PROGRAM GUIDANCE 300.01
IT SECURITY MANUAL

OF INTEREST TO

The Office of Early Learning (OEL), Early Learning Coalitions (ELCs), ELC contractors, ELC sub-contractors, OEL contractors, OEL sub-contractors and University of North Florida.

SUMMARY

OEL Information Technology (IT) Policies and Procedures govern the use and management of the information technology resources and services under control and jurisdiction of the Florida Office of Early Learning.

This manual includes practices, policies and procedures approved by the Florida Office of Early Learning. Standards, policies and procedures contained in this document supersede any and all previous OEL IT Policies and Procedures Manual versions.

Policies, rules, and procedures contained herein should be followed in a manner consistent with federal and State of Florida statutes and regulations.

REFERENCES

The full list of references is included within the Information Technology Policy and Procedures Manual. Below is a list of governing bodies that were used within the manual.

- American National Standards Institute (ANSI)
- Florida Statutes
- Florida Administrative Code
- Federal Information Processing Standard (FIPS)
- Federal Information Security Management Act (FITSOA)
- Governor's Code of Ethics
- Health Insurance Accountability and Portability Act (HIPPA)
- International Organization for Standardization (ISO)
- International Committee for IT Standards (INCITS)
- National Institute of Standards and Technology (NIST)

EFFECTIVE DATE

Issuance of this guidance represents approval by OEL management of the indicated guidance and related administrative forms.

HISTORY

Revised – June 30, 2014. Issued – July 1, 2014. Issued – July 1, 2015

ATTACHMENTS

Information Technology Policy and Procedures Manual

If you have questions or concerns regarding the guidance provided here, please contact the OEL Service Desk at (850) 717- 8600 or email Service.Desk@OEL.MyFlorida.com

Office of Early Learning
Information Technology Policy and Procedures Manual

TABLE OF CONTENTS

POLICY NUMBER/SUBJECT:

5.05 APPLICATION AND DATA SERVICES ROLES AND RESPONSIBILITIES

PURPOSE/SCOPE:

Information system development and management is a repetitive process that must include active involvement and strong commitment from all Office of Early Learning (Office) employees. This policy assures the Office has

- the best information resource management system to support our business and strategic goals.
- Office personnel who are informed of, competent in and capable of using information resource technology to enhance our effectiveness and efficiency.
- the technological capacity to develop, maintain and support Office's information systems goals and objectives.

When filling vacancies, managers should fill positions with individuals that have Application and Data Services experience in addition to their specific job skills. These individuals will work with personnel from the Application and Data Services (ADS) division to develop processes for the Office's business needs.

All Office employees, contract employees, vendors and others who do official business with Office are expected to comply with the provisions of this policy.

I. REFERENCES:

A. Chapter 282, Florida Statutes; Communications and Data Processing.

B. Section 815, Florida Statutes

C. Rule 71A-1, Florida Administrative Code

II. DEFINITIONS

Employees - Individuals employed in an established position in the Senior Management Service, Selected Exempt Service, Career Service, or paid from Other Personnel Services funds. For purposes of this policy, employees also include personal services contractors, consultants and experts hired on contract.

Information Technology Services Officer (ITSO) - Senior manager or member of executive staff responsible for developing, implementing and maintaining an ISSP for the Office.

III. ROLES AND RESPONSIBILITIES

A. Application and Data Services (ADS) roles and responsibilities.

1. The Application and Data Services group will be responsible for the following:
   a. Administration of the Office's information resource management and communications programs.
   b. Providing staff highly trained in information resource management and technology.
   c. Ensuring the integrity and safeguarding of the data within the Office's computers and networks.
   d. The development, acquisition, maintenance and operational support of all Office mission critical applications (mission critical applications are those whose poor performance or failure will degrade or harm the performance and management of the Office).

e. Developing, publishing and distributing procedures, directives, policy statements, rules, standards and guidelines for information resources.

f. Overseeing computer systems developed or acquired by employees to solve particular business needs.

g. Providing consulting services to employees on Application and Data Services issues to make the most efficient use of the appropriate technology for a particular application.

h. Testing and certifying hardware and software.

i. Serving as coordinator for the distribution of hardware and software to employees.

j. Establishing and directing quality assurance monitoring to assure integration and smooth functioning of all information resources.

2. Additional roles and responsibilities.

a. All employees share the responsibility of protecting the Office's information resources and adhering to the Office's policy regarding their usage.

b. The office Chief Information Officer (CIO) will monitor, evaluate and report the status of Office's information management system to executive management. The CIO will ensure the Application and Data Services business objectives align with the Office Long Range Strategic Plan, including an analysis of the risks involved with Application and Data Services decision-making. CIO responsibilities are set in statute and may be undertaken by an Office deputy director.

c. Office: IT Security Lead: The Application and Data Services security lead will work with the Office Information Technology Services Officer and the Agency CIO to develop, implement and maintain an Information Systems Security Plan for Office. The Office IT security lead will ensure the confidentiality, integrity and availability of Office's information resources via formal policies, awareness training and security controls.

The IT security lead will work with the CIO to assess risk, develop policies and procedures, provide security guidance, assist Office business units in conducting compliance reviews and ensure investigation of information security incidents. The information security lead may establish working groups regarding security matters.

d. Office: IT Help Desk Lead: The IT Help Desk lead will provide the project oversight and administrative duties to ensure the Application and Data Services group optimally performs Office's stated goals and objectives related to Application and Data Services. The person holding this position acts as the principal liaison between Office personnel and support staff at FDOE in all matters regarding the good function of integrated information resources.

e. Information Owners - While the day-to-day function of administering and protecting data is the responsibility of Office's Application and Data Services group, information owners will have final responsibility for their information resources. Information owners are responsible for the following:

1. Categorizing their business processes, information and systems according to a standard policy or framework.

2. Ensuring the information resources they own are adequately protected based on their classification and the level of risk.
3. Authorizing access to information resources based on a need-to-know.
4. Communicating procedures for securely transferring information resources to information users.
5. Delegating stewardship of information resources to an information custodian.
6. Authorizing information users and custodians and identifying these employees to ADS.
7. Ensuring employees understand their information security responsibilities and taking disciplinary actions related to employee violations of IT policies, procedures and guidelines.

IV. POLICY AND GUIDELINES

INCORPORATED ADS POLICIES

The following ADS policies are related to this guidance and incorporated in this manual. Each may be updated and approved independently without revising this manual.

5.05.01 - IT Customer Support (CIO Office).
5.05.02 - IT Security and Risk Mitigation Services.
5.05.03 - Server Administration Services.
5.05.04 - Network Services.
5.05.05 - Electronic Communications Service.
5.05.06 - Help Desk.
5.05.07 - Desktop Computing Services.
5.05.08 - Data Services.

POLICY NUMBER/SUBJECT:
5.05.01 APPLICATION AND DATA SERVICES

PURPOSE/SCOPE:

This policy establishes the duties and responsibilities of the Application and Data Services group, including planning, project management and administrative duties. This policy's scope includes all employees and consultants associated with the Application and Data Services group and all affiliated contractors.

I. REFERENCES

A. Rule 71A-2.001-2.010, Florida Administative Code; Florida Information Resource Security Policies & Standards

II. DEFINITIONS

CIO - Chief Information Officer
Office - Office of Early Learning (the Office).
ADS - Application and Data Services Support Services.
Senior staff - those managers or consultants selected by the director or the deputy director for positions of special responsibility.

ROLES AND RESPONSIBILITIES

A. The ADS group, under the leadership of the CIO, supports all operations, logistic and administrative duties ensuring optimal technological support of Office's stated mission and goals.

B. ADS supervisors manage the business aspects of the Application and Data Services group including: day-to-day operational support of information resources, data services and analysis, contract review and analysis, budget analysis, quotes, reviewing/approving IT purchase requests and strategic planning impact analysis.

III. POLICY AND GUIDELINES

INCORPORATED ADS POLICIES

The following ADS policies are related to this guidance and incorporated in this manual. Each may be updated and approved independently without revising this manual.

5.05.01.01 - Application and Data Services Strategic Planning/Management.
5.05.01.02 - Policy, Standard and Procedure Management.
5.05.01.03 - IT Project Management.
5.05.01.04 - IT Change Management.

POLICY NUMBER/SUBJECT:

5.05.02 IT SECURITY/RISK MITIGATION SERVICES

PURPOSE/SCOPE:

This policy implements Office's Information Systems Security Program, establishing responsibilities and operating policies ensuring an adequate level of information security for all information collected, created, processed, transmitted, stored or disseminated on Office information systems. All Office employees, contract employees, vendors and others who do official business with Office are expected to comply with the provisions of this policy.

I. REFERENCES:

A. 18 U.S.C. 1030, Fraud and Related Activities in Connection with Computers

B. 5 U.S.C. 552A, Records Maintained on Individuals and The Privacy Act of 1974

C. 5 C.F.R. Part 2635, Standards of Ethical Conduct for Employees of the Executive Branch

D. 5 C.F.R. Part 735, Employee Responsibilities and Conduct

E. Chapter 815, Florida Statutes; Computer Related Crimes

F. Clinger-Cohen Act of 1996, PL 104-106, February 1996

G. Computer Abuse Amendments Act of 1994, PL 103-322, September 1994

H. Computer Fraud and Abuse Act of 1986, PL 99-474, October 1986

I. Computer Security Act of 1987, PL 100-235, January 1988

J. Federal Information Processing Standard (FIPS)

K. Federal Information Security Management Act (FITSOA), PL 107-347, December 2002

L. Federal Managers Financial Integrity Act of 1982 PL 97-255 (H.R. 1526)

M. Foreign Corrupt Practices Act of 1977, as amended, PL 95-213, December 1977

N. Homeland Security Presidential Directive /HSPD-7, December 2003

O. NIST Special Publication 500-153, 800 Series

P. Executive Order 12674, April 12, 1989, Part I, Principles of Ethical Conduct

Q. Presidential Decision Directive 67, Continuity of Operations, October 21, 1998

R. Rule 71A-2.001-2.010, FAC (Florida Information Resource Security Policies & Standards)

II. DEFINITIONS

Employees - Individuals employed in an established position in the Senior Management Service, Selected Exempt Service, Career Service, or paid from Other Personnel Services funds. For purposes of this policy, employees also include personal services contractors, industrial contractors, consultants and experts hired on contract.

Information custodians - Individuals who maintain or administer information resources on behalf of information owners.

Information owners - Individuals ultimately responsible for information resources, who are generally executive management, or designated senior managers. The initial owner is the individual who creates, or initiates the creation or storage of, information. Once information is created or stored, the individual's respective Office business unit becomes the owner, with the executive management of that unit taking official responsibility. Acts as or appoints the Information Systems Security Officer for the business unit.

Information resources - Equipment, facilities, software and data that are designed, built, operated and maintained to collect, record, process, store, retrieve, display and transmit information.

Information Technology Services Officer (ITSO) - Senior manager or member of executive staff responsible for developing, implementing and maintaining an ISSP for Office.

Information Security Training and Awareness Program - A program to maintain effective awareness of information security policy, standards and acceptable practices.

Information Systems Security Program (ISSP) - The multiple components which comprise the 'program' aimed at protecting the confidentiality, integrity and availability of Office information systems resources.

Information Users - Individuals who use or have access to Office's information resources, including employees, vendors and visitors.

