - Gain approval of security and access administration before granting third-party access
 - Protect institutional networks connected to the Internet with an access control system
 - Protect outbound connections initiated from institution offices by routing them through systems expressly established to provide secure network access
 - Encrypt all links that allow access to sensitive institution information outside the network
 - Avoid shared file systems between internal and external systems

- Install and enable anti-virus programs on all web servers, LAN servers, mail servers, and networked PCs
 - Develop session time-outs for systems accepting remote connections from public networks, such as dial-up phone network or the Internet
 - Use login banners on all networks and computers that are directly accessible through external networks
 - Maintain system logs on all networks and computers which interface with external networks. Logs should indicate time, date, identity, and activity
 - Implement control mechanisms on all networks connected to external networks
 - Apply authentication to host systems that accept automatic connections from remote computers, such as Virtual Private Networks (VPN) and remote access services
 - Use remote diagnostic port protection
- Segregate large networks that cross organizational boundaries with separate logical domains, each protected with suitable security perimeters and access controls.
 - 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.

11.3.2 Control the network connection

- Develop additional access control for in-bound connections to internal institution networks and systems through external sources.
- 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.
- 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.
- 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.
- Apply proper access control lists to communication devices such as firewalls, routers, and servers to prevent unauthorized access.
- Disable unused ports.

11.3.3 Develop security measures for service providers

- Review all documentation for a system prior to using service providers to avoid disclosing confidential information.
- Note: Service providers acting as common carriers assume no responsibility for institutional information.
- Sign security agreements with potential service providers who will handle institutional information.

11.3.4 Develop wireless network access policies

- Develop operating system hardening to include the following:
 - Removal of default shares, such as C\$
 - Strong administrator passwords
 - No unnecessary services/applications running on machines
- Employ secure transmissions.

11.4 Secure system utilities

- Develop policies to secure system utilities that:
 - Employ user authentication of all system level utilities
 - Segregate utilities from other general user executables
 - Limit the use of system utilities to a subset of authorized users with specific training and privileged user access
 - Use system utility logging
 - Develop documentation to describe system utilities and their purposes
 - Harden the operation system to remove unnecessary utilities
 - Place time constraints on the use of system utilities
- 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

11.5 Controlling Network Connection Times

Valdosta State University will control network connectivity. This includes restricting user utilization, such as bandwidth usage, limiting the time and dates when user connections are accepted and, automatically log users off after a period of inactivity. Strategies for network connection control include:

11.5.1 Limit connection times

- 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.

11.5.2 Establish session time-outs

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:

- Level of risk associated with a logged in session
- Sensitivity of data

11.6 Monitoring System Access

Valdosta State University will develop a plan to audit its systems to monitor the activities of system users. Guidelines for monitoring system access are:

11.6.1 Assess the risk of unauthorized use

Determine the risk of unauthorized use of a system with a risk assessment. The assessment should consider the following:

- Authorized access:
 - User ID
 - Date and time of key events
 - Types of events
 - Files or resources accessed
 - Program, utilities, and applications
- Privileged operations:
 - Supervisor account use
 - System start and stop activity
 - I/O device attachment/detachment
- Unauthorized access attempts:
 - Failed attempts
 - Access policy violations and notifications network gateways and firewalls
 - Alerts from proprietary intrusion detection systems
- System alerts or failures:
 - Console alerts or messages
 - System log exceptions
 - Network management alarms

11.6.2 Monitor system use

- Develop monitoring procedures based on the findings of the risk assessment. These procedures should facilitate the discovery of attempts at unauthorized use.
- Develop a system to maintain and regularly review log files. Secure log files to prevent alterations.

11.6.3 Monitor events

- Develop a system to monitor logging events to contain the following, at a minimum:
 - User ID
 - Dates and times of login and logoff
 - Login method, location, terminal identity, network address
 - Records of successful and unsuccessful system access attempts
 - Records of successful and rejected data access and other resource access attempts
- 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.
- Develop a system to maintain data access event logs and correlate the information with system access logs.

11.7 Managing Remote Access

Valdosta State University will manage remote access to its networks, systems, and their resources. Guidelines for managing remote access are:

11.7.1 Assess the risk of remote access

- 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.

11.7.2 Assess the benefits of telecommuting

Determine if telecommuting will benefit an organization by considering the following:

- Can the telecommuting site meet current physical security requirements for internal systems?
- Will the proposed telecommuting environment promote staff productivity?
- Are the networking and communications systems reliable, robust, and secure enough to meet current security requirements for data communications?
- Is physical access to the telecommuting environment secure enough to ensure no compromise of the computing resources connected to it?
- Does the telecommuting environment provide sufficient, secure storage space for materials and equipment?
- Does the local environment have provisions for securing any unused network connections into the networked infrastructure?
- Does the telecommuting environment have timely procedures for revoking access to its facilities as needed?

