# Information Security Policy

## Agency
## Guidelines


## Agency for Enterprise Information Technology
## Office of Information Security

**August 2007**

## Security Policy Program Development

The cornerstone of the Agency for Enterprise Information Technology (AEIT), the Office of Information Security (OIS) responsibility is an integrated statewide security program development.

> Privacy policy dictates ***how a state will collect and use personal information and data***.
> Security policy dictates ***how a state will protect that information from misuse or loss***.

By creating and enforcing a common set of standards that have been developed to mitigate known risks to State information resources (Tri Annual Audit (NIST 800-30) in 2005)), the agencies can develop and deploy security and privacy programs with the confidence that their programs will meet baseline requirements clearly defined by OIS experts. Without a common understanding of critical program elements, statewide integration of systems and information sharing will be subject to the lowest standard set by any single agency. By clearly communicating baseline standards, the OIS can drive the state toward cost effective enterprise level security solutions in a federated model that supports agency level risk mitigation for decentralized operations.

### Security Standards Oversight

The effectiveness of the statewide security program will depend upon the amount of oversight provided. If no one is "minding the store," the standards will not be continuously deployed or operate effectively. Therefore, the OIS was elevated to a cabinet member of the AEIT and given the responsibility to facilitate and coordinate for the agencies to measure and periodically report effectiveness of the controls deployed within their agency including policy. This oversight will not only serve to enforce current baseline standards but also provide input into the security planning process. If current standards are not routinely achieved, the OIS can consider program adjustments based upon feedback from the oversight process.

### Security Policy and Guidance

> *Information security policy is an aggregate of directives, rules, and practices that prescribes how an organization manages, protects, and distributes information.*
>
> Information security policy is an essential component of information security governance—without the policy, governance has no substance and rules to enforce.

Information security policy should be based on a combination of appropriate state legislation, such as F.S.282.318 and 60 DD Rule; applicable standards, such as NIST SP 800 series and ISO 17799; and internal agency requirements. In 2005 the OIS in partnership with the governor's office spearheaded a 'special guidance' effort intended for future policy development in terms of listing fundamental or core agency policies with minimal content requirements in the form of policy templates for the purpose of uniformity. Prior to this effort agencies developed policies based upon agency need only and not necessarily for the enterprise. Furthermore based upon content analysis and inter agency comparison the same policy titles contained significant differences not to mention the lack of an enterprise numbering and/or nomenclature system or standard.

Supporting procedures on how to effectively implement specific controls within the agency should be derived by the agency from the tri annual and in between year risk assessment to augment any of the agency's security policies.

The OIS with approval from the Governor's Office created a focus group whose members were selected from the participating Agencies at the Information Security Managers (ISM) level. Consequently it is important to note guidance on information security policies was developed by agency members.

**List of Policies**

1. Agency Information Security Program
2. Confidential Information and Data Classification
3. Information Technology Management and Operations
4. Application Security
5. Acceptable Use
6. Information Security Awareness
7. Computer Information Security Incident Response
8. Mobile Computing
9. Wireless
10. Disposition of Computer Equipment
11. Risk Assessment

It was understood the results of the focus group considerations in the form of external policy guidance superseded existing agency information security policy in terms of revisions, additions, replacement, or modification. Agencies should ensure that their information security policy is sufficiently current to accommodate the information security environment and agency mission and operational requirements. To ensure that information security does not become obsolete, agencies should implement a policy review and revision cycle. As a part of the periodic review and the initial development of the information security policies, agencies should work to ensure that all internal security policies (i.e., physical and personnel) are sufficiently coordinated to ensure effective implementation of crosscutting and convergent security objectives, such as access control initiatives.

As a distinction the Mobile Computing template was given singular attention by the Governor in the form of a mandate. A special project management effort followed including a comprehensive gap analysis prior to agency approval in order to assess the impact of potential costs, especially the need and cost for encryption on laptops.

The result was the expedition of the mobile template over the others toward agency acceptance, approval and publication. What's more the gap analysis framework was lifted from the project context and applied to all the templates as a generalized model within the policy guideline.

Still, the Mobile Computing *policy* will be audited with the other templates in terms of maturity level and expected integration with agency business need and services.

## List of Policies

1. Agency Information Security Program
2. Confidential Information and Data Classification
3. Information Technology Management and Operations
4. Application Security
5. Acceptable Use
6. Information Security Awareness
7. Computer Information Security Incident Response
8. Mobile Computing
9. Wireless
10. Disposition of Computer Equipment
11. Risk Assessment

## 1. Agency Information Security Program

**Subject: Agency Information Security Program**

**Background**

The State of Florida government information technology resources are valuable assets to its citizens; the confidentiality, integrity, and availability of those resources must be protected.

Planning and implementation of proven security practices is required to protect information technology resources.

**Policy Objective**

Each agency shall have a defined information security program.

**Policy**

Agencies must implement an agency information security program, incorporating standards that meet or exceed those listed below.

Deviation from this policy requires a written approval for an exception from the agency head, in consultation with the State Office of Information Security.

### 1. Standards

1.1 Each agency head shall appoint in writing an Information Security Manager to administer the agency information security program. Written notification of the appointment shall be sent to the State Office of Information Security.

1.2 Each agency head or designee shall designate staff responsible for developing the agency information security program.

1.3 Each agency head or designee shall designate staff responsible for documenting and implementing an agency information security program.

1.4 The agency information security program must be consistent with applicable federal and state laws and rules.

1.5 The agency Information Security Manager shall review and update the agency information security program annually.

### 2. Definitions

2.1 **Availability—** The principle that authorized users have access to information and assets.

2.2 **Confidentiality**— The principle that information is accessible only to those authorized.

2.3 **Information Security Manager** - The person designated to administer the agency's information resource security program in accordance with section 282.318(2) (a) 1, Florida Statutes, and the agency's internal and external point of contact for all information security matters.

2.4 **Information Security Program** — A coherent assembly of plans, project activities, and supporting resources contained within an administrative framework, the purpose of which is to support the agency's mission and establish controls to assure adequate security for all information processed, transmitted or stored in agency automated information systems, *e.g.,* Information Technology Security Plans, contingency plans, security awareness and training and systems acquisition, disposal and auditing.

2.5 **Information Technology Resources** – Agency computer hardware, software, networks, devices, connections, applications, and data.

2.6 **Integrity—** The principle that assures information remains intact, correct, and authentic. Integrity involves preventing unauthorized creation, modification, or destruction of information.

2.7 **State Office of Information Security** (OIS) - The State of Florida information security office, which guides, coordinates and assists state agencies in identifying threats to their information assets and mitigating their vulnerabilities, so effective security controls can be implemented.

## 2. Confidential Information and Data Classification

**Subject: Confidential Information and Data Classification**

**Background**

The State of Florida government information technology resources are valuable assets to its citizens; the confidentiality, integrity, and availability of those resources must be protected.

Confidential information is information not subject to inspection by the public and may be released only to those persons and entities designated in statute. Exempt information is information the agency is not required to disclose under section 119.07(1), Florida Statutes, but which the agency is not necessarily prohibited from disclosing in all circumstances.

**Policy Objective**

Confidential information must be kept secured using appropriate administrative, technical, and physical safeguards.

**Policy**

Agencies must implement a confidential information and data classification policy incorporating standards that meet or exceed those listed below.