Risk Management - The process of identifying, assessing and taking steps to reduce risk to an acceptable level. The risk management process allows the Office to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data that support the Agency's mission.

Security Incident - Any activity that is a threat to the availability, integrity, or confidentiality of the Office's information resources, or any action that is in violation of this policy or its implementing administrative orders.

Supervisors - Office employees who have formal supervisory responsibility for employees, contractors, or other information users. This includes managers and other supervisory personnel.

III. ROLES AND RESPONSIBILITIES

All employees share the responsibility of protecting the Offices's information resources and adhering to the Office's policy regarding their usage.

A. The Information Technology Services Officer (ITSO) will develop, implement and maintain an ISSP for Office. The ITSO will ensure the confidentiality, integrity and availability of Office information resources via formal policies, awareness training and security controls. The ITSO will assess risk, develop policies and procedures, provide security guidance, and assist in conducting compliance reviews and ensure investigation of information security incidents. The ITSO may establish working groups regarding security matters.

B. The ITSO will develop, implement and maintain an ISSP for a specific system/application within a business unit of Office. The ITSO will ensure the confidentiality, integrity and availability of their system's information resources through support of formal policies, awareness training, compliance monitoring and security controls. The ITSO will assess risks, develop policies and procedures, provide security guidance, conduct compliance reviews and ensure investigation of information security

incidents related to their system. The ITSO may establish working groups regarding security matters. The ITSO will ensure employees, contractors and any other individual granted access to information systems sign an appropriate individual confidentiality agreement.

C. Information Owners - While the day-to-day function of administering and protecting data is the responsibility of an information custodian, information owners will have final responsibility for their information resources. Information owners are responsible for the following:

1. Delegating security responsibilities by designating an ITSO.
2. Categorizing their business processes, information and systems according to a standard classification framework developed by the ITSO.
3. Ensuring the information resources they own are adequately protected based on their classification and the level of risk.
4. Authorizing access to information resources based on a need-to-know.
5. Communicating procedures for securely transferring information resources to information users.
6. Delegating stewardship of information resources to an information custodian.

D. Information custodians must be authorized in writing by information owners.

E. Supervisors are responsible for ensuring their employees understand their information security responsibilities and for taking disciplinary actions related to employee violations of ISSP policies, procedures and guidelines.

IV. POLICY AND GUIDELINES

A. The Office Information Systems Security Program (ISSP) consists of a set of information security protocols, as well as standards, procedures and guidelines for their implementation. These protocols are contained in the Office Information Systems Security Program Handbook ("ISSP Handbook") which will be followed by all Office employees, contract employees, vendors and others who do official business with Office. The ISSP Handbook is incorporated in this manual as a part of Office policy for all employees.

B. The Information Technology Services Officer (ITSO) will educate Office employees (and when necessary, individuals doing official business with the Office) about information security and the protocols and procedures with which they must comply, by implementing an Information Security Training and Awareness Program. The program will include both periodic training classes as well as an ongoing security awareness campaign designed to maintain vigilance toward information security. New employees will receive information security training within 30 days of their employment start date as part of the orientation process. Awareness and training in security will include on-going education and continual reinforcement of the value of security. Once trained, employees will sign an agreement that they understand and will comply with the Office's information security policies. information owners and ITSO's will also provide training to information users regarding the security policies and procedures for their specific systems.

C. Risk Management will be integrated into the Office's decision-making and systems development life cycle.

D. An annual review will be conducted to determine any necessary changes to any portions of the ISSP policy. All changes will be routed for approval following the Office policy approval process.

V. VIOLATION OF THIS POLICY MAY RESULT IN LOSS OR LIMITATIONS ON USE OF INFORMATION RESOURCES AS WELL AS DISCIPLINARY OR LEGAL ACTION, INCLUDING TERMINATION OF EMPLOYMENT OR REFERRAL FOR CRIMINAL PROSECUTION.

POLICY NUMBER/SUBJECT:

5.05.02.01 ACCEPTABLE USE OF INFORMATION RESOURCES

PURPOSE/SCOPE:

This protocol establishes Office procedures for acceptable use of information resources and applies to all users of Office information resources, individuals using information resources belonging to the State of Florida must act in a legal, ethical, responsible and secure manner, with respect for the rights of others.

I. REFERENCES:

A. Chapter 282, Florida Statutes; Communications and Data Processing

B. Rule 71A-2.001-2.010, Florida Administrative Code; Florida Information Resource Security Policies & Standards

C. Section 110.227, Florida Statutes

D. Chapter 282, Florida Statutes

E. Rule 60L-36, Florida Administrative Code

F. Health Insurance Accountability and Portability Act (HIPPA)(Public Law 104-191(1996))

G. Chapter 815, Florida Statutes

H. Title 17 of the United States Code

I. Governor's Code of Ethics

J. Florida's Office of Early Learning Policy 4.04 Communications Equipment

II. DEFINITIONS

Access - The right to enter or make use of a computer system. To approach, view, instruct, communicate with, store data in, retrieve data from, or otherwise make use of computers or information resources.

Administrative Access - Enhanced privilege level that allows the user to perform administration of the system.

Account - A set of privileges for authorization to system access, which are associated with a userid.

Information Resources - The procedures, equipment, facilities, software and data that are designed, built, operated and maintained to collect, record, process, store, retrieve, display and transmit information.

Audit Trail - In computer security systems, a chronological record of system resource usage. This includes user login, file access, other various activities and whether any actual or attempted security violations occurred, legitimate and unauthorized.

Information Custodians - Individuals (e.g., IT staff) who maintain or administer information resources on behalf of Information Owners. They are guardians or caretakers who are charged with the resource owner's requirements for processing, telecommunications, protection controls and output distribution for the resource.

Information Owners - The individuals ultimately responsible for information resources and are generally deputy directors or designated senior managers. The initial owner is the individual who creates, or initiates the creation or storage of, information. Once information is created or stored, the individual's respective Office business unit becomes the Owner, with the Manager of that unit taking official responsibility.

Information Technology Services Officer (ITSO) - Directs the organization's day-to-day management of its Information Security Program. This individual is also responsible for coordinating all security-related interactions among organizational elements involved in the Information Systems Security Program.

Information users - Individuals who use or have access to Office's information resources, including associates, vendors and visitors.

Password - Any secret string of characters which serves as authentication of a person's identity (personal password), or which may be used to grant or deny access to private or shared data (access password).

Personal Use - Activity that is conducted for purposes other than accomplishing official or otherwise authorized activity.

System Administrator - A designated individual who has special privileges to maintain the operation of a computer application or system.

III. ROLES & RESPONSIBILITY

A. Information users are responsible for the following:

1. Using information resources responsibly and in compliance with all Office information security policies and guidelines, and
2. Reporting any suspected inappropriate use of information resources to either their manager or the ITSO.

B. Supervisors are responsible for the following:

1. Ensuring their personnel understand Office protocol regarding acceptable usage of information resources.
2. Monitor their associates' use of information resources (Report any suspicious activity to the ITSO).

C. Information owners are responsible for implementing measures to protect their resources against inappropriate use.

D. Information custodians are responsible for assisting information owners with implementing measures to protect their resources against inappropriate use.

E. The Information Technology Services Officer (ITSO) is responsible for auditing usage of the Office information resources to ensure compliance with policies and guidelines.

IV. POLICY AND GUIDELINES

A. Policy

1. Inappropriate use of information resources exposes the Office to risks including compromise of systems and services, legal issues, financial loss and damage to reputation. The purpose of this protocol is not to impose restrictions that are contrary to the Office's established culture of openness, trust and integrity, but to protect the Office's associates and the government from illegal or damaging actions by individuals, either knowingly or unknowingly.

2. Access to computers, computing systems and networks owned by the government is a privilege which imposes certain responsibilities and obligations and which is granted subject to Office policies and guidelines and governing laws. This protocol sets forth the principles that govern appropriate use of information resources and is intended to promote the efficient, ethical and lawful use of these resources. Individuals using information resources belonging to the government must act in a responsible manner and with respect for the rights of others.

B. Guidance

1. Employees will use Office-provided information resources for Office-related business in accordance with their job functions and responsibilities, except as otherwise provided by management directives or other Office policies.
2. Associates are permitted limited personal use of information resources if the use does not result in a loss of associate productivity, interfere with official duties or business and involves minimal additional expense to the government. Unauthorized or improper use of information resources may result in loss of use or limitations on use of those resources.
3. When using government information resources, associates are expected to:
    a. Act responsibly so as to ensure the ethical use of Office information resources in compliance with the Standards of Ethical Conduct for State Employees.
    b. Acknowledge the right of the Office to restrict or rescind computing privileges at any time.
    c. Use security measures to protect the confidentiality, integrity and availability of information, data and systems.
    d. Act professionally in the workplace and to refrain from using government information resources for activities that are inappropriate.
    e. Respect all pertinent licenses, copyrights, contracts and other restricted or proprietary information.
    f. Use good judgment in accessing the Internet. Each use of the Internet should be able to withstand public scrutiny without embarrassment to the Office or the federal government.
    g. Safeguard their user IDs and passwords and use them only as authorized. Any actions taken under an assigned identification (e.g., userid) are the responsibility of the user.
    h. Respect government property.
    i. Make only appropriate use of data to which they have access.
    j. Exercise good judgment regarding the reasonableness of personal use.
    k. Use information resources efficiently.
4. The following activities are strictly prohibited:
    a. Intentionally corrupting, misusing, or stealing software or any other computing resource.
    b. Accessing Office systems that are not necessary for the performance of the associate’s duties.
    c. Performing functions that are not related to the associate’s job responsibilities on systems that they are otherwise authorized to access.

d. Making unauthorized changes to Office computer resources, including installation of unapproved software or interfering with security measures (such as audit trail logs and antivirus software).

e. Copying Office proprietary software or business data for personal or other non-government use.

f. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music and the installation of any copyrighted software for which Office or the end user does not have an active license.

g. Disseminating trade secrets or business confidential information, except as permitted by law or regulation.

h. Transmitting, storing, or processing classified data except as authorized and in accordance with the Office Information Systems Security Plan.

i. Unauthorized access to other computer systems using Office information resources.

j. Accessing information resources, data, equipment, or facilities in violation of any restriction on use, such as Peer-to-Peer.

k. Using government computing resources for personal or private financial gain.

l. Using another person's computer account, with or without their permission.

m. Implementing any computer systems without authorization from the Office IT Unit.

n. Knowingly, without written authorization, executing a program that may hamper normal Office computing activities, such as Peer-to-Peer.

o. Adding components or devices (e.g., PDAs, thumb drives, cameras, etc) to Office desktops without explicit approval from the IT Manager or the IT Manager designee.

p. Knowingly introducing malicious programs into the network or server (e.g., viruses, worms, Trojan horses, Email bombs, etc.).

q. Revealing account passwords to others or allowing the use of one’s account by others, including family and other household members when work is being done at home.

r. Revealing system passwords (e.g. Office system passwords, database passwords, etc) to anyone who is not specifically authorized to use them.

s. Exporting software, technical information, encryption software, or technology, in violation of international or regional export control laws.

t. Effecting security breaches or disruptions of network communication.

u. Unauthorized security scanning, network monitoring, or data interception that is not part of the associate’s regular job duties.

v. Circumventing any Office information security measures.

w. Interfering with or denying service to other information resource users, such as using Peer-to-Peer.

x. Providing information about, or lists of, Office associates to parties outside of the government that are not required for Office business.

y. Sending unsolicited Email messages (spam).

z. Any form of harassment via Email, telephone, pager, IRC, SMS, or other communication method, whether through language, frequency, or size of messages.

aa. Creating or forwarding "chain letters," "Ponzi," or other "pyramid" schemes of any type.

bb. Engaging in any outside fund-raising activity, endorsing any product or service, participating in any lobbying activity, or engaging in any partisan political activity without specific permission from Office.

cc. Posting agency information to external news groups, bulletin boards or other public forums without authority, or conducting any activity that could create the perception that communication was made in one's official capacity as a Federal government associate, unless appropriate Office approval has been obtained.

dd. Any personal use that could cause congestion, delay, or disruption of service to any government system or equipment, such as Peer-to-Peer.

ee. Using government office equipment or information resources for activities that are illegal, inappropriate, or offensive to fellow associates or the public. This includes, but is not limited to, materials related to:

1) Sexually explicit or sexually oriented content.
2) Ethnic, racial, sexist, or other offensive comments.
3) Anything that is in violation of sexual harassment or hostile workplace laws.
4) Making fraudulent offers of products, items, or services.
5) Gambling.
6) Illegal weapons or terrorist activities, and
7) Planning or commission of any crime.

ff. Forging or misrepresenting one's identity.