11.7.3 Train users

Train users about their responsibility for the security of remote access connections.

Responsibilities include:

- Physical security of a connected laptop
- Security of the information on a laptop
- Cryptographic data storage and appropriate uses of cryptographic techniques
- Awareness of 'overlooking', such as a person watching a users logon sequence or seeing proprietary information

12. Systems Development and Maintenance

12.1 Adhering to Existing Security Requirements

Valdosta State University will ensure that all system development and maintenance adhere to existing security requirements. Business requirements for system development will specify and define the necessary system controls based on existing policy. Guidelines for adhering to existing security policies when developing or updating systems are:

12.1.1 Develop business requirements

- Develop business requirements that include specifications for security controls before developing new systems or updating existing ones. Specifications should include requirements for the following:
 - Automated controls
 - Manual controls
 - ‘Off the shelf’ controls
- Analyze the security needs of a new or updated system. Business requirements should address the following security concerns:
 - Types of risk associated with the system
 - Sensitivity of the information handled by the system
 - Pertinent data security standards that may affect security, such as HIPAA

12.1.2 Control access to data

- Control access to data in new or updated systems based on existing security requirements. Data access requirements should address the following:
 - Ownership of data
 - Sensitivity of data
- 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:
 - Perform tests on operational data only when required safeguards for that data are in place
 - Obtain authorization each time operational information is copied to a test application system
 - Erase operational information from the test application immediately after testing
 - Log all events that involve copying and using operational information

12.1.3 Control access to program source libraries

- Remove program source libraries from production systems unless it is required.
- Note: Removed libraries should be archived and labeled with the exact version of the software.

- Control access to program source libraries that remain on the system. Consider the following:
 - Appoint a program source librarian or administrator
 - Restrict access by IT support staff
 - Avoid storing programs under development or maintenance in production program source libraries
 - Obtain authorization from the IT support manager for an application before updating program source libraries or issuing program sources to programmers
 - Keep program listings in a secure environment
 - Maintain an audit log for all program source libraries
 - Avoid multiple updates to production modules between backups
 - Archive old versions of source programs and label them clearly
 - Apply strict change control procedures to program source libraries

12.1.4 Control operational software

- Develop business requirements that prohibit the use of unapproved or unlicensed software. Periodically audit the software on desktop systems.

- Develop strict change management processes for production systems. Approvals for change at the operating system level should include security administration.

- Minimize operating system files to only those files required for the purpose for which the system is designed.

- Audit operating system files for authenticity and directory structures before placing the system into change management.

- Develop a regular audit schedule for production systems to monitor changes during operation.

- 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.

- Obtain approval from the application owners before placing static data under change management.
- Establish roll-back plans and event logging for all change control operations.
- Establish controls for production and operational systems that include the following:
 - Operation program libraries should be updated by the designated administrator only after receiving appropriate change management approval
 - Production systems should only hold operationally relevant code and data
 - Executable code should not be installed on a production system until it is successfully tested
 - An audit log should be maintained to record all updates to operational system files
 - Previous versions of software should be retained as a contingency measure

12.1.5 Avoid malicious code

- 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:
 - Buy programs from reputable sources, only
 - Buy programs with verifiable source code
 - Use evaluated, third-party products
 - Inspect all source code before use
 - Control access to code once installed
 - Screen users before allowing them access to key systems
 - Establish security policies regarding e-mail attachments and e-mail from unknown sources
- 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.
- Train users about their responsibilities to avoid malicious code. Responsibilities should include the following:
 - Use safe practices while connected to the Internet through an institutional network
 - Avoid 'open-source' software available over the Internet unless approved by management
 - Avoid opening e-mail attachments from unknown sources unless the it has been screen with antivirus software

12.2 Implementing Cryptographic Techniques

Valdosta State University will implement cryptographic techniques for sensitive systems as needed. Guidelines for implementing cryptographic techniques include:

12.2.1 Assess the need for cryptographic techniques

- Determine the need for cryptographic techniques by conducting a risk assessment on the system.
- Select a cryptographic technique based on the following:
 - Risks
 - Type of key management required
 - Level of data classification
 - Responsible parties for implementation and key management
 - Compatibility of existing data storage systems
 - Import and export laws regarding encryption technology