Deviation from this policy requires a written approval for an exception from the agency head, in consultation with the State Office of Information Security.

### 1. Standards

1.1 The agency Office of General Counsel shall maintain a reference list of state and federal statutes and rules relevant to agency confidential information.

1.2 Agency information owners shall be responsible for classifying information as confidential.

1.3 Agency information owners shall be responsible for authorizing access to information.

1.4 Agency information owners shall maintain documentation of users authorized to access confidential information.

1.5 Confidential information sent by email must be encrypted.

1.6 Electronic transmission of confidential information must be encrypted when the transport medium is not owned or managed by the agency.

1.7 Confidential information shall be accessible only to authorized individuals.

1.8 Due diligence must be taken to protect confidential information.

1.9 Procedures for handling and protecting confidential information must be documented in each agency's information security program.

1.10 The agency shall implement procedures to establish accountability for accessing confidential data stores.

1.11 The agency shall implement procedures to establish accountability for modifying confidential data.

1.12 The agency Information Security Manager or other authorized personnel shall be granted access to review audit logs containing accountability details.

1.13 Agreements and procedures shall be in place for sharing, handling or storing confidential data with entities outside the agency.

1.14 When authorized by the applicable retention schedule, confidential information, regardless of media type, must be destroyed.

1.15 Members of the workforce shall be knowledgeable of the classifications of data/information and the proper handling of data/information.

## 2. Definitions

2.1 **Accountability** – The principle stating that a specific action is associated with an individual.
2.2 **Audit logs –** Documentation of activity incorporating, at a minimum, date, time, action, and account details.
2.3 **Authorization—**Official or legal permission or approval.
2.4 **Availability—** The principle that authorized users have access to information and assets.
2.5 **Confidential Information**—Information that is prohibited from disclosure under the provisions of applicable state and federal law.
2.6 **Confidentiality**— The principle that information is accessible only to those authorized.
2.7 **Data store** – A collection of information organized so it can be accessed, managed, and updated.
2.8 **Information Owner —** The executive business manager who is responsible for the collection, maintenance, and dissemination of an information set.
2.9 **Information Security Manager (ISM)**—The person designated to administer the agency's information resource security program and plans in accordance with section 282.318, Florida Statutes, and the agency's internal and external point of contact for all information security matters.
2.10 **Information Technology Resources** – Agency computer hardware, software, networks, devices, connections, applications, and data.
2.11 **Integrity**— The principle that assures information remains intact, correct, and authentic. Integrity involves preventing unauthorized creation, modification, or destruction of information.
2.12 **Media –** A storage vessel for electronic data and information (*e.g.,* hard drive, laptop, CD, tape, thumb drive).
2.13 **Public Information**—All documents, papers, letters, maps, books, tapes, photographs, films, sound recordings, data processing software, or other material, regardless of the physical form, characteristics, or means of transmission, made or received pursuant to law or ordinance or in connection with the transaction of official business by any agency which is not confidential and has not been exempted from public disclosure by statute.
2.14 **State Office of Information Security** (OIS) - The State of Florida information security office, which guides, coordinates and assists state agencies in identifying threats to their information assets and mitigating their vulnerabilities, so effective security controls can be implemented.
2.15 **Workforce**—Employees, contractors, volunteers, trainees, and other persons whose conduct, in the performance of work for the agency, is under the direct control of the department, whether or not they are paid by the agency.

## 3. Information Technology Management and Operations

**Subject: Information Technology Management and Operations**

**Background**

The State of Florida government information technology resources are valuable assets to its citizens; the confidentiality, integrity, and availability of those resources must be protected.

The agency mission cannot be accomplished without a reliable information technology infrastructure and competent and responsible information technology workers. These goals can only be achieved through effective information technology management and operations.

**Policy Objective**

The agency information technology infrastructure and information technology workers must be managed appropriately and effectively.

**Policy**

Agencies must implement an information technology management and operations policy incorporating standards that meet or exceed those listed below.

Deviation from this policy requires a written approval for an exception from the agency head, in consultation with the State Office of Information Security.

### 1. Standards

#### 1.1 Physical Security for Information Technology Resources

1.1.1 State information technology resources must be protected by physical controls.

1.1.2 The agency must implement procedures to manage physical access to state information technology facilities.

1.1.3 Physical controls shall be appropriate for the size and criticality of the information technology resources.

1.1.4 Information technology resources shall be protected from environmental hazards (*i.e.,* temperature, humidity, air movement, cleanliness, and power) in accordance with manufacturers' specifications.

#### 1.2 Infrastructure Management

1.2.1 Only agency-owned or agency-managed information technology resources shall connect to agency networks.

1.2.2 The agency shall monitor for unauthorized information technology resources connected to the agency network.

1.2.3 The agency shall implement procedures to track agency information technology resources.

1.2.4 The agency shall identify and document information technology infrastructure resources and associated owners and custodians

1.2.5 The agency shall specify standard software and hardware.

1.2.6 The agency shall specify standard configurations used to harden information technology resources.

1.2.7 The agency shall perform a risk assessment prior to introducing a new technology (*e.g.,* voice over IP).

1.2.8 The development infrastructure, test infrastructure, and production infrastructure shall be physically or logically separated.

1.2.9 Information technology resources must be certified according to agency standard configuration prior to production implementation.

1.2.10 The agency shall implement a change management process for modifications to production information technology resources.

1.2.11 The agency shall ensure anti-malware software is maintained on agency information technology resources.

1.2.12 The agency shall implement a patch management process for information technology resources.

1.2.13 The agency Information Security Manager or other authorized personnel shall be granted access to review audit logs containing accountability details.

1.2.14 The agency must ensure service accounts are maintained in a manner that protects information technology resources.

1.2.15 Service accounts may be exempted from password expiration.

1.2.16 Service accounts must not be used for interactive sessions.

1.2.17 Administration of hardware, software, or applications performed over a network shall be encrypted (where technology permits).

1.2.18 The agency must ensure network perimeter security measures are in place to prevent unauthorized connections to agency information technology resources.

1.2.19 The agency must block unauthorized peer-to-peer traffic.

1.2.20 The agency Information Security Manager or designee must be granted access to monitor agency information technology resources.

1.2.21 The agency shall establish procedures to ensure regular review of system activity logs.

### 1.3 Backup and Recovery

1.3.1 The agency shall ensure recovery procedures for information technology resources are implemented and periodically tested.

1.3.2 The agency shall ensure security controls over backup resources are appropriate to the criticality and confidentiality of the primary resources.

## 1.4 Information Technology Workers and Accounts

1.4.1 Information technology positions are positions of special trust.

1.4.2 The agency shall conduct background investigations for personnel in positions of special trust as set forth in sections 110.1127, Florida Statutes.

1.4.3 The agency must provide on-going training for information technology workers to ensure competency in both technical and security aspects of their positions.

1.4.4 The agency shall establish procedures to ensure administrative rights for information technology resources are restricted to information technology workers who have received appropriate technical training and who are authorized based on job duties and responsibilities.

1.4.5 The agency must ensure accounts with administrative rights are created, maintained, monitored and removed in a manner that protects information technology resources.

1.4.6 Administrative account activities shall be traceable to an individual.

1.4.7 Information technology workers shall be granted access to agency information technology resources based on the principles of “least privilege” and “need to know.”