5. Auditing and Privacy:

a. All use of Office information resources may be monitored by Office.

b. Employees do not have an expectation of privacy or anonymity while using any government information resource at any time, including accessing the Internet and Email.

c. Users agree to be governed by acceptable usage policies and to have their usage audited. By using government office equipment, associates imply their consent to disclosing the contents of any files or information maintained or passed-through government office equipment.

d. To the extent that employees wish that their private activities remain private, they should avoid using agency office equipment such as their computer, the Internet, or Email, for those activities.

e. Auditing procedures will be implemented to ensure compliance with Office security policies.

f. System administrators have the ability to audit network logs, employ monitoring tools and perform periodic checks for misuse.

g. Employees agree to be bound by the conditions for continued use of Office information resources: Employees and contractors will sign an agreement to comply with Office information security protocol.

h. Usage of Office IT resources for illegal purposes will be reported to appropriate authorities.

V. ENFORCEMENT

Unauthorized or improper use of government information resources could result in loss or limitations of use of these resources, as well as disciplinary and/or legal action, including termination of employment or referral for criminal prosecution.

SUBJECT/POLICY NUMBER:

5.05.02.02 INFORMATION RESOURCES

PURPOSE/SCOPE:

This establishes policy for all Office information systems and data created, owned, stored, or transferred by the Office that are not designated as secure or classified.

I. REFERENCES:

A. FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems

B. Special Publication 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories

C. 4.09 Records Management Policy, Florida's Office of Early Learning

II. DEFINITIONS

Information Resources - The procedures, equipment, facilities, software and data that are designed, built, operated and maintained to collect, record, process, store, retrieve, display and transmit information.

III. ROLES AND RESPONSIBILITIES

Information owners are responsible for the following:

Categorizing their resources in accordance with Office's classification framework.

Ensuring their resources are protected commensurate with their categorization level.

Information Systems Security Officer (ITSO) is responsible for the following:

Developing and communicating Office's information classification framework.

Assisting information owners with assessing the classification level of their resources.

Auditing to ensure compliance with this protocol.

IV. POLICY AND GUIDELINES

In order to ensure appropriate levels of protection are applied to information resources, a framework is needed to classify those resources based on their criticality to the Office and the confidentiality of the data that they contain.

This includes developing procedures and standards for assessing the criticality and confidentiality of the systems and determining minimum security requirements based on those classification levels.

A. All Office information resources will be categorized based on Office's information classification framework.

B. Risks and threats to information resources will be assessed and security measures will be applied, based on the resource's classification level, in accordance with Office risk management procedures.

C. The Office's information classification framework will be based on the reference guidance and subsequent publications.

V. ENFORCEMENT

Violation of this protocol could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment or referral for criminal prosecution.

SUBJECT/POLICY NUMBER:

5.05.02.03 RISK MANAGEMENT

PURPOSE/SCOPE:

This policy establishes a risk management protocol ensuring appropriate safeguards are employed to protect Office resources. This protocol applies to all Office information resources

I. REFERENCES:

A. FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems

B. Special Publication 800-60, Guide for Mapping Types of Information and Information Systems to Security Categories

C. 4.09 Records Management Policy, Florida's Office of Early Learning

II. DEFINITIONS

Availability - Assuring information and communications services will be ready for use when expected.

Confidentiality - Assuring information will be kept secret, with access limited to appropriate persons.

Integrity - Assuring information will not be accidentally or maliciously altered or destroyed. Information has integrity when it is timely, accurate, complete and consistent.

Risk - The possibility of something adversely affecting the confidentiality, availability and integrity of Office's information resources.

Risk Assessment - The process of analyzing and interpreting risk. Risk assessment is used to identify security risks, examine threats to and vulnerabilities of systems, determine the magnitude of risks, identify areas needing safeguarding and determine the acceptability of risk.

Risk Management - The process of identifying risk, assessing risk and taking steps to reduce risk to an acceptable level. The risk management process allows Office to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data that support Office's mission.

Threat - A circumstance, event, or person with the potential to cause harm to a system in the form of destruction, disclosure, data modification and/or Denial of Service (DoS).

Vulnerability - Any characteristic of a computer system that renders it susceptible to destruction or incapacitation. A design, administrative, or implementation weakness or flaw in hardware, firmware, or software that, if exploited (either intentionally or accidentally), could lead to an unacceptable impact in the form of unauthorized access to information or disruption of critical processing.

Vulnerability Testing - Systematic examination of a system to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures and confirm the adequacy of such measures after implementation.

III. ROLES & RESPONSIBILITIES

A. information owners and Office managers are responsible for the following:

1. Committing to performing on-going periodic risk management of information resources.
2. Considering the results of a risk assessment in making decisions about the use of information resources.
3. Implementing appropriate safeguards based on the results of risk analysis.

B. Information Custodians are responsible for Assisting with the assessment and mitigation of risks for the information resources with which they have been entrusted.

C. Information Systems Security Officer (ITSO) is responsible for the following:

1. Developing Office risk management procedures.
2. Conducting risk assessments on Office information systems.
3. Identifying potential threats to the confidentiality, integrity and availability of Office information resources.
4. Performing vulnerability testing in accordance with Office policies and procedures.
5. Providing recommendations for the cost-effective mitigation of risks to information resources.

IV. POLICY AND GUIDELINES

In determining a security strategy for a system or the organization, the Office will determine the correct balance between mitigating risks and expending resources. Appropriate controls must be implemented to protect against the occurrence of serious threats to the business, while addressing financial and operational concerns. The objective of performing risk management is to enable Office to accomplish its mission by the following:

A. Better securing the IT systems that store, process, or transmit organizational information.

B. Enabling management to make well-informed risk management decisions to justify the expenditures that are part of an IT budget.

C. Assisting management in authorizing (or accrediting) their IT systems on the basis of the supporting documentation resulting from the performance of risk management.

D. Risk management is an essential management function and should not be treated solely as a technical function relegated to IT operational or security personnel for implementation. Effective risk management processes support sound risk-based decision-making.

E. Office will use a risk-based approach which includes vulnerability scanning to determine information security requirements to ensure security is commensurate with the risk and magnitude of harm that can result from the loss, misuse, unauthorized access to, or modification of, Office information.

F. Office management will make all Application and Data Services decisions based on a thorough analysis of the risks involved.

G. Risk management procedures must be integrated into the Office's systems development life cycle (SDLC). Risk management is an iterative process and has activities relevant to every phase of the life cycle. Security considerations must be included in the initiation, development/acquisition, implementation, operation/maintenance and disposal of all Office information resources.

H. Risk management is a cyclical process and will be performed on an ongoing basis for all information resources.

I. The Office will adhere to NIST guidance as set forth in Special Publication 800-30, Risk Management and subsequent publications.

V. ENFORCEMENT

Violation of this protocol could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment or referral for criminal prosecution.

SUBJECT/POLICY NUMBER:

5.05.02.04 SECURITY TRAINING AND AWARENESS

PURPOSE/SCOPE:

The Office's Information System Security Program protocols and procedures will be communicated to all associates. A program to maintain effective awareness of information security protocol, standards and acceptable practices will be implemented. This protocol applies to all Office associates and contractors, including interns and temporary workers, who have access to Office information resources. The term "associates" is used in this protocol to specify all personnel within this scope.

I. REFERENCES:

A. Federal Information Security Management Act (FITSOA)

B. NIST Special Publication 800¬-50, Building an Application and Data Services Security Training and Awareness Program

C. Office of Management and Budget (OMB) Circular A-130

II. DEFINITIONS

Awareness - A state of focused attention on security that allows individuals to recognize IT security concerns and respond accordingly.

III. ROLES & RESPONSIBILITIES:

A. The Information Systems Security Officer (ITSO) is responsible for developing and operating the Information Security Training & Awareness program, including the following:

1. Preparing protocol on security awareness.
2. Assisting Office staff and early learning coalitions with security related issues and questions.
3. Developing and distributing awareness material and bulletins and ensuring all personnel receive the appropriate security training associated with their jobs and maintaining records of training provided.

B. Supervisors are responsible for the following:

1. Ensuring their associates are briefed and understand their roles in implementing Office's Information Security program.
2. Communicating changes in policies and procedures to their staff.
3. Providing opportunities for staff to complete information security training.
4. Assisting with the monitoring of information security compliance within their departments.

C. Employees are responsible for the following:

1. Completing security training as mandated by Office training policy.
2. Reviewing and understanding Office information security policies and procedures.
3. Complying with all Office information security policies and procedures.

D. information owners are responsible for ensuring personnel who use their resources are appropriately trained to fulfill their security responsibilities for those resources.

IV POLICY AND GUIDELINES

Aside from compliance with legal requirements, a Security Training and Awareness program is crucial to the safeguarding of Office information resources. Information security protocol and standards cannot be effective unless everyone at Office, regardless of position in the organization, is aware of the importance of security, understands Office security procedures and performs required practices.

To make information security effective, standards and procedures must be known, understood, believed to be beneficial and be appropriately and consistently practiced.

Information Security is not a one-time event, but a continuous effort and "state of mind". This is achieved by reinforcing concerns and appropriate behaviors on a continuous basis. Effective information security is achieved when it becomes part of everyone's thinking with regard to daily operations and assignments.

A. Office will develop and maintain an Information Security Training and Awareness Program in accordance with Office's training policy. The purpose of the Security Training and Awareness program is to educate associates about information security policies and procedures and make them aware of their roles and responsibilities in safeguarding Office's information resources. The program will be composed of two major initiatives:

   1. A Training program designed to build relevant and needed security skills and competencies to facilitate job performance.

   2. An Awareness program designed to focus attention on security and to change behavior or reinforce good security practices. Ongoing development of security awareness builds a culture that encourages good security practices.

B. All employees will complete training on Office Information security policies and procedures. Information security training will be incorporated into the orientation processes for all new staff. Training must be completed within 30 days of employment or initiation of contract and refresher trainings as specified in Office training policy.