12.2.2 Develop key management

- Develop policies to manage the electronic cryptographic keys if necessary. Types of key encryption are:
 - Symmetric
 - Public
 - Private
- Protect keys from modification and destruction. Private keys require protection from unauthorized disclosure.
- Create defined activation and deactivation of keys.
- 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.
- Ensure that key management is based on existing security standards. Key management policies should include the following:
 - Generate keys for different cryptographic systems and different applications
 - Generate and obtain public key certificates
 - Distribute keys to intended users with complete instructions
 - Store keys in secure areas
 - Update the key management rules when keys are changed
 - Develop procedures for handling compromised keys

- Develop procedures to revoke and deactivate keys when necessary
- Develop procedures to archive keys when the user terminates employment
- Develop procedures to recover lost or corrupted keys
- Develop procedures for key destruction
- Log and audit key management activities

12.3 Developing Change Control Procedures

Valdosta State University will develop change control procedures before upgrading or changing operating systems and software to avoid security risks and disruption.

Guidelines for developing change control are:

12.3.1 Develop change control for data communications infrastructure

- Develop a change control process that ensures continued availability of communications resources.
- Document all change control processes and assign staff responsibilities as necessary.
- Develop a review process to determine the quality of change controls.

12.3.2 Develop change control for software development

- Develop a change control process that prevents unauthorized access to software design, code, libraries, and databases.
- Document all change control processes and assign staff responsibilities as necessary.
- Develop a review process to determine the quality of change controls.
- Develop change control for mainframe systems that include the following:
 - Maintain a record of agreed authorization levels
 - Ensure changes are submitted by authorized users
 - Review controls and the integrity of procedures to ensure that they will not be compromised by the changes
 - Identify all computer software, information, database entities, and hardware that will change
 - Obtain formal approval for detailed proposals before work commences
 - Ensure the authorized user accepts changes prior to implementation
 - Ensure the implementation is carried out to minimize disruptions
 - Update system documentation

- Archive old documentation
 - Maintain version control of all software updates
 - Maintain an audit trail of all change requests
- Ensure the security of software development for midrange and small servers by following the same change control procedures for larger systems.
 - Document the new mid-range or small server application. Include the following:
 - Function or purpose
 - Special tuning requirements
 - User account requirements
 - File and directory structures
 - Super user account requirements
 - Account and file permissions
 - Network ports
 - System library requirements and versions
 - Device file requirements
 - Data storage requirements
 - Kernel changes
 - Scheduled tasks
 - Develop change control for desktop software to include the following:
 - Test the install or upgrade on all types use desktops that will be affected
 - Notify users and help-desk staff prior to the change to minimize disruption
 - Develop automated or server-based installs to minimize disruption
 - Provide extra on-call support during the change
 - Follow-up with users to ensure that the change was successful

12.3.3 Develop change control for third-party software

- 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.
- Document all change control processes and assign staff responsibilities as necessary.
- Develop change control procedures for modifying third-party software if necessary. If it is necessary to modify a software package, consider the following:
 - Risk of built-in controls

- Risk to integrity controls
- Legality of changes without vendor consent
- Responsibility for future maintenance as a result of modification
- Undetected security compromises

12.3.4 Develop change control for operating systems

- Develop a change control process for operating system upgrades, such as the installation of security patches, performance patches, and maintenance upgrades.
- Document all change control processes and assign staff responsibilities as necessary.
- Develop a review process to determine the quality of change controls.
- 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.
- Backup the existing system and databases just prior to a new installation or upgrade.
- Schedule installations and upgrades at times that will have the minimum impact on business operations and notify all affected parties of any downtime.
- 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.
- 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:
 - Review of application controls and integrity procedures to ensure they have not been compromised by the changes
 - Ensure the annual support plan and budget cover reviews and system testing
 - Notify administrators of changes in time for appropriate reviews before implementation
 - Make appropriate changes to business continuity plans

13. Compliance

13.1 Complying with Legal Requirements

Valdosta State University will comply with state and federal information security regulations and provide awareness and compliance training to all users. Strategies for developing compliance policies include:

13.1.1 Comply with state and federal regulations

- 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:
 - HIPAA
 - FERPA
 - COPPA
 - Gramm Leach Bliley Act
 - CJIS

13.1.2 Develop acceptable usage policies

- 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.

13.1.3 Develop security awareness

Develop security awareness training for all users that is commensurate with their access to the institute's information.

13.2 Reviewing Security Policies and Technical Compliance

Valdosta State University will periodically review documented procedures and operations to ensure compliance with state and federal security requirements. Guidelines for reviewing compliance procedures are:

13.2.1 Develop compliance audits

Develop compliance audits to ensure that campus departments are complying with security policies. Audit frequency should be based on the sensitivity of the system.

13.2.2 Develop technical compliance audits

- 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.