1.4.8 The agency shall implement controls to ensure access to information technology infrastructure resources is restricted to authorized users and uses.

1.4.9 The agency shall ensure separation of duties, so no individual has the ability to control an entire process.

## 1.5 Remote Access

1.5.1 The agency must establish standards for remote access.

1.5.2 The agency must implement procedures for granting remote access.

1.5.3 Remote access client connections must not be shared.

## 1.6 Contracts

1.6.1 The agency shall establish procedures to ensure contracts and agreements involving the use of information technology resources guarantee contractor compliance with the agency information technology security policies and procedures.

1.6.2 Prior to connecting to the agency network, non-agency entities must execute a network connection agreement guaranteeing compliance with agency security policies.

1.6.3 The agency Chief Information Officer or designee is responsible for maintaining network connection agreements.

## 2. Definitions

2.1 **Accountability –** The principle stating that a specific action is associated with an individual.

2.2 **Agency-managed device** – A device not owned by the agency, but which the agency ensures the hardware and software used is in compliance with agency standards.

2.3 **Anti-malware Software** – Software installed on a computing device that protects it from malicious software.

2.4 **Audit logs –** Documentation of activity incorporating, at a minimum, date, time, action, and account details.

2.5 **Availability** - The principle that authorized users have access to information and assets.

2.6 **Chief Information Officer** – The person who coordinates all information resource management activities and information technology assets to ensure they are appropriately planned and managed in accordance with the agency mission.

2.7 **Confidential Information and/or Confidential Data** – Information/Data that is exempted from disclosure under the provisions of applicable state and federal law.

2.8 **Confidentiality**— The principle that information is accessible only to those authorized.

2.9 **Custodian of an Information Resource** – Individuals who maintain or administer information resources on behalf of information owners. Person or team that holds the day-to-day responsibility for information technology infrastructure resources.

2.10 **Development Infrastructure** – A technical environment that is used for design, development, and/or piloting of new technical capabilities or applications. The development infrastructure is separated logically or physically from the production and test infrastructures.

2.11 **Directly connect** [to the agency network] – A device that is joined to and becomes an extension of the agency's internal network. Dial-up and Virtual Private Network (VPN) connections to the agency are considered to be directly connected.

2.12 **Encryption** – The process of transforming readable text into unreadable text (cipher text) for the purpose of security or privacy.

2.13 **Information Security Manager** - The person designated to administer the agency's information resource security program and plans in accordance with section 282.318(2) (a) 1, Florida Statutes, and the agency's internal and external point of contact for all information security matters.

2.14 **Information Technology Infrastructure** - Network devices, server hardware, and host operating systems

2.15 **Information Technology Resources** – Agency computer hardware, software, networks, devices, connections, applications, and data.

2.16 **Information Technology Worker** - An agency user whose job duties and responsibilities specify development, maintenance, or support of information technology resources.

2.17 **Integrity** - The principle that assures information remains intact, correct, and authentic. Integrity involves preventing unauthorized creation, modification, or destruction of information.

2.18 **Interactive Session** – A work session where there is an exchange of communication between a user and a computer.

2.19 **Least Privilege** – The principle that grants the minimum possible privileges to permit a legitimate action, in order to enhance protection of data and functionality from faults and malicious behavior.

2.20 **Malware** – Malicious software.

2.21 **Need to Know** – The principle where individuals with authorization to access information are further restricted to specific information based on individual duties.

2.22 **Network Perimeter** – The boundary of an agency's information technology infrastructure.

2.23 **Owner** - The manager of the business unit ultimately responsible for an information technology resource.

2.24 **Peer to peer** – Communications model that allows the direct sharing of files (audio, video, data, and software) among computers.

2.25 **Production Infrastructure** – Network devices, server hardware, and host operating systems that comprise an agency's operational or real-time environment.

2.26 **Remote Access** – Any access to an agency's network through a network, device, or medium that is not controlled by the agency (such as the Internet, public phone line, wireless carriers, or other external connectivity).

2.27 **Separation of Duties** - The concept of having more than one person required to complete a task. This is a way to ensure that no individual has the ability to control an entire process.

2.28 **Service Account** – An account used by a computer process (e.g., an account used by the backup process for file access).

2.29 **Special Trust or Position of Trust –**A position in which an individual is granted system-level (administrative) access to agency data or agency essential infrastructure. This includes positions where an individual has been granted access rights to information for which they have not been authorized to view or alter (e.g. application developers, database administrators, system administrators).

2.30 **Standards –** A specific set of practices or procedures to regulate how a system or organization provides services.

2.31 **Standard configuration –** Documentation of the specific rules or settings used in setting up agency hardware, software, and operating systems.

2.32 **Standard hardware** – A list of agency-approved hardware.

2.33 **Standard software** – A list of agency-approved software.

2.34 **State Office of Information Security (OIS)** - The State of Florida information security office, which guides, coordinates and assists state agencies in identifying threats to their information assets and mitigating their vulnerabilities, so effective security controls can be implemented.

2.35 **System Administrators** – A person in charge of managing and maintaining computer or telecommunication systems.

2.36 **Systems Hardening** – The process of securing a system.

2.37 **Test Infrastructure** - A technical environment that mirrors part or all of the production environment and is used for final testing of a technology or an application

prior to production implementation. The test infrastructure is separated logically or physically from the production and development infrastructure.

2.38 **Track** – The documented assignment of an asset to a user and/or location.

2.39 **User** – Any authorized agency worker who uses information technology resources.

2.40 **Workforce** - Employees, contractors, volunteers, trainees, and other persons whose conduct, in the performance of work for the agency, is under the direct control of the department, whether or not they are paid by the agency.

## 4. Application Security

**Subject: Application Security**

**Background**

The State of Florida government information technology resources are valuable assets to its citizens; the confidentiality, integrity, and availability of those resources must be protected.

Agency data is critical to the agency's mission. Software applications are the methods to access that data. In order to protect data, applications must be designed and configured with proper security controls.

**Policy Objective**

Agency software applications obtained, purchased, leased, and/or developed must provide appropriate security controls to minimize risks to the confidentiality, integrity, and availability of the application, its data, or other information technology resources.

**Policy**

Agencies must implement an application security policy incorporating standards that meet or exceed those listed below.

Deviation from this policy requires a written approval for an exception from the agency head, in consultation with the State Office of Information Security.

### 1. Standards

1.1 Each agency shall develop procedures to ensure application security is addressed throughout the application procurement process and/or application development lifecycle.

1.2 Application owners are responsible for defining application security-related business requirements.

1.3 The application development team shall implement appropriate security controls to achieve the security requirements of the application owner.

1.4 The application development team shall implement appropriate security measures to minimize risks to agency information technology resources.

1.5 The agency shall implement procedures to establish accountability for accessing confidential applications.

1.6 The agency shall implement procedures to establish accountability for modifying confidential data.

1.7 The agency Information Security Manager or other authorized personnel shall be granted access to review audit logs containing accountability details.

1.8 A final application security review must be approved by the application owner, Information Security Manager and the Chief Information Officer, or their respective designees, before an application is placed into production.

1.9 The application maintenance process shall include reviews of application security requirements and controls to ascertain effectiveness and appropriateness relative to new technologies and applicable state and federal regulations.