C. Employees and contractors will be made aware of the penalties for non-compliance with Office security policies and procedures.

D. Materials will be posted or presented in a variety of formats on a regular basis to maintain employee awareness of information security issues.

E. Changes to Office information security policies or procedures will be communicated to all information employees.

IV. ENFORCEMENT

VIOLATION OF THIS PROTOCOL COULD RESULT IN LOSS OR LIMITATIONS ON USE OF INFORMATION RESOURCES, AS WELL AS DISCIPLINARY AND/OR LEGAL ACTION, INCLUDING TERMINATION OF EMPLOYMENT OR REFERRAL FOR CRIMINAL PROSECUTION.

SUBJECT/POLICY NUMBER:

5.05.02.05 INCIDENT REPORTING

PURPOSE/SCOPE:

Office employees must report any suspected information security incidents using the procedures outlined in this protocol.

I. REFERENCES:

None.

II. DEFINITIONS

Security Incident - Any activity that is a threat to the availability, integrity, or confidentiality of information resources, or any action that is in violation of security policies.

III. ROLES AND RESPONSIBILITIES

A. Information users are responsible for reporting suspected incidents to the ITSO or information owner immediately, using the procedures set forth in this protocol.

B. Supervisors are responsible for ensuring their associates understand and adhere to incident reporting policies and procedures and for ensuring security incidents are reported as quickly as possible.

C. Information Systems Security Officer (ITSO) is responsible for the following:

1. Developing and maintaining incident reporting and handling procedures.
2. Researching, documenting, resolving and tracking reported incidents.
3. Reporting incidents to upper management and appropriate external entities.
4. Determining if incident follow-up is needed.

D. Information Custodians are responsible for the following:

1. Reporting any incidents they encounter to the ITSO;
2. Researching and resolving incidents within their administrative domain;
3. Providing documentation of incidents and steps taken to resolve them to the ITSO; and
4. Fully cooperating with and assisting the ITSO with incident handling as requested.

E. System Administrators are responsible for assisting the ITSO with research, documenting, resolving and tracking reported incidents.

IV. POLICY AND GUIDELINES

A. Maintaining the security of Office information resources requires cooperation and participation from everyone. It is important that all information users maintain vigilance regarding information security and immediately report any suspected incidents in order to minimize potential damage to Office.

B. The Office's security incident reporting protocol and procedures enable The Office to quickly and efficiently recover from security incidents; respond in a systematic manner to incidents and carry out all

the necessary steps to correctly handle an incident; prevent or minimize disruption of critical computing services; and minimize loss or theft of confidential or mission-critical information.

V. ENFORCEMENT

Violation of this protocol could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment or referral for criminal prosecution.

SUBJECT/POLICY NUMBER:

5.05.02.06 INCIDENT RESPONSE

PURPOSE/SCOPE:

The Office will be able to respond to computer security-related incidents in a manner that protects its own information and helps to protect the information of others that might be affected by the incident. This policy applies to all Office information users, owners and custodians.

I. REFERENCES

A. The Federal Information Security Management Act (FITSOA)

B. OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Systems

II. DEFINITIONS

Security Incident - Any activity that is a threat to the availability, integrity, or confidentiality of information resources, or any action that is in violation of security policies.

Critical Incident - An incident that could result in a severe impact to Office resources if not addressed quickly.

III. ROLES AND RESPONSIBILITIES

A. The Information Systems Security Officer (ITSO) is responsible for the following:

1. Preparing protocol guidelines for establishing and implementing a computer security incident response capability.
2. Developing incident response procedures.
3. Working with law enforcement, the users, information owners and system administrators to formulate and implement a response plan.
4. Notifying the information owners and Office management of significant incidents and the response plan.
5. Ensuring all incidents and resolution activities are fully documented and tracked.
6. Providing information on incidents to the Department of Homeland Security/US-CERT.

B. Information users are responsible for the following actions if they suspect a security incident may have occurred:

1. Understanding and complying with the Office's incident handling procedures.
2. Documenting all relevant information about the suspected incident.
3. Sharing the suspicion and information with their manager and/or the ITSO.
4. Fully cooperating with and assisting the ITSO, system administrators and other designated personnel with resolution of the incident as requested.

C. Supervisors are responsible for the following:

1. Ensuring their associates understand Office incident response protocol and procedures;
2. Contacting the ITSO within one working day after the incident; and
3. Providing incident-related information to the ITSO when requested.

D. information owners are responsible for the following:

1. Ensuring incident response procedures are in place for their resources;
2. Informing Office management of significant incidents (major compromise of data, denial of service); and
3. Providing follow up to ensure incidents have been resolved.

E. Information Custodians are responsible for the following:

1. Assisting with evaluation and mitigation of the incident;
2. Working with the ITSO, system owner and/or users, to formulate and implement a response plan; and
3. Documenting and reporting steps taken to handle the incident to the ITSO.

IV. POLICY AND GUIDELINES

References A. and B. require all organizations to have an incident response capability and to share information concerning common vulnerabilities and threats.

This policy establishes a formally documented and clearly understood incident response process that will make it possible for the Office to respond quickly and effectively to situations that might compromise the Office's information resources.

A. All reported security incidents will be responded to quickly and in adherence to Office Information Security incident handling procedures.

B. The Office will establish Information Security Incident Response procedures to address computer security incidents, including theft, misuse of data, intrusions, hostile probes and malicious software.

C. When an incident occurs, the information user or their supervisor must provide a verbal report to the ITSO within one working day after the incident. Critical incidents must be reported immediately.

D. A written preliminary report must be completed within two working days using the Office's incident reporting form. This report is to be completed by the individual handling the incident. Within five working days of the resolution of an incident, a written final report must be submitted. In cases where incident resolution is expected to take more than thirty days, a weekly status report must be submitted to the ITSO.

E. Priority in incident handling should be given to preventing further damage to Office information resources.

F. A log must be kept of all the actions taken, including triage steps and other regular or routine work performed on the affected systems. This log should be separate from normal system logs, since it may be used as evidence in a criminal prosecution if warranted.

G. The Office will enter into and maintain a cooperative agreement with the Department of Homeland Security/US-CERT to facilitate share incident information and provide assistance with incident resolution.

H. The Office will adhere to NIST guidance as set forth in Special Publication 800-61, Computer Security Incident Handling Guide and subsequent publications, as well as relevant guidance from US-CERT.

V. ENFORCEMENT

Anyone who violates this protocol is subject to disciplinary action, up to and including termination of employment.

SUBJECT/POLICY NUMBER:

5.05.02.07 SYSTEM SECURITY PLANS

PURPOSE/SCOPE:

Each major Office information system will have an approved security plan. This policy covers all major Office information systems and establishes an approved security plan for each.

I. REFERENCES

A. National Institute of Standards and Technology (NIST) Special Publication 800-18, Guide for Developing Security Plans for Application and Data Services Systems and subsequent publications

II. DEFINITIONS

Major Information System - An information system that requires special management attention because of its importance to an Office mission; high development, operating, or maintenance costs; or its significant role in the administration of Office programs, finances, property, or other resources.

Memorandum of Understanding (MOU) - A document providing a general description of the responsibilities that are to be assumed by two or more parties in their pursuit of some goal(s).

III. ROLES AND RESPONSIBILITIES

A. The Information Systems Security Officer (ITSO) is responsible for the following:

1. Assisting with the development and review of system security plans.
2. Auditing systems to ensure their security plans have been effectively implemented.

B. information owners are responsible for the following:

1. Ensuring system security plans are developed for the systems that they own.
2. Formally approving and accepting system security plans for their systems.
3. Information Custodians are responsible for assisting information owners and the ITSO with the development and implementation of system security plans.

IV. POLICY AND GUIDELINES

A security plan lists security requirements, defines risks and describes security measures to be implemented for a particular system. This helps to ensure a security risk analysis is performed for the system and that appropriate security controls are put in place. The security plan also defines roles and responsibilities for security of the system, as well as standard operating procedures.

Each new major information system must have an approved Security Plan before going into operation.

A. Owners of existing major information systems that do not have an approved Security Plan must develop one as soon as possible.

B. Each system security plan must be reviewed, updated and re-approved at least once every two years, or when there is a major change to the system, whichever is earlier.

C. The System Security Plan will be used as a critical component of the Certification and Accreditation of the system.

D. Other organizations or systems that are connected to or share data with the Office system must have a Memorandum of Understanding (MOU) or other formal documented agreement that describes the rules governing the interconnection.

E. System Security Plans must be marked, handled and controlled as confidential but unclassified information.

F. The Office will adhere to NIST guidance as set forth in.

V. ENFORCEMENT

Violation of this protocol could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment or referral for criminal prosecution.

SUBJECT/POLICY NUMBER:

5.05.02.08 CERTIFICATION AND ACCREDITATION (C&A)

PURPOSE/SCOPE:

Each of the Office's major information systems will be certified and accredited every 3 years or upon each significant change to the system (whichever comes first). This protocol establishes a procedure for certificate and accreditation of the Office's major information systems and applies to all major information systems at the Office.

I. REFERENCES

A. Federal Information Security Management Act (FITSOA)

B. National Institute of Standards and Technology (NIST) Certification and Accreditation, Special Publication 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems and subsequent publications

II. DEFINITIONS

Accreditation - A risk-based decision that determines whether an IT system should be allowed to operate under a particular security configuration. Accreditation is based on the facts, plans and schedules developed during Certification.

Certification - An assessment of the security controls of an information system.

Designated Approving Authority (DAA) - The senior management official or executive with the authority to approve the operation of an information system at an acceptable level of risk to Office operations (including mission, functions, image, or reputation), Office assets, or individuals.

General Support Systems - An interconnected information resource under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, facilities and people and provides support for a variety of users and applications. Individual applications support different mission-related functions. Users may be from the same or different organizations.

III. ROLES AND RESPONSIBILITIES

A. Designated Approving Authority (DAA) is responsible for the following:

1. Acting as the authorizing official for accreditation of IT resources;
2. Completing and signing C&A statements and forwarding them to the ITSO; and
3. Granting Interim Authority to Operate (IATO) and developing timeframes in which remedial actions must be taken.

B. Information Systems Security Officer (ITSO) is responsible for the following:

1. Developing and communicating the Office's C&A procedures;
2. Ensuring major information systems have been certified and accredited;
3. Assisting with the development of system security plans;

4. Conducting Security Testing & Evaluations (ST&E) of major information systems; and
5. Forwarding C&A statements to the DAA for review.

C. Information Custodians are responsible for the following:

1. Assisting information owners in ensuring major information systems are certified; and
2. Assisting the ITSO with conducting ST&E.

D. information owners are responsible for the following:

1. Ensuring C&A requirements are met for any major information systems they own, including developing a security plan for each system;
2. Notifying the ITSO when there is a significant change to the security posture of a major information system;
3. Reviewing C&A statements before they are signed by the DAA; and
4. Addressing any remedial action that must be taken subsequent to the ST&E.

IV. POLICY AND GUIDELINES

The purpose of Certification and Accreditation (C&A) is to ensure information systems have adequate security commensurate with the level of risk. To this end, C&A is the formalized process used to assess the risks and security requirements of each system and to determine whether the system's security needs are being met.