1.10 Application security documentation shall be maintained by the agency and be available to the Information Security Manager.

## 2. Definitions

2.1 **Accountability** – The principle stating that a specific action is associated with an individual.

2.2 **Application –** A software program or group of software programs designed to work together to accomplish specific business objectives.

2.3 **Application Development Lifecycle –** A set of procedures to guide the development of production application software and data items. A typical application development lifecycle includes design, development, maintenance, quality assurance and acceptance testing.

2.4 **Application development team –** A group responsible for developing and/or maintaining applications including, at a minimum, programmers, data base administrators, data administrators, system administrators, and network administrators.

2.5 **Application owner –** The manager of the business unit that requested the application be developed.

2.6 **Application Security Review –** An evaluation of an application's security requirements and associated controls (planned or implemented) with the goal of determining if controls are sufficient to minimize risks to the confidentiality, integrity, and availability of the application, its data, or other information technology resources.

2.7 **Audit logs –** Documentation of activity incorporating, at a minimum: date, time, action, and account details.

2.8 **Availability—** The principle that authorized users have access to information and assets.

2.9 **Confidentiality**— The principle that information is accessible only to those authorized.

2.10 **Information Technology Resources** – Agency computer hardware, software, networks, devices, connections, applications, and data.

2.11 **Integrity**— The principle that assures information remains intact, correct, and authentic. Integrity involves preventing unauthorized creation, modification, or destruction of information.

2.12 **Security controls** – Hardware, software, programs, procedures, policies or physical safeguards implemented to fulfill security requirements and mitigate risks to information technology resources**.**

2.13 **State Office of Information Security** (OIS) - The State of Florida information security office, which guides, coordinates and assists state agencies in identifying threats to their information assets and mitigating their vulnerabilities, so effective security controls can be implemented.

## 5. Acceptable Use

**Subject: Acceptable Use**

**Background**

The State of Florida government information technology resources are valuable assets to its citizens; the confidentiality, integrity, and availability of those resources must be protected.

Agency computer hardware, software, network devices and connections, user programs and data (information technology resources), are and shall remain the property of the State of Florida, subject to its sole control. Improper use of information technology resources poses increased risks to these resources. Agency workers have a responsibility to safeguard the information technology resources.

**Policy Objective**

Appropriate standards must be in place to prevent improper use of information technology resources and thereby to mitigate security risks.

**Policy**

Agencies must implement an acceptable use policy incorporating standards that meet or exceed those listed below.

Deviation from this policy requires a written approval for an exception from the agency head, in consultation with the State Office of Information Security.

### 1. Standards

#### 1.1 Compliance with Applicable Laws

1.1.1 Each member of the agency workforce is responsible for complying with agency security policies and procedures when performing agency work or when using agency information technology resources.

1.1.2 Each member of the agency workforce is responsible for complying with applicable State and Federal security rules and laws.

#### 1.2 Computer Use and Confidentiality Agreement

1.2.1 Each member of the agency workforce must acknowledge, in writing, these responsibilities by completing an agency computer use and confidentiality agreement prior to the use of State of Florida information technology resources.

#### 1.3 Use of State Information Technology Resources

1.3.1 Access to agency information technology resources is reserved for agency-approved users.

1.3.2 Each agency shall document its own parameters that govern personal use of agency information technology resources.

1.3.3 Each agency shall have sole discretion to determine whether a use is personal or business.

1.3.4 Personal use, if allowed by the agency, must not interfere with the normal performance of a worker's duties.

1.3.5 Personal use, if allowed by the agency, must not consume significant amounts of state information technology resources.

1.3.6 To prevent loss of data, agency users must ensure agency data stored on workstations or mobile devices is backed up.

**1.4 Authentication**

1.4.1 Agency computer users shall have unique user accounts.

1.4.2 Agency computer users shall be held accountable for their account activities.

1.4.3 User accounts must be authenticated at a minimum by a password.

1.4.4 Agency computer users are responsible for safeguarding their passwords and other authentication methods.

1.4.5 Agency workers must not share their agency accounts, passwords, personal identification numbers, security tokens, smart cards, identification badges, or other devices used for identification and authentication purposes.

1.4.6 Agency workers shall immediately report suspected account compromises according to agency incident reporting procedures.

1.4.7 Agency workers shall immediately report lost security tokens, smart cards, identification badges, or other devices used for identification and authentication purposes according to agency incident reporting procedures.

**1.5 Privacy**

1.5.1 Agency computer users shall have no expectation of privacy.

1.5.2 The agency may inspect any and all files stored on agency network or computer systems, including attached removable media.

1.5.3 The agency may monitor the use of state information technology resources.

1.5.4 Use of state information technology resources constitutes consent to monitoring activities whether or not a warning banner is displayed.

**1.6 Email**

1.6.1 Agency computer users shall follow agency established guidelines for acceptable use of email resources.

1.6.2 Confidential information sent by email must be encrypted.

1.6.3 Inappropriate use of agency email includes, but is not limited to, the following:

a. distribution of malware;

b. forging email headers;

c. propagating “Chain” letters; and

d. auto-forwarding agency email to a non-agency email address

**1.7 Internet**

1.7.1 Agency computer users shall follow agency-established guidelines for acceptable use of Internet resources.

1.7.2 Inappropriate use of the Internet includes, but is not limited to, non-work related access to the following:

a. chat rooms, news groups, political groups, singles clubs, or dating services;

b. material relating to gambling, weapons, illegal drugs, illegal drug paraphernalia, or violence;

c. hacker web-site/software; and

d. pornography and sites containing obscene materials

### 1.8 Workstation Security

1.8.1 Agency computer users shall not disable, alter, or circumvent agency workstation security measures.

1.8.2 Agency computer users shall logoff or lock their workstations prior to leaving the work area.

1.8.3 Workstations shall be secured with a password-protected screensaver with the automatic activation feature set at no more than 15 minutes.

### 1.9 Software

1.9.1 Only agency-approved software shall be installed on agency-owned or agency-managed computers.

1.9.2 Illegal duplication of software is prohibited.

### 1.10 Hardware

1.10.1 No privately-owned devices (e.g., MP3 players, thumb drives, printers) shall be connected to state-owned information technology resources without agency authorization.

### 1.11 Network

1.11.1 Monitoring, sniffing, and related security activities shall be performed only by workers based on job duties and responsibilities when given explicit consent.

### 1.12 Unacceptable Uses

1.12.1 Agency computer users must not attempt to access information technology resources for which they do not have authorization or explicit consent.

1.12.2 State information technology resources shall not be used for any purpose which violates state or federal laws or rules.

1.12.3 State information technology resources must not be used for personal profit, benefit or gain.

1.12.4 State information technology resources shall not be used to access, create, store, or transmit offensive, indecent or obscene material.

1.12.5 Agency computer users must not use State information technology resources to engage in activities that may harass, threaten, or abuse others.

1.12.6 State information technology resources shall not be used for political campaigning or unauthorized fund raising.

1.12.7 Agency computer users must not circumvent agency computer security measures.

1.12.8 State information technology resources shall not be used for any activity which adversely affects the availability, confidentiality or integrity of information technology resources.

### 1.13 Enforcement

1.13.1 Violation of this policy may result in an agency taking disciplinary action appropriate to the violation up to and including termination and/or criminal prosecution.