Reference A. requires the Office to perform C&A of its information systems. For each system, this process must be completed either every 3 years or when there is a change that affects the system's security posture.

A. Office will assign a senior executive to act as the Designated Approving Authority (DAA) to accredit Office information systems.

CERTIFICATION:

The Office's Certification program is implemented to test and evaluate technical and non-technical IT security features and other safeguards used by Office systems, in support of the Accreditation process.

1. Certification will not only address software and hardware security safeguards, but also procedures, physical protections and personnel security measures.
2. Security Testing & Evaluation (ST&E) will be performed during the Certification process to evaluate the effectiveness of security measures implemented for the system.
3. The following minimum requirements must be met for a system to be certified:
    a. The system must be thoroughly documented.
    b. A system security plan must be developed and approved.
    c. An ST&E of the system must be completed.
    d. A risk assessment must be conducted.
    e. Standard operating procedures must be developed for the system.
    f. The system must meet all applicable legal requirements and Office policies.
    g. A contingency plan must exist for the system.

ACCREDITATION:

The Office's Accreditation process will be used for obtaining official management authorization for the operation of an IT resource.

1. Accreditation will be in the form of a formal declaration by the DAA that an IT resource is approved to operate in a particular security mode using a prescribed set of safeguards.
2. The Accreditation determination will be based on findings, facts and support documents produced during the Certification process, as well as other management considerations.
3. An Accreditation statement, which affixes security responsibility with the accrediting authority (DAA), will be used to certify that proper attention has been afforded to the security of the IT resource.
4. The statement will address the residual risks associated with the respective system or network, subsequent to the implementation of countermeasures applied during the system test and evaluation.

B. Certification and Accreditation statements will be completed for all major applications and general support systems.

C. Information owners will review Certification and Accreditation statements before they are signed by the DAA.

D. An Interim Authority to Operate (IATO) may be issued in those cases in which systems must be implemented expeditiously, but the IATO should last no longer than 6 months and should only be granted if it does not pose a significant risk to Office information resources.

E. Existing operational systems that have not been certified and accredited within the last 3 years will undergo Certification and Accreditation within 1 year of the issue date of this order.

F. All new Office IT systems will be certified and accredited prior to being allowed into operation.

G. All systems will be recertified and reaccredited at least every three years or when there is a significant change to the security posture of the system, whichever is earlier.

H. The Office will adhere to NIST Certification and Accreditation guidance as required by Reference B. and subsequent publications.

V. ENFORCEMENT

Violation of this protocol could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment or referral for criminal prosecution.

SUBJECT/POLICY NUMBER:

5.05.02.09 VULNERABILITY TESTING

PURPOSE/SCOPE:

In order to assess the Office's information security posture and determine the security risks that should be mitigated, the Office will conduct periodic vulnerability assessments. These assessments will assist in the discovery of security vulnerabilities, gauge the threat posed by these vulnerabilities and assist the Office with decreasing security risk. This protocol establishes vulnerability testing procedures and applies to all Office owned or operated systems, networks, applications, data repositories and other information resources.

I. REFERENCES

A. Federal Information Security Management Act (FITSOA)

B. National Institute of Standards and Technology (NIST) Guideline on Network Security Testing, Special Publications 800-42.

C. NIST, Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme, Special Publications 800-51.

D. NIST, Techniques and Procedures for Verifying the Effectiveness of Security Controls in Information Systems, Special Publications 800-53A.

II. DEFINITIONS

Threat - A circumstance, event, or person with the potential to cause harm to a system in the form of destruction, disclosure, data modification and/or Denial of Service (DoS).

Vulnerability - Any characteristic of a computer system that renders it susceptible to destruction or incapacitation. A design, administrative, or implementation weakness or flaw in hardware, firmware, or software that, if exploited (either intentionally or accidentally), could lead to an unacceptable impact in the form of unauthorized access to information or disruption of critical processing.

Vulnerability Assessment (or Vulnerability Testing) - Systematic examination of a system to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures and confirm the adequacy of such measures after implementation.

III. ROLES AND RESPONSIBILITIES

A. The Information Systems Security Officer (ITSO) is responsible for the following:

1. Developing testing procedures.
2. Performing periodic testing.
3. Documenting test results.
4. Communicating vulnerabilities to information owners and Custodians.
5. Auditing to ensure vulnerabilities have been mitigated.
6. Providing advice to information owners and Custodians regarding potential mitigation strategies.

B. information owners are responsible for the following:

1. Allowing vulnerability testing to be performed on their resources.
2. Ensuring any identified vulnerabilities are resolved for their resources.

C. Information Custodians are responsible for the following:

1. Assisting the ITSO with performing security testing, as requested.
2. Helping information owners with selecting and implementing mitigation strategies.
3. Documenting mitigations that are implemented.
4. Informing the ITSO about mitigations performed.

IV. POLICY AND GUIDELINES

Today's information systems are complex and composed of many interdependent and interconnected components. Despite how well they have been developed, all systems have some inherent vulnerabilities or exploitable flaws. Over time, these vulnerabilities are likely to be exploited, either intentionally or accidentally.

Security testing is an important means of detecting weaknesses and determining the threat posed by them. It also helps to determine the effectiveness of security measures that have been implemented and to assess how well the organization can withstand security attacks. A vulnerability testing program provides the crucial details to prepare the Office to avoid the significant financial costs or damage to its reputation that could result from security malfeasance.

Because threats, vulnerabilities and the configurations of the systems themselves are always changing, Reference A. requires the Office to perform security testing on a periodic basis.

This protocol establishes a systematic, comprehensive, ongoing and priority-driven security testing program that will assist the Office in determining its security priorities and making prudent investments to enhance the security posture of its information resources.

A. Vulnerability testing should be conducted at least annually while systems are running in their operational environments.

B. Testing should not disrupt critical business operations.

C. Procedures for testing should be clearly defined and documented.

D. All test results should be well documented.

E. If necessary, the "rules of engagement" should be communicated to the system owners.

F. information owners and Information Custodians should be informed of the results to ensure vulnerabilities are patched or mitigated.

G. All systems should be retested once vulnerabilities are addressed to ensure they have been effectively mitigated.

H. Vulnerability testing should be integrated into the Office's risk management processes.

I. The Office will adhere to NIST guidance as set forth in References B - D and other relevant best practices.

V. ENFORCEMENT

Violation of this protocol could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment or referral for criminal prosecution.

SUBJECT/POLICY NUMBER:

5.05.02.10 CONTINGENCY PLANNING

PURPOSE/SCOPE:

Contingency Planning establishes a comprehensive and effective program to ensure continuity of essential Office functions during a broad spectrum of emergencies or situations that may disrupt normal operations. This protocol establishes contingency planning and applies to all major information systems and mission-critical applications.

I. REFERENCES

A. National Institute of Standards and Technology (NIST), Contingency Planning Guide for Application and Data Services Systems Special Publication 800-34.

II. DEFINITIONS

Contingency Plan - Management protocol and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disaster.

Continuity of Support Plan (COSP) - The documentation of a predetermined set of instructions or procedures mandated by the Office of Management and Budget (OMB) A-130 that describe how to sustain major applications and general support systems in the event of a significant disruption.

Continuity of Operations Plan (COOP) - A predetermined set of instructions or procedures that describe how an organization's essential functions will be sustained for up to 30 days as a result of a disaster event before returning to normal operations.

Disaster Recovery Plan (DRP) - A written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities.

Disruption/Disaster - An unplanned event that causes the system to be inoperable for an unacceptable length of time (e.g., minor or extended power outage, extended unavailable network, or equipment or facility damage or destruction).

Major Information System - An information system that requires special management attention because of its importance to an Office mission, i.e., mission critical business processes.

III. ROLES AND RESPONSIBILITIES

A. Information Systems Security Officer (ITSO) is responsible for the following:

1. Assisting in identifying major information systems and mission critical applications.
2. Reviewing contingency plans to ensure they align with the overall agency COOP plan and information security policies.
3. Providing training, support and coordination for information owners and Custodians as they develop and coordinate contingency plans.
4. Ensuring contingency plans are updated and tested annually.

5. Monitoring the contingency planning process and reporting progress to management as required.
6. Maintaining current copies of all contingency plans, tests, evaluations and subsequent follow-up actions and making this information available as required.
7. Activating and coordinating established contingency plans during an emergency.

B. Information owners are responsible for the following:

1. Developing, reviewing and testing system and application contingency plans for the resources they own.
2. Developing a strategy for providing adequate alternate processing capability based on the prioritization of major systems or critical applications which they own.
3. Providing personnel for contingency plan testing.
4. Maintaining a list of the personnel involved in the disaster planning/recovery process, including their functions, roles and assigned tasks.

C. Information custodians are responsible for the following:

1. Working with information owners and the ITSO to develop contingency plans.
2. Participating in contingency plan testing.

IV. POLICY AND GUIDELINES

In addition to being a legal mandate for federal agencies, contingency planning is simply a good business practice and part of the fundamental mission of the Office as a responsible and reliable public institution. For the success of the Office's programs, its information systems must be available in the event of disruptions/disasters.

The Office's information systems are vulnerable to a variety of disruptions, ranging from mild (e.g., short-term power outage) to severe (e.g., equipment destruction, fire) and from a variety of sources ranging from natural disasters to terrorists actions. While much vulnerability may be minimized or eliminated through technical, management, or operational solutions as part of the Office's risk management program, it is virtually impossible to completely eliminate all risks. In many cases, critical resources reside outside the Office's control (such as electric power or telecommunications) and the Office may be unable to ensure their availability.

The Office of Early Learning must establish effective contingency planning, execution and testing to mitigate the risk of system and service unavailability.

A. The Office will develop and maintain a viable contingency planning program for its major information systems and mission-critical applications.

B. The program will support the Office's Continuity of Operations (COOP) Planning.

C. The program will yield documented plans on how the Office will continue its mission and provide continuity of data processing if service, use, or access is disrupted for an extended period of time.

D. Each major IT system will have its own Contingency Plan, Continuity of Support Plan, or Disaster Recovery Plan.

E. Contingency planning will be based on business impact analyses that will identify and rank major information systems and mission-critical applications according to priority and the maximum permissible outage for each.

F. Preventive measures will be identified to reduce the effects of system disruptions and increase system availability.

G. Recovery strategies and procedures will be developed to ensure systems may be recovered quickly and effectively following a disruption.

H. Contingency plan testing and training will be held to address deficiencies and to prepare information owners and Custodians for plan activation.

I. Testing will occur annually or when a significant change occurs to the Office's major information systems or mission-critical applications.

J. Contingency plans will be reviewed regularly and updated as needed to remain current with Office Application and Data Services enhancements.

K. The Office will adhere to and subsequent publications.

V. ENFORCEMENT

Violation of this protocol could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment or referral for criminal prosecution.

5.05.02.11 ACCESS CONTROL

PURPOSE/SCOPE:

Access to Office information resources will be limited to individuals who need those resources to perform their duties. The principles of separation of duties and least privilege will be applied to the allocation of access rights. This protocol establishes Access Control procedures and applies to all of the Office's information employees, contractors, owners and custodians, as well as access to any Office information resources.

I. REFERENCES

A. National Institute of Standards and Technologies (NIST), Control Families, Special Publication 800-53.

II. DEFINITIONS

Access - The rights to enter, view, instruct, communicate with, store data in, retrieve data from, or otherwise make use of specific information resources.