## 2. Definitions

2.1 **Agency-approved software** – Software that has been reviewed and deemed acceptable by the agency for use with agency information technology resources.
2.2 **Agency-managed device** – A device not owned by the agency, but which the agency ensures the hardware and software used is in compliance with agency standards.
2.3 **Anti-malware Software** – Software installed on a computing device that protects it from malicious software.
2.4 **Authentication** – The process of verifying that a user is who he or she purports to be. Techniques fall into one of three categories: (1) something the user knows, such as a password or PIN; (2) something the user has, such as a smartcard or ATM card; and (3) something that is part of the user, such as a fingerprint or the iris of the eye.
2.5 **Availability—** The principle that authorized users have access to information and assets.
2.6 **Computer use and confidentiality agreement** – An individual's acknowledgement of acceptance of an agency's security policies and procedures, and the individual's acknowledgement of accountability for compliance.
2.7 **Computer user** – See definition for "User."
2.8 **Confidential Information and/or Confidential Data** – Information/Data that is exempted from disclosure requirements under the provisions of applicable state and federal law.
2.9 **Confidentiality**— The principle that information is accessible only to those authorized.
2.10 **Encryption** – The process of transforming readable text into unreadable text (cipher text) for the purpose of security or privacy.
2.11 **Information Technology Resources –** Agency computer hardware, software, networks, devices, connections, applications, and data.
2.12 **Integrity—** The principle that assures information remains intact, correct, and authentic. Integrity involves preventing unauthorized creation, modification, or destruction of information.
2.13 **Malware**–Malicious software.
2.14 **Privately-owned device** – A device owned by an individual and not purchased with government funds.
2.15 **Sniffing** – Capturing network data.
2.16 **State Office of Information Security** (OIS) - The State of Florida information security office, which guides, coordinates and assists state agencies in identifying threats to their information assets and mitigating their vulnerabilities, so effective security controls can be implemented.
2.17 **User** – Any authorized agency worker who uses information technology resources.
2.18 **Warning banner –** Message displayed prior to or upon connection to a resource informing the user that activities may be monitored or access is restricted.
2.19 **Worker –** A member of the workforce (a worker may or may not use information technology resources).
2.20 **Workforce** - Employees, contractors, volunteers, trainees, and other persons whose conduct, in the performance of work for the agency, is under the direct control of the department, whether or not they are paid by the agency.
2.21 **Workstation** - A computer used by members of the workforce for work-related duties.

## 6. Information Security Awareness

**Subject: Information Security Awareness**

**Background**

The State of Florida government information technology resources are valuable assets to its citizens; the confidentiality, integrity, and availability of those resources must be protected.

Employees who understand the value of the agency information they handle, the need to protect that information, and the knowledge of responsible technology use are vital to the protection of agency information. An effective level of awareness and training is key to this goal.

**Policy Objective**

Agencies shall provide an ongoing information security awareness and training program.

**Policy**

Agencies must implement an information security awareness policy incorporating standards that meet or exceed those listed below.

Deviation from this policy requires a written approval for an exception from the agency head, in consultation with the State Office of Information Security.

### 1. Standards

1.1 The agency Information Security Manager shall implement and maintain the agency information security awareness program.

1.2 Initial training must cover minimum security policies and practices applicable to the employee's job duties and responsibilities and shall be consistent with federal regulations, state laws and rules, as well as agency policies and procedures.

1.3 Members of the State of Florida government workforce shall receive initial security awareness training within 30 days of employment start date and prior to accessing confidential information.

1.4 Awareness and training in security shall include on-going education and continual reinforcement of the value of security.

1.5 The agency shall provide specialized training for employees whose duties bring them into contact with confidential information resources.

1.6 The agency shall maintain records of individuals who have completed security awareness training.

### 2. Definitions

2.1 **Availability**— The principle that authorized users have access to information and assets.
2.2 **Confidential Information**—Information that is exempted from disclosure under the provisions of applicable state and federal law.
2.3 **Confidentiality**— The principle that information is accessible only to those authorized.
2.4 **Information Security Manager (ISM)**—The person designated to administer the agency's information resource security program and plans in accordance with section 282.318, Florida Statutes, and the agency's internal and external point of contact for all information security matters.
2.5 **Information Technology Resources** – Agency computer hardware, software, networks,

devices, connections, applications, and data.

2.6 **Integrity**— The principle that assures information remains intact, correct, and authentic. Integrity involves preventing unauthorized creation, modification, or destruction of information.

2.7 **State Office of Information Security** (OIS) - The State of Florida information security office, which guides, coordinates and assists state agencies in identifying threats to their information assets and mitigating their vulnerabilities, so effective security controls can be implemented.

2.8 **Workforce**—Employees, contractors, volunteers, trainees, and other persons whose conduct, in the performance of work for the agency, is under the direct control of the department, whether or not they are paid by the agency.

## 7. Computer Security Incident Response

**Subject: Computer Security Incident Response**

**Background**

The State of Florida government information technology resources are valuable assets to its citizens; the confidentiality, integrity, and availability of those resources must be protected.

Computer security incidents include any actions or activities that compromise the confidentiality, integrity, or availability of agency information technology resources. A consistent approach to address and respond to computer security incidents will minimize the impact of such events.

**Policy Objective**
Each State of Florida government agency must have a standard process for reporting, responding to, mitigating, and documenting computer security incidents.

**Policy**
Agencies must implement a computer security incident response policy incorporating standards that meet or exceed those listed below.

Deviation from this policy requires a written approval for an exception from the agency head, in consultation with the State Office of Information Security.

### 1. Standards

1.1 Each agency shall establish a Computer Security Incident Response Team (CSIRT) to respond to suspected computer security incidents by identifying and controlling the incidents, notifying designated CSIRT responders, and reporting findings to agency management.

1.2 The CSIRT membership shall include at least one individual with expertise from the agency's legal, human resources, inspector general, and information technology areas, as well as the Chief Information Officer and Information Security Manager.

1.3 The CSIRT shall develop, document, and implement the agency computer security incident reporting process.

1.4 The CSIRT shall develop, document, and implement the agency computer security incident response process.

1.5 Members of the workforce must report suspected computer security incidents in accordance with agency reporting procedures.

1.6 Suspected computer security incidents must be reported to the Inspector General, agency Chief Information Officer, and the Information Security Manager.

1.7 The CSIRT shall determine the appropriate response required for each suspected computer security incident.

1.8 Computer security incidents shall be reported to the Office of Information Security according to Office of Information Security procedures.

1.9 Each suspected computer security incident, including findings and corrective actions, must be documented and maintained as specified in the agency computer security incident procedures.

1.10 Computer security Incident documentation is exempt from public disclosure (282.318, F.S.).

## 2. Definitions

2.1 **Availability—** The principle that authorized users have access to information and assets.
2.2 **Computer Security Incident** - Any action or activity that compromises the confidentiality, integrity, or availability of agency information technology resources. Inappropriate use of agency technical resources does not necessarily constitute a computer security incident.
2.3 **Confidentiality**— The principle that information is accessible only to those authorized.
2.4 **Information Security Manager (ISM)**—The person designated to administer the agency's information resource security program and plans in accordance with Section 282.318, Florida Statutes, and the agency's internal and external point of contact for all information security matters.
2.5 **Information Technology Resources** – Agency computer hardware, software, networks, devices, connections, applications, and data.
2.6 **Integrity**— The principle that assures information remains intact, correct, and authentic. Integrity involves preventing unauthorized creation, modification, or destruction of information.
2.7 **State Office of Information Security** (OIS) - The State of Florida information security office, which guides, coordinates and assists state agencies in identifying threats to their information assets and mitigating their vulnerabilities, so effective security controls can be implemented.
2.8 **Workforce -** Employees, contractors, volunteers, trainees, and other persons whose conduct, in the performance of work for the agency, is under the direct control of the department, whether or not they are paid by the agency.

## 8. Mobile Devices

**Subject: Mobile Devices**

**Background**

The State of Florida government information technology resources are valuable assets to its citizens; the confidentiality, integrity, and availability of those resources must be protected.

The use of mobile devices poses risks to the information they contain, as well as to the devices themselves. Use of mobile devices on non-agency networks poses risks to agency information technology resources upon subsequent connection to the agency network.

**Policy Objective**

Appropriate security controls must be in place to mitigate security risks presented by using mobile devices.

**Policy**

Agencies must implement a mobile devices policy incorporating standards that meet or exceed those listed below.

Deviation from this policy requires a written approval for an exception from the agency head, in consultation with the State Office of Information Security.

### 1. Standards

1.1 Security and privacy policies applicable in the agency facility apply when using or connecting to agency information technology resources from outside the agency facility.
1.2 Only agency-owned or agency-managed mobile devices are allowed to directly connect to the agency network.
1.3 Only agency-owned or agency-managed mobile storage devices may store agency data.
1.4 State mobile computing devices must be tracked by the agency.
1.5 Mobile computing devices connecting to the agency network must use current and up-to-date anti-malware software.
1.6 State mobile computing devices must activate an agency-approved personal firewall (where technology permits) when connected to a non-agency network.
1.7 State mobile devices will be configured and maintained according to agency standards.
1.8 Only agency-approved software will be installed on state mobile computing devices.
1.9 State mobile computing devices will be issued to and used by only agency-authorized users.
1.10 Mobile computing devices will require user authentication.
1.11 Mobile computing devices shall be secured with a password-protected screensaver with the automatic activation feature set at no more than 15 minutes.
1.12 Users must take reasonable precautions to protect mobile computing devices in their possession from loss, theft, tampering, unauthorized access, and damage.
1.13 Users may remotely connect mobile computing devices directly to the agency network only through agency-approved, secured remote access methods.
1.14 To prevent loss of data, agency data stored on mobile devices must be backed up.
1.15 Mobile computing devices used with confidential information require encryption.
1.16 Confidential data must be encrypted when transmitted over a network.
1.17 Mobile storage devices with confidential agency data must have encryption technology enabled such that all content resides encrypted.
1.18 Users must report theft of mobile devices immediately to the appropriate agency personnel. In addition, the agency Information Security Manager and the Office of Information Security shall be notified.

## 2. Definitions

2.1 **Agency-managed device** – A device not owned by the agency, but which the agency ensures the hardware and software used is in compliance with agency standards.

2.2 **Anti-malware Software** – Software installed on a computing device that protects it from malicious software.

2.3 **Authentication** – The process of verifying that a user is who he or she purports to be. Techniques fall into one of three categories: (1) something the user knows, such as a password or PIN; (2) something the user has, such as a smartcard or ATM card; and (3) something that is part of the user, such as a fingerprint or the iris of the eye.

2.4 **Availability—** The principle that authorized users have access to information and assets when required.

2.5 **Chief Information Officer –** The person who coordinates all information resource management activities and information technology assets to ensure they are appropriately planned and managed in accordance with the agency mission.

2.6 **Confidential Information and/or Confidential Data** – Information/Data that is exempted from disclosure requirements under the provisions of applicable state and federal law. Ensuring that information and/or data is accessible only to those authorized to have access.

2.7 **Confidentiality**— The principle that information is accessible only to those authorized to have access.

2.8 **Directly connect [to the agency network]** – A mobile device that is joined to and becomes an extension of the agency's internal network.

2.9 **Encryption** – The process of transforming readable text into unreadable text (cipher text) for the purpose of security or privacy.

2.10 **Information Technology Resources** – Agency computer hardware, software, networks, devices, connections, applications, and data.

2.11 **Integrity**— The principle that assures information remains intact, correct, and authentic. Integrity involves preventing unauthorized creation, modification, or destruction of information.

2.12 **Mobile Computing Device** – A laptop, PDA, or other portable device that can process data.

2.13 **Mobile Devices** – A general term describing both mobile computing and mobile storage devices.

2.14 **Mobile Storage Device** – Portable data storage media including, but not limited to, external hard drives, thumb drives, floppy disks, recordable compact discs (CD-R/RW), recordable digital videodiscs (DVD-R/RW), IPODs, media players, and cell phones or tape drives that may be easily attached to and detached from computing devices.

2.15 **Personal Firewall** – Software installed on a computer or device which helps protect that system against unauthorized access.

2.16 **Remote Access** – Any access to an agency's network through a network, device, or medium that is not controlled by the agency (such as the Internet, public phone line, wireless carriers, or other external connectivity).

2.17 **State Office of Information Security** (OIS) - The State of Florida information security office, which guides, coordinates and assists state agencies in identifying threats to their information assets and mitigating their vulnerabilities, so effective security controls can be implemented.

2.18 **Track** – The documented assignment of an asset to a user and/or location.

2.19 **User** – Any authorized agency worker who uses information technology resources.

2.20 **Wireless network** – A computing network made up of, but not limited to, computers and access points or repeaters joined by radio communication using a frequency spread-spectrum technology.

## 9. Wireless

**Subject: Wireless**

**Background**

The State of Florida government information technology resources are valuable assets to its citizens; the confidentiality, integrity, and availability of those resources must be protected.

The use of wireless technologies poses risks to State of Florida government information technology resources.

**Policy Objective**

Appropriate security measures must be implemented to mitigate increased security risks presented by using wireless technologies.

**Policy**

Agencies must implement a wireless policy incorporating standards that meet or exceed those listed below.

Deviation from this policy requires a written approval for an exception from the agency head, in consultation with the State Office of Information Security.

### 1. Standards

1.1 Only agency-approved wireless devices, services, and technologies must be used when connecting to the agency network.

1.2 The agency shall monitor for unauthorized access points.

1.3 Agency wireless access points shall be tracked by the agency.

1.4 Unauthorized access points connected to the agency network must be removed immediately.

1.5 Agency wireless devices must be configured and maintained according to agency standards.

1.6 Wireless transmission of agency data must be encrypted.

1.7 Clients connected to the agency network must not be simultaneously connected to any other network.

1.8 Wireless access into the agency network must require user-authentication.

### 2. Definitions

2.1 **Availability—** The principle that authorized users have access to information and assets.
2.2 **Confidentiality—** The principle that information is accessible only to those authorized.
2.3 **Encryption**— The process of transforming readable text into unreadable text (cipher text) for the purpose of security or privacy.
2.4 **Information Security Manager (ISM)**—The person designated to administer the agency's information resource security program and plans in accordance with section 282.318(2)(a)1, Florida Statutes, and the agency's internal and external point of contact for all information security matters.