Access Control - The enforcement of specified authorization rules based on positive identification of employees and the systems or data they are permitted to access.

Access Privilege (Privilege) - A specific activity that a user has been granted access to perform on an information resource (e.g., view or modify).

Account - A set of privileges for authorization to system access, which are associated with a UserID.

Authorization - The formal granting of access to an individual to perform certain activities.

Least Privilege - Granting employees only the minimum privileges required to provide the level of access needed to perform their official duties.

Separation of Duties - Concept that provides the necessary checks and balances to mitigate against fraud, errors and omissions by ensuring no individual or function has control of the entire process.

System Permissions - The technical configuration that provides an individual the ability to perform certain actions on information resources.

UserID - Character string (i.e., logon name) that uniquely identifies a computer user.

III. ROLES AND RESPONSIBILITIES

A. Information Systems Security Officer (ITSO) is responsible for the following:

1. Auditing to ensure compliance with the procedures and guidelines specified in this protocol
2. Ensuring all personnel are trained on their computer security responsibilities

B. Information custodians are responsible for the following:

1. Assisting information owners with controlling access to their resources.
2. Promptly removing access from a system when requested.
3. Reporting any unauthorized accesses that they discover.

C. information owners are responsible for the following:

1. Determining who should have access to their resources.

2. Ensuring their resources are protected against unauthorized access.
3. Periodically reviewing access permissions.
4. Ensuring information employees have undergone appropriate background checks and security training. This includes contractors.

D. Supervisors are responsible for the following:

1. Adhering to Office procedures for obtaining and removing access to information resources for their associates, contractors and interns.
2. Ensuring their associates are authorized to access the resources needed to perform their duties.
3. Notifying the ITSO when access privileges or accounts are to be removed.
4. Immediately reporting suspected violations of this protocol.

E. Employees are responsible for the following:

1. Understanding Office information resource access policies and procedures.
2. Adhering to Office procedures for obtaining and removing access to information resources for themselves.
3. Safeguarding their access credentials.
4. Accessing only those resources for which they are authorized and using information in accordance with job function and Office protocol.
5. Immediately reporting suspected violations of this protocol to their supervisor or the ITSO.
6. Understanding the consequences of their failure to adhere to this protocol.

IV. POLICY AND GUIDELINES

Employees must have access to the information resources required to do their jobs. However, Reference A. and best practices suggests excessive or uncontrolled access can lead to the unauthorized or unintentional disclosure, modification, or destruction of those resources, as well as liability for negligence in protecting those resources.

Only authorized personnel who have a legitimate need to use Office resources may be granted access to specific resources and their access privileges will be limited to those required to perform their duties.

A. Employees will be granted specific access privileges on each system, limited to those required to perform their job functions.

B. Employees must be authorized by the information owner prior to being granted access to a particular resource.

C. Employees will only access resources to which they have been authorized, regardless of actual system permissions.

D. Employees will not circumvent the permissions granted to their accounts in order to gain access to unauthorized information resources.

E. Employees will protect their own accounts:

F. Employees will not allow anyone else to use their account, or use their computers while logged in under their account, except as required for system administration.

G. When leaving their computer unattended, employees will either log out or invoke protection of their system (such as a password-protected screensaver).

H. Employees are responsible for any activity initiated by their own userID (only they should have access to their userID).

I. The level of access control will depend on the classification of the resource and the level of risk associated with the resource.

J. Criteria will be established for account eligibility, creation, maintenance and expiration for each system.

K. Information Custodians (i.e. system administrators) will periodically review user privileges and modify, revoke, or deactivate as appropriate, based on the above criteria.

L. Inactivity timeouts (i.e., computer being idle for a set amount of time) will be implemented, where technically feasible, for access to confidential information.

V. ENFORCEMENT

Violation of this protocol could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment or referral for criminal prosecution.

VI. FORMS

Office of Early Learning Security Agreement Form

SUBJECT/POLICY NUMBER:

5.05.02.12 IDENTIFICATION AND AUTHENTICATION

PURPOSE/SCOPE:

Access to Office information systems will only be granted to identified and authenticated employees. Office will establish procedures and controls for granting, changing and terminating access to information systems. This protocol establishes procedures for Identification and Authentication and applies to all Office owned or operated information systems, both operational and in development.

I. REFERENCES

A. National Institute of Standards and Technology (NIST), Recommendations for Electronic Authentication, Special Publication 80063.

II. DEFINITIONS

Authentication - The process of verifying that an employee is who he or she purports to be. Techniques are usually broken down into three categories: (1) something the employee knows, such as a password or PIN; (2) something the employee has, such as a smartcard or ATM card; and (3) something that is part of the employee, such as a fingerprint or iris.

Brute Force Attack - attack where the attacker attempts to systematically "guess" a password or other secret by trying all possible values.

Identification - The process of determining who an employee claims to be; usually performed by presenting an employee ID (i.e., "jsmith").

Information Resources - The procedures, equipment, facilities, software and data that are designed, built, operated and maintained to collect, record, process, store, retrieve, display and transmit information.

Password - Any secret string of characters which serves as authentication of a person's identity and which may be used to grant or deny access.

Strong Authentication - An authentication process using techniques which would require a high level of effort to compromise. Strong authentication usually entails the use of multiple, integrated authentication techniques (factors), such as using both a token and a PIN number together.

Employee ID - Character string that uniquely identifies an employee or computer process.

III. ROLES AND RESPONSIBILITIES

A. Information Systems Security Officer (ITSO) will prepare guidelines and standards for employee credentials, perform compliance reviews and approve issuance of administrator credentials.

B. System Developers must ensure their systems support the procedures and guidelines specified in this protocol document.

C. Information Custodians will implement appropriate identification and authentication methods for the information resources in their care, instruct employees as to their usage and report any compromises of these resources to the ITSO and the Information Owner.

D. information owners will ensure appropriate identification and authentication methods are implemented for the resources that they own, based on the classification and level of risk assigned to the resource.

E. Supervisors will ensure their personnel understand and comply with the guidelines contained in this protocol, promptly notify Information Custodians of accounts that should be deactivated and report any suspected violations or compromises of credentials to the ITSO and the Information Custodian.

F. Employees will understand their responsibilities for safeguarding Employee IDs and passwords and immediately notify a supervisor or the Information Custodian (e.g., the Office IT Unit department) if they suspect that a password or other system credential has been compromised.

IV. POLICY AND GUIDELINES

In order to ensure unauthorized persons do not have access to confidential Office information resources, it is necessary to first establish the identity of the employee who is attempting to access the resource. Access controls can then be used to allow or limit access based on the established employee identity.

A. The specific method(s) of authentication used for each system will be commensurate with the level of confidentiality of the system to be accessed (i.e. more confidential systems should use stronger authentication methods).

B. Multiple authentication methods (e.g. use of both a password and a token) may be required for high-confidentiality or high-risk situations.

C. Each Office system will incorporate proper employee authentication and identification to ensure access is not granted to unauthorized persons. Employees will not have access to Office information resources without identifying and authenticating themselves (i.e. “logging on”).

D. The Office will develop and follow detailed procedures for the creation, removal and modification of employee accounts and authentication credentials.

E. Employee accounts must adhere to the following guidelines:

1. Allow only one employee per account; Employee IDs are never to be shared.
2. Never install a guest/guest account. Remove any guest accounts that are created by default by the system unless absolutely required and approved by the system owner and the ITSO.
3. No accounts will be named with easily guessed generic names (such as “anonymous,” “guest,” “admin,” “ftp,” “telnet,” “www,” “host,” “employee,” “test,” “bin,” “nobody,” etc.,) unless absolutely technically required by the system.
4. Default accounts that are present upon initial installation of the system should be removed or renamed unless absolutely technically required by the system.
5. Accounts should be deactivated immediately upon termination of an associate or contractor.
6. Unused accounts will be deactivated on at least a quarterly basis.
7. Accounts for contractors and temporary associates will expire on the final date of their contract unless otherwise approved and documented.

F. Administrator accounts must adhere to the following guidelines:

1. The names of the administrator accounts will be renamed, if possible, to make it more difficult for attackers to guess the names of these accounts.

2. Each person who has a legitimate need to use Administrator privileges should have their own administrative account that they will use to perform administrative functions. Usage of the main administrator account for each system should be limited to emergencies and is to be limited to designated Office IT Unit staff. This will protect the main administrator account and also provide an audit trail of administrative activities.
3. All accounts with administrator privileges will have strong passwords or other alternative strong authentication methods.
4. If passwords are used for authentication, they must adhere to the Office Password Management Protocol 5.05.02.32.

G. If authentication methods other than passwords are used (e.g., biometrics, smartcards, tokens, etc), then:

1. They must be approved by the ITSO.
2. Additional policies and procedures will be developed to govern their usage.

H. Account credential information (e.g., Employee IDs, passwords) that are stored on the devices (such as enable passwords in router configuration files) must be encrypted.

I. To preclude brute force attacks, an intruder lockout feature shall be implemented on each system to temporarily suspend the account after three invalid logon attempts. Manual action by a security system administrator is required to reactivate the ID.

J. The Office will restrict access to authentication data. Authentication data will be protected with access controls and encryption to prevent unauthorized individuals from obtaining the data.

K. It is the protocol of the Office to adhere to and subsequent publications.

V. ENFORCEMENT

Violation of this protocol could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment or referral for criminal prosecution.

SUBJECT/POLICY NUMBER:

5.05.02.13 AUDIT TRAILS

PURPOSE/SCOPE:

Audit trails must be maintained to provide accountability for the use of the Office's information resources. This protocol establishes procedures for implementing Audit trails and applies to all Office information systems and all employees.

I. REFERENCES

A. National Institute of Standards and Technology (NIST) Audit Trails. Introduction to Computer Security, Special Publication 800-12.

II. DEFINITIONS

Audit Trail - In computer security systems, a chronological record of system resource usage. This includes employee login, file access, other various activities and whether any actual or attempted security violations occurred, legitimate and unauthorized.

Security Incident - Any activity that is a threat to the availability, integrity, or confidentiality of information resources, or any action that is in violation of security policies.

III. ROLES AND RESPONSIBILITIES

A. Information Systems Security Officer (ITSO) is responsible for periodically reviewing audit trails for all systems to ensure compliance with this protocol.

B. Information Custodians are responsible for assisting information owners with implementing and maintaining audit trails for the resources for which they are responsible.

C. information owners are responsible for ensuring audit trails are implemented and maintained for their resources.

D. Supervisors are responsible for assisting the ITSO in reconciling audit trail anomalies.

E. Employees are responsible for understanding and acknowledging that their use of Office systems may be logged and audited.

IV. POLICY AND GUIDELINES

In order for the Office to enforce information usage policies and security measures and to investigate security incidents, it must maintain automated logs of access to and alteration of information systems and data. It must maintain a record of activity (or "audit trail") of system and application processes and employee activity of systems and applications.

The Office uses this information to investigate security incidents, monitor use of Office resources, provide accountability for transactions, track system changes and assist in detection of system anomalies. In conjunction with appropriate tools and procedures, audit trails can assist in detecting security violations, performance problems and flaws in applications.