2.5 **Information Technology Resources—** Agency computer hardware, software, networks, devices, connections, applications, and data.
2.6 **Integrity**— The principle that assures information remains intact, correct, and authentic. Integrity involves preventing unauthorized creation, modification, or destruction of information.
2.7 **State Office of Information Security** (OIS) - The State of Florida information security office, which guides, coordinates and assists state agencies in identifying threats to their information assets and mitigating their vulnerabilities, so effective security controls can be implemented.
2.8 **Track** – The documented assignment of an asset to a user and/or location.
2.9 **Wireless Technology** – A technology that uses radio waves to transmit and receive data.

## 10. Disposition of Computer Equipment

**Subject: Disposition of Computer Equipment**

**Background**

The State of Florida government information technology resources are valuable assets to its citizens; the confidentiality, integrity, and availability of those resources must be protected.

Without proper sanitization, destruction, and disposal of information technology resources, agency information could be compromised.

**Policy Objective**

Disposition of computer equipment must be performed in a manner to ensure that confidentiality is maintained.

**Policy**

Agencies must implement a disposition of computer equipment policy incorporating standards that meet or exceed those listed below.

Deviation from this policy requires a written approval for an exception from the agency head, in consultation with the State Office of Information Security.

### 1. Standards

1.11 Each agency shall document procedures for sanitization of agency-owned computer equipment prior to reassignment or disposal.

1.12 Equipment sanitization must be performed such that no data remains. File deletion and formatting media are not acceptable or approved methods of sanitization.

1.13 Acceptable methods of sanitization include:

- using software to overwrite data on computer media;
- degaussing; or
- physically destroying media.

### 2. Definitions

2.1 **Availability—** The principle that authorized users have access to information and assets.
2.2 **Confidentiality**— The principle that information is accessible only to those authorized.
2.3 **Degaussing** - A method to magnetically erase the data from electronic media.
2.4 **Information Technology Resources** – Agency computer hardware, software, networks, devices, connections, applications, and data.
2.5 **Integrity**— The principle that assures information remains intact, correct, and authentic. Integrity involves preventing unauthorized creation, modification, or destruction of information.
2.6 **Media** – A storage vessel for electronic data and information (*e.g.,* hard drive, laptop, CD, tape, thumb drive).
2.7 **State Office of Information Security** (OIS) - The State of Florida information security office, which guides, coordinates and assists state agencies in identifying threats to their

information assets and mitigating their vulnerabilities, so effective security controls can be implemented.

2.8 **User** – Any authorized agency worker who uses information technology resources.

## 11. Risk Assessment

**Subject: Risk Assessment**

**Background**

The State of Florida government information technology resources are valuable assets to its citizens; the confidentiality, integrity, and availability of those resources must be protected.

Risk assessment is the process of applying cost benefit analysis to information technology resources, associated security risks, and mitigation strategies.

**Policy Objective**

Each State of Florida government agency shall implement an on-going documented program of risk management, including risk analysis for critical information resources.

**Policy**

Agencies must implement a risk assessment policy incorporating standards that meet or exceed those listed below.

Deviation from this policy requires a written approval for an exception from the agency head, in consultation with the State Office of Information Security.

### 1. Standards

1.1. Each agency shall conduct a comprehensive risk analysis of critical information resources every three years.

1.2. The agency Information Security Manager shall notify the Office of Information Security when a comprehensive risk analysis has been completed.

1.3. Documentation of the information security risk analysis and risk mitigation plans is confidential and not subject to public disclosure (section 282.318, Florida Statute).

1.4. Agencies shall implement appropriate risk mitigation plans.

1.5. The agency Information Security Manager shall monitor and document risk mitigation implementation.

### 2. Definitions

2.1 **Availability—** The principle that authorized users have access to information and assets.

2.2 **Comprehensive Risk Analysis**—A process that systematically identifies valuable information system resources and threats to those resources, quantifies loss exposure (*i.e*., loss potential) based on the estimated frequency and cost of threat occurrences, and recommends how to allocate resources to countermeasures so as to minimize total exposure. The analysis lists risks in order of cost and criticality, thereby determining where countermeasures should be applied first. An example of a risk analysis standard is the National Institute of Standards and Technology methodology.

2.3 **Confidentiality—** The principle that information is accessible only to those authorized.

2.4 **Critical Information Resources**— The resources determined by agency management to be essential to the agency's critical mission and functions, the loss of which would have an unacceptable impact.

2.5 **Information Security Manager (ISM)**—The person designated to administer the agency's information resource security program and plans in accordance with section 282.318, Florida Statutes, and the agency's internal and external point of contact for all information security matters.

2.6 **Information Technology Resources** – Agency computer hardware, software, networks, devices, connections, applications, and data.

2.7 **Integrity**— The principle that assures information remains intact, correct, and authentic. Integrity involves preventing unauthorized creation, modification, or destruction of information.

2.8 **National Institute of Standards and Technology** (NIST) – A non-regulatory federal agency within the U.S. Commerce Department's Technology Administration. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.

2.9 **State Office of Information Security** (OIS) - The State of Florida information security office, which guides, coordinates and assists state agencies in identifying threats to their information assets and mitigating their vulnerabilities, so effective security controls can be implemented.

**APPENDIX B, Glossary**

1. **Accountability** – The principle stating that a specific action is associated with an individual.
2. **Agency-approved software** – Software that has been reviewed and deemed acceptable by the agency for use with agency information technology resources.
3. **Agency-managed device** – A device not owned by the agency, but which the agency ensures the hardware and software used is in compliance with agency standards.
4. **Anti-malware Software** – Software installed on a computing device that protects it from malicious software.
5. **Application** – a software program or group of software programs designed to work together to accomplish specific business objectives.
6. **Application development lifecycle -** a set of procedures to guide the development of production application software and data items. A typical SDLC includes design, development, maintenance, quality assurance and acceptance testing.
7. **Application development team -** A group responsible for developing and/or maintaining applications including, at a minimum, programmers, data base administrators, data administrators, system administrators, and network administrators.
8. **Application owner –** the manager of the business unit that requested the application be developed.
9. **Application security review –** an evaluation of an application's security requirements and associated controls (planned or implemented) with the goal of determining if controls are sufficient to minimize risks to the confidentiality, integrity, and availability of the application, its data, or other information technology resources.
10. **Audit logs –** Documentation of activity incorporating, at a minimum date, time, action, and account details.
11. **Authentication –** The process of verifying that a user is who he or she purports to be. Techniques fall into one of three categories: (1) something the user knows, such as a password or PIN; (2) something the user has, such as a smartcard or ATM card; and (3) something that is part of the user, such as a fingerprint or the iris of the eye.
12. **Authorization—** Official or legal permission or approval.
13. **Availability—**The principle that authorized users have access to information and assets.
14. **Chief Information Officer –** The person who coordinates all information resource management activities and information technology assets to ensure they are appropriately planned and managed in accordance with the agency mission.
15. **Comprehensive Risk Analysis**—A process that systematically identifies valuable information system resources and threats to those resources, quantifies loss exposure (i.e., loss potential) based on the estimated frequency and cost of threat occurrences, and recommends how to allocate resources to countermeasures so as to minimize total exposure. The analysis lists risks in order of cost and criticality, thereby determining where countermeasures should be applied first.
16. **Computer Security Incident -** any action or activity that compromises the confidentiality, integrity, or availability of agency information technology resources. Inappropriate use of agency technical resources does not necessarily constitute a computer security incident (e.g., Accessing pornography via State resources is not a computer security incident).
17. **Computer use and confidentiality agreement –** An individual's acknowledgement of acceptance of an agency's security policies and procedures, and the individual's acknowledgement of accountability for compliance.
18. **Computer user** – See definition for "User."
19. **Confidential Information and/or Confidential Data –** Information/Data that is exempted from disclosure under the provisions of applicable state and federal law. **Confidentiality—** The principle that information is accessible only to those authorized.