A. Audit Trails will be maintained for Office information systems.

B. At minimum, the following transactions should be logged for each server:

1. Server startup and shutdown.
2. Loading and unloading of services.
3. Installation and removal of software.
4. System alerts and error messages.
5. Employee logon and logoff.
6. System administration activities.
7. Accesses to confidential information and systems.
8. Modifications of privileges and access controls.
9. Additional security related events.

C. At minimum, the following transactions should be logged for each application:

1. Modifications to the application.
2. Application alerts and error messages.
3. Employee sign on and sign off.
4. System administration activities.
5. Accesses to confidential information.
6. Modifications of privileges and access controls.

D. At minimum, the following transactions should be logged for each router, firewall, or other major network device:

1. Device startup and shutdown;
2. Administrator logon and logoff;
3. Configuration changes;
4. Account creation, modification, or deletion;
5. Modifications of privileges and access controls; and
6. System alerts and error messages.

E. Type of event, date, time and employee identification must be recorded for each logged transaction.

F. Confidential information, such as passwords and actual system data, should not be stored in the logs.

G. Periodic reviews of audit logs will be conducted by the ITSO or other designated personnel.

H. Only designated personnel should have access to the audit logs.

I. All audit trail files will be kept for three (3) years

J. Audit trails associated with known incidents (including those used for legal action) are to be retained for the period of time designated by the Office's Legal Department.

K. Audit trails must be kept in a secure location. Audit data should be some of the most carefully secured data at the site and in the backups. If an intruder were to gain access to audit logs, the systems themselves, in addition to the data, would be at risk.

L. The Office will follow NIST guidance regarding audit trails.

V. ENFORCEMENT

Violation of this protocol could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment or referral for criminal prosecution.

SUBJECT/POLICY NUMBER:

5.05.02.16 PERSONNEL SECURITY

PURPOSE/SCOPE:

Access to Office information resources is to be limited to only those persons who have been appropriately screened and authorized. This protocol establishes procedures for personnel utilizing Office information systems. This applies to all Office associates and external information employees.

I. REFERENCES

A. National Institute of Standards and Technology (NIST), Guide to Selecting Application and Data Services Security Products, Special Publication 800-36.

B. American National Standards Institute/International Committee for IT Standards (ANSI/INCITS) 359-2004 Application and Data Services-Role Based Control

II. DEFINITIONS

Access Privilege - An authorized ability to perform a certain action on a computer, such as read a specific computer file.

Account - A set of privileges for authorization to system access, which are associated with an employee ID.

Authentication Token - A hardware device, the possession of which can be verified and which helps to confirm identity as part of the authentication process (e.g., smartcard, SecureID).

Least Privilege - A concept that means granting employees only the minimum level of access they need to perform their official duties.

Separation of Duties - Refers to dividing roles and responsibilities so that a single individual cannot subvert a critical process or bypass security controls. Where feasible, the responsibilities of programmers, system administrators, database administrators and system auditors should not overlap.

III. ROLES AND RESPONSIBILITIES

A. The Information Systems Security Officer (ITSO) is responsible for implementing procedures to ensure access to classified information via Office information systems is controlled pursuant to the Office's security policies and procedures and for monitoring the adherence to the personnel security protocol. ITSOs are also responsible for designating both the risk level and the sensitivity level for all contractor positions and for ensuring a background investigation is completed.

B. Information custodians are responsible for following the Office's procedures for adding and removing access for personnel to the resources they manage, including promptly deleting or disabling accounts when employees terminate employment. Custodians are responsible for implementing least privilege and separation of duties for resources they manage and for verifying that employees have appropriate clearance for the resources to which they are being granted access, in accordance with clearance requirements set by information owners.

C. Information owners are responsible for determining who should have access to their resources and for determining the level of screening required for access. They are also responsible for ensuring personnel security policies and procedures are being followed.

D. Human Resources Management is responsible for designating both the risk level and the sensitivity level for all competitive and excepted civil service positions and for notifying the ITSO when background investigations have been completed.

E. Supervisors are responsible for communicating to their personnel the security requirements outlined in this protocol and ensuring all personnel are trained in the computer security responsibilities and duties associated with their jobs. Supervisors are also responsible for adhering to Office policies and procedures for adding and removing access for their employees and for ensuring their contractors undergo the appropriate level of background screening.

F. Employees are responsible for understanding their personnel security responsibilities and duties and following Office procedures for obtaining access to information resources. Employees are also responsible for promptly notifying the information owner, information custodian, or their own supervisor when they no longer need access to a resource.

IV. POLICY AND GUIDELINES

The greatest harm/disruption to a system comes from the actions of individuals, both intentional and unintentional. Employees, designers, implementers, administrators and managers are involved in many important issues in securing information.

It is important to ensure the personnel who have access to the Office's information resources can be trusted to institute controls over the access provided to those personnel and to implement procedures that minimize the personnel-related risks to the Office's resources.

Any access granted to Office information resources will be based on the principles of separation of duties and least privilege and in compliance with References A. and B.

A. Employees must have appropriate clearance for the sensitivity level of the resources which they are given access.

B. Prior to being granted access to classified information resources, employees for whom no previous investigation and/or no recent, documented positive suitability determination has been made, must submit to a Request for Background Investigation through the Office Human Resource Department.

C. Employees must be trained in the information security responsibilities and duties associated with their jobs.

D. A detailed process will be implemented to manage employee accounts, including processing requests for new accounts, establishing accounts and closing accounts as well as tracking accounts and employee access authorizations.

E. Procedures will be implemented for outgoing or transferring employees. These will include, but are not limited to, the following:

1. The removal of access privileges, computer accounts and authentication tokens.
2. The return of any Office information resources (property or data).
3. Procedures for unfriendly termination that include the prompt removal of system access.

F. Contractors must sign a non-disclosure agreement protecting any confidential data to which the contractor requires access.

V. ENFORCEMENT

Violation of this protocol could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment or referral for criminal prosecution.

SUBJECT/POLICY NUMBER:

5.05.02.17 PHYSICAL AND ENVIRONMENTAL SECURITY

PURPOSE/SCOPE:

Information resources require physical security measures to ensure proper and timely operation, to protect value, to safeguard the integrity of information and to ensure the safety of personnel. Computer systems, facilities and tape storage areas will be protected from theft, alteration, damage by fire, dust, water, power loss and other contaminants and unauthorized disruption of operation. This protocol prescribes the procedures, guidelines and standards that govern the implementation of physical security measures designed to protect Office information resources. It does not govern protection of personnel, facilities and property not directly associated with information technologies, which are covered by Office Policy 4.05 - Office Property Management Procedures.

I. REFERENCES

A. Section 1002.75, F.S., Records of Children in the Voluntary Prekindergarten Program
B. Section 1002.97, Records of Children in the School Readiness Program
C. Section 1002.221, K-12 Education Records
D. 45 C.F.R. Pt. 5b, Privacy Act Regulations
E. 20 U.S.C. § 1232g, Family Rights and Educational Privacy Act

II. DEFINITIONS

Confidential Data - Any data that is categorized as "confidential" under the Office's information resource classification protocol and framework.

III. ROLES AND RESPONSIBILITIES

A. Information Systems Security Officer (ITSO) is responsible for performing auditing to ensure compliance with these policies and guidelines.

B. Information Custodians are responsible for assisting information owners with implementing physical and environmental security measures.

C. information owners are responsible for implementing measures to protect their resources against physical and environmental threats, as well as unauthorized physical access.

D. Supervisors are responsible for the following:

1. Ensuring their personnel understand Office protocol regarding physical and environmental security.
2. Monitoring their associates' compliance with this protocol.

E. Employees are responsible for the following:

1. Understanding and adhering to the security requirements prescribed in this protocol.
2. Physically protecting the Office information resources entrusted into their possession.
3. Reporting any incident or condition contrary to the specified requirements to the ITSO.

IV. POLICY AND GUIDELINES

It is crucial that the Office implement physical security safeguards to protect its information resources. These safeguards must be applied in all administrative, physical and technical areas and can include the use of locks, guards, administrative controls and measures to protect against damage from intentional acts, accidents, fires and environmental hazards.

Physical access to information resources is to be controlled commensurate with the classification of the resource and the level of risk.

A. Areas containing confidential information resources require special restrictions to limit access to these resources:

1. Admittance to these areas is to be limited to personnel assigned to the area and persons who have been specifically authorized access to the area.
2. Personnel assigned to the area must escort personnel without an appropriate security clearance.
3. When unauthorized personnel are present in these areas, confidential information must be protected from observation, disclosure, or removal. This includes storing away documents and positioning all computer monitors to prevent viewing by unauthorized persons.
4. Each person within a confidential area, regardless of position, will be subject to challenge by another Office associate, facility security personnel, or any law enforcement officer and will display appropriate identification when challenged. Failure to do so may result in removal from the facility or other administrative action.

B. Areas containing critical information resources require special protections to safeguard the availability of these resources:

1. Protection must be implemented against fire, flood, humidity, electromagnetic disturbance and other environmental factors that could damage the resources.
2. Automated systems should monitor for environmental problems and alert specified personnel as appropriate.
3. Backups and other media, both originals and copies, containing data and programs must be kept in good condition and protected from theft. It is important to keep backups in a separate location from the originals, not only for damage considerations, but also to guard against thefts.

C. Other areas where physical access should be restricted are wiring closets and computer storage areas.

V. ENFORCEMENT

Anyone who violates this protocol is subject to disciplinary action, up to and including termination of employment.

SUBJECT/POLICY NUMBER:

5.05.02.18 CHANGE CONTROL

PURPOSE/SCOPE:

Authorized changes must occur to the Office's information systems and these changes must occur in a timely manner without disruption or compromise to existing system operation. However, the Office must protect its information systems from unauthorized changes, intrusions or misuse. One way of facilitating this requirement is to formally manage and control hardware and software configuration changes. This protocol establishes procedures for Change Control and applies to all Office information systems.

I. REFERENCES

None.

II. DEFINITIONS

Change Control - Documented procedures used to control the revision of applications, operating systems and hardware configurations in computing environments.

III. ROLES AND RESPONSIBILITIES

A. The Information Systems Security Officer (ITSO) is responsible for the following:

1. Developing change control procedures.
2. Working with information owners and Custodians to ensure change control policies and procedures are followed and documented.
3. Monitoring Office information systems to ensure compliance with this protocol.

B. Information custodians are responsible for the following:

1. Participating in the development of procedures for change control.
2. Evaluating, recommending and coordinating the implementation of solutions/changes consistent with Office technical plans.
3. Maintaining change log documentation.

C. Information owners are responsible for ensuring changes to the systems they own are documented and implemented in compliance with the protocols and procedures listed in this document.

IV. POLICY AND GUIDELINES

Change control involves controlling and managing changes to the Office's information systems to ensure integrity of data and information. Office information systems require appropriate administrative, physical and technical controls to be incorporated into both new additions and changes to systems.

These controls must encompass not only the software, but also the routine activities that enable the Office's information systems to function properly (e.g., fixing software or hardware problems, loading and maintaining software, updating hardware and software and maintaining a historical record of application changes). Change control prevents unexpected changes from inadvertently leading to denial of service, unauthorized disclosure of information and other problems.

Informal operational processes with no means of controlling changes to information systems impede the Office's ability to determine the status of its current architecture and even to propose changes. Change control planning addresses this deficiency and establishes a consistent, cross-organizational change management process for Office information systems. Change control history is a valuable tool for both emergency response and information architecture planning.