20. **Critical Information Resources**— the resources determined by agency management to be essential to the agency's critical mission and functions, the loss of which would have an unacceptable impact.
21. **Custodian of an Information Resource** – Individuals who maintain or administer information resources on behalf of information owners. Person or team that holds the day-to-day responsibility for information technology infrastructure resources.
22. **Data store** – A collection of information organized so it can be accessed, managed, and updated.
23. **Degaussing -** A method to magnetically erase the data from electronic media.
24. **Development Infrastructure** – A technical environment that is used for design, development, and/or piloting of new technical capabilities or applications. The development infrastructure is separated logically or physically from the production and test infrastructures.
25. **Directly connect [to the agency network] –** A device that is joined to and becomes an extension of the agency's internal network. Dial-up and Virtual Private Network (VPN) connections to the agency are considered to be directly connected.
26. **Elevated position** – a position having access to critical network or data center locations, whose duties allow access to confidential information, or whose computer related duties are depended on for the continuity of essential information resources.
27. **Encryption –** The process of transforming readable text into unreadable text (cipher text) for the purpose of security or privacy.
28. **Information Owner —** The executive business manager who is responsible for the collection, maintenance, and dissemination of an information set.
29. **Information Security Manager -** The person designated to administer the agency's information resource security program and plans in accordance with section 282.318(2)(a)1, Florida Statutes, and the agency's internal and external point of contact for all information security matters.
30. **Information Security Program —** A coherent assembly of plans, project activities, and supporting resources contained within an administrative framework, the purpose of which is to support the agency's mission and establish controls to assure adequate security for all information processed, transmitted or stored in agency automated information systems, *e.g.,* Information Technology Security Plans, contingency plans, security awareness and training and systems acquisition, disposal and auditing.
31. **Information Technology Infrastructure -** Network devices, server hardware, and host operating systems.
32. **Information Technology Resources –** Agency computer hardware, software, networks, devices, connections, applications, and data.
33. **Information Technology Worker** - An agency user whose job duties and responsibilities specify development, maintenance, or support of information technology resources.
34. **Integrity—**The principle that assures information remains intact, correct, and authentic. Integrity involves preventing unauthorized creation, modification, or destruction of information.
35. **Interactive Session** – A work session where there is an exchange of communication between a user and a computer.
36. **Least Privilege –** The principle that grants the minimum possible privileges to permit a legitimate action, in order to enhance protection of data and functionality from faults and malicious behavior.
37. **Malware–**Malicious software.
38. **Media –** A storage vessel for electronic data and information (*e.g.,* hard drive, laptop, CD, tape, thumb drive).
39. **Mobile Computing Device –** A laptop, PDA, or other portable device that can process

data.

40. **Mobile Devices –** general term describing both mobile computing and mobile storage devices.
41. **Mobile Storage Device –** Portable data storage media including, but not limited to, external hard drives, thumb drives, floppy disks, recordable compact discs (CD-R/RW), recordable digital videodiscs (DVD-R/RW), IPODs, media players, and cell phones or tape drives that may be easily attached to and detached from computing devices.
42. **National Institute of Standards and Technology** (NIST) – A non-regulatory federal agency within the U.S. Commerce Department's Technology Administration. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.
43. **Need to Know –** The principle that individuals with authorization to access information are further restricted to specific information based on individual duties.
44. **Network Perimeter** – the boundary of an agency's information technology infrastructure.
45. **Owner** - The manager of the business unit ultimately responsible for an information technology resource.
46. **Peer to peer –** Communications model that allows the direct sharing of files (audio, video, data, and software) among computers.
47. **Personal Firewall –** Software installed on a computer or device which helps protect that system against unauthorized access.
48. **Privately-owned device** – A device owned by an individual and not purchased with government funds.
49. **Production Infrastructure** – Network devices, server hardware, and host operating systems that comprise an agency's operational or real-time environment.
50. **Public Information**—All documents, papers, letters, maps, books, tapes, photographs, films, sound recordings, data processing software, or other material, regardless of the physical form, characteristics, or means of transmission, made or received pursuant to law or ordinance or in connection with the transaction of official business by any agency which is not confidential and has not been exempted from public disclosure by statute.
51. **Remote Access –** Any access to an agency's network through a network, device, or medium that is not controlled by the agency (such as the Internet, public phone line, wireless carriers, or other external connectivity)
52. **Security controls** – hardware, software, programs, procedures, policies or physical safeguards implemented to fulfill security requirements and mitigate risks to information technology resources**.**
53. **Separation of Duties -** The concept of having more than one person required to complete a task. This is a way to ensure that no one individual has the ability to control an entire process.
54. **Service Account** – An account used by a computer process (e.g., an account used by the backup process for file access).
55. **Sniffing –** Capturing network data.
56. **Special Trust or Position of Trust –**A position in which an individual is granted system-level (administrative) access to agency data or agency essential infrastructure. This includes positions where an individual has been granted access rights to information for which they have not been authorized to view or alter (*e.g.,* application developers, database administrators, system administrators).
57. **Standards –** A specific set of practices or procedures to regulate how a system or organization provides services.
58. **Standard configuration –** Documentation of the specific rules or settings used in setting

up agency hardware, software, and operating systems.

59. **Standard hardware** – A list of agency-approved hardware.
60. **Standard software** – A list of agency-approved software.
61. **State Office of Information Security (OIS) -** The State of Florida information security office, which guides, coordinates and assists state agencies in identifying threats to their information assets and mitigating their vulnerabilities, so effective security controls can be implemented.
62. **System Administrator** – A person in charge of managing and maintaining computer or telecommunication systems.
63. **Systems Hardening –** the process of securing a system.
64. **Test Infrastructure** - A technical environment that mirrors part or all of the production environment and is used for final testing of a technology or an application prior to production implementation. The test infrastructure is separated logically or physically from the production and development infrastructure.
65. **Track** –The documented assignment of an asset to a user and/or location.
66. **User –** Any authorized agency worker who uses information technology resources.
67. **Warning banner –** Message displayed prior to or upon connection to a resource informing the user that activities may be monitored or access is restricted.
68. **Wireless network –** A computing network made up of, but not limited to, computers and access points or repeaters joined by radio communication using a frequency spread-spectrum technology.
69. **Wireless Technology** – a technology that uses radio waves to transmit and receive data.
70. **Worker –** A member of the workforce (a worker may or may not use information technology resources).
71. **Workforce -** Employees, contractors, volunteers, trainees, and other persons whose conduct, in the performance of work for the agency, is under the direct control of the department, whether or not they are paid by the agency.
72. **Workstation –** A computer used by members of the workforce for work-related duties.