The Office will develop baseline information that includes a current list of all components (hardware, software and their documentation), configuration of peripherals, version releases of current software, information on batch files, environmental settings such as paths and switch settings of machine components.

A. Changes to each Office information system will be systematically planned, approved, tested and documented at a level appropriate with the size, complexity and confidentiality of the system.

B. For each information system, the Office will maintain a log of all configuration changes made, the name of the person who performed the change, the date of the change, the purpose of the change and any observations made during the course of the change.

C. Procedures will be implemented to ensure maintenance and repair activities are accomplished without adversely affecting system security. The procedures will include the following:

   1. Establish who performs maintenance and repair activities.
   2. Contain procedures for performance of emergency repair and maintenance.
   3. Contain the management of hardware/software warranties and upgrade policies to maximize use of such items to minimize costs.

D. Version control that associates system components to the appropriate system version will be followed.

E. Procedures identified for the Office's operations will be implemented for testing and/or approving system components (operating system, other system, utility, applications) and configuration changes prior to promotion to production.

F. Employees will be notified regarding how they will be impacted by changes.

G. Current backups will be available when changes are made.

H. All software, operating systems and patches will be installed in accordance with U.S. copyright regulations, the license for that software and applicable Office Information Security policies.

I. Only authorized personnel may make changes to Office information systems.

J. Change control procedures will be documented for all systems to provide a complete audit trail of decisions and design modifications.

K. Change control documentation (especially change logs) will be available even if the network is down and will not contain passwords for affected components.

V. ENFORCEMENT

Violation of this protocol could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment or referral for criminal prosecution.

SUBJECT/POLICY NUMBER:

5.05.02.19 BACKUP AND RECOVERY

PURPOSE/SCOPE:

Backups of critical information resources must be performed, tested and appropriately managed. This protocol establishes procedures for Backup and Recovery and applies to all Office information resources. The Northwest Regional Data Center (NWRDC) hosts the Office's information systems and data on its network. The Policy and Guidelines in this protocol apply to the backup and recovery process that is performed by Office staff on the Office's network.

I. REFERENCES

A. National Institute of Standards and Technology (NIST), Guide to General Server Security, Special Publication 800-123

II. DEFINITIONS

Back Up - The process of copying data to alternative or redundant media.

Backup - A copy of data that is made in order to provide redundancy in case the original becomes corrupted or unavailable.

Restore - The process of copying data from a previously-made backup to the original (or an alternate) system.

Critical Data - Data which has been designated as "critical" under the Office's Information Resource Classification protocol 5.05.02.02.

III. ROLES AND RESPONSIBILITIES

A. The Information Systems Security Officer (ITSO) will perform auditing to ensure compliance with this protocol. The ITSO will work with Northwest Regional Date Center to address any issues.

B. Information custodians will assist information owners with backing up and restoring their resources.

C. Information owners will ensure their resources are backed up in accordance with this protocol.

D. Employees will ensure any critical data residing on their workstations or portable media are backed up in accordance with this protocol.

IV. POLICY AND GUIDELINES

There are many threats that exist which could cause the loss, corruption, or temporary unavailability of data. These include, but are not limited to, hardware failures, accidental deletion, incorrect modification, software corruption and malicious activities. These threats are very common and it is inevitable that some of these events will occasionally occur at the Office.

The Office of Early Learning must maintain backup copies of all critical data and systems so that they can be used to provide the continued availability and viability of these resources when these events occur.

A. All critical Office information resources will be backed up in a recoverable fashion.

B. Backups will be performed according to the following schedule:

1. All critical data and system configurations must be backed up on at least a daily basis;
4. Applications and licenses will be backed up whenever there are changes to them; and
5. The backing up of non-critical data is at the discretion of the data owner.

C. Backups will be stored off-site in a secure, environmentally-controlled location.

D. Each system will have a defined backup retention schedule which complies with the Florida Department of State Records Retention Schedules.

E. The Office will periodically test the back up and restore procedures to ensure data can be effectively restored from the backups.

F. The Office will develop and implement detailed procedures for performing back ups restoring data, performing testing of backups, transferring tapes to/from the storage facility and recycling or disposing of backups upon expiration of their retention period.

G. Backups will be treated with the same level of criticality and confidentiality as the data and applications stored on them.

H. Persons who have access to the backups, or who have access to perform back up or restore functions, must undergo appropriate background screening in accordance with Office and Northwest Regional Data Center Personnel Security practices prior to being given such access.

I. Backup media (e.g., tapes) must be handled in accordance with Office Media Management protocol.

J. System custodians will back up data stored on their servers. However, employees are responsible for backing up any data stored on workstations and portable storage media (i.e., diskettes, flash drives, CDs, etc).

K. Employees may copy their data to servers to be backed up or may perform their own back ups of data not stored on NWRDC servers.

L. Backups made by employees must be handled in accordance with Office Media Management protocol.

M. The Office will follow the Reference A. guidance regarding backups.

V. ENFORCEMENT

Violation of this protocol could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment or referral for criminal prosecution.

SUBJECT/POLICY NUMBER:

5.05.02.22 MOBILE COMPUTING

PURPOSE/SCOPE:

Laptops and other mobile computing devices require additional security controls to mitigate the risks posed by using them outside the Office physical environment. This protocol establishes procedures for Mobile Computing and applies to all laptops and other mobile computing devices that are used to store or process Office data.

I. REFERENCES

A. National Institute of Standards and Technology (NIST), Wireless Network Security: 802.11, Bluetooth and Handheld Devices, Special Publication 800-48.

B. The Office of Early Learning, Communications Equipment Policy 4.09.

II. DEFINITIONS

Antivirus Software - Software that searches for evidence of computer virus infection and attempts to remove the malicious code and repair any damage the virus caused.

Authentication - The process of verifying that an employee is who he or she purports to be, via password, token or other credential.

Mobile Computing Device - A laptop, PDA, or other portable device that can store or process data.

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

III. ROLES AND RESPONSIBILITIES

A. The Information Systems Security Officer (ITSO) is responsible for auditing the use of mobile computing devices to ensure compliance with the procedures and guidelines set forth in this protocol.

B. Information custodians are responsible for assisting information owners with managing and protecting their mobile computing devices, including inventorying and tracking them, as well as defining security countermeasures that will be applied.

C. Information owners are responsible for ensuring any mobile computing resources they own are being managed and used in accordance with the procedures and guidelines set forth in this protocol.

D. Supervisors are responsible for ensuring their associates understand and comply with these policies and guidelines.

E. Employees are responsible for the following:

1. Complying with the procedures and guidelines set forth in this protocol.
2. Taking all reasonable precautions to protect mobile computing devices in their possession from loss, theft, tampering, unauthorized access and damage.
3. Immediately reporting to their supervisor and the ITSO the loss, theft, tampering, unauthorized access, or damage of any mobile device covered by this protocol.

IV. POLICY AND GUIDELINES

The use of laptop computers and mobile devices (such as PDAs) provide flexibility and enhanced communications that allow Office personnel to be more productive. However, the use of these devices outside of the Office office poses risks to those devices and the information they contain. These devices may also present a hazard to other Office resources upon their return to the Office (for example, by spreading a virus that was obtained outside). These devices have the capability for direct connectivity to the Internet or other networks outside of the state's network, which lack the protections afforded by the Office's corporate firewall and other perimeter protections.

The Office of Early Learning must implement additional security measures to mitigate increased security risks presented by mobile computing.

A. Laptops and other mobile computing devices must be inventoried and tracked.

B. Laptops must use antivirus and personal firewall software when connected to any network other than the state's network.

C. Access to mobile devices which store or transmit confidential data, or which can be used to connect to other confidential Office systems, must be authenticated.

D. All security policies applied in the Office physical environment must also be applied when using or connecting to Office resources outside the Office physical environment.

E. Employees are responsible for backing up their data that is stored on the mobile computer on a regular basis.

F. Office confidential data placed on any mobile device is to be protected against unauthorized access via encryption, biometrics, or other appropriate measures. Storage of Office confidential data on any mobile device is prohibited.

G. The Office will adhere to Reference A. and subsequent publications.

V. ENFORCEMENT

Violation of this protocol could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment or referral for criminal prosecution.

SUBJECT/POLICY NUMBER:

5.05.02.25 REMOTE ACCESS

PURPOSE/SCOPE:

Laptops and other mobile computing devices require additional security controls to mitigate the risks posed by using them outside the Office's physical environment. This protocol establishes procedures for Mobile Computing and applies to all laptops and other mobile computing devices that are used to store or process Office data.

I. REFERENCES

A. National Institute of Standards and Technology (NIST), Security for Telecommuting and Broadband Communications, guidance as set forth in Special Publication 800-46.

B. Office of Early Learning, Telecommuting Policy and Agreement Policy 1.09.

II. DEFINITIONS

Authentication - The process of verifying that an employee is who he or she purports to be. Techniques are usually broken down into three categories: (1) something the employee knows, such as a password or PIN; (2) something the employee has, such as a smartcard or ATM card; and (3) something that is part of the employee, such as a fingerprint or iris.

Confidential Data - Any data that is categorized as "confidential" under the Office's information resource classification protocol and framework.

Encryption - The process of transforming readable text into unreadable text (cipher text) for the purpose of security or privacy. Data is encoded to prevent unauthorized access.

Remote Access - Any access to the office network through a network, device, or medium that is not controlled by the office (such as the Internet, public phone line, wireless carrier, or other external connectivity).

Strong Authentication - An authentication process using techniques which would require a high level of effort to compromise and are not subject to compromise by eavesdropping. Strong authentication processes may use challenge/response password devices, SmartCards, or one-time passwords.

III. ROLES AND RESPONSIBILITIES

A. The Information Systems Security Officer (ITSO) is responsible for auditing the use of remote access to ensure compliance with Information Custodians are responsible for assisting information owners with implementing the guidelines outlined in this protocol.

B. Information owners are responsible for ensuring any remote access to their information resources is conducted in accordance with the procedures and guidelines set forth in this protocol.

C. Supervisors are responsible for ensuring their associates understand and comply with these policies and guidelines.

D. Employees are responsible for the following:

1. Complying with the procedures and guidelines set forth in this protocol.

2. Protecting their remote access credentials and devices from disclosure to, or use by, unauthorized persons.
3. Immediately reporting any suspected unauthorized use of their remote access account or any damage to or loss of Office computer hardware, software, or data that has been entrusted to their care.

IV. POLICY AND GUIDELINES

Remote access to the Office's network provides many benefits. It allows personnel traveling on business to connect to Office information resources and provides the capability for telecommuting. However, remote access to the Office's network via dialup or other connectivity poses a risk of intrusion into the network by unauthorized persons, as well as interception of the data being transferred through the remote connection.

Direct connectivity to the Internet or other network outside of the Office's network also lacks the protections afforded by the Office's corporate firewall and other perimeter protections.

The Office of Early Learning must implement additional security measures to mitigate the increased security risks presented by remote access.

A. All remote connectivity must be authenticated using strong or multi-factor authentication (such as the use of passwords in conjunction with tokens).

B. All confidential data transferred over a remote access connection must be encrypted to protect it from unauthorized disclosure.

C. All security policies for use in the Office physical environment must also be observed when using or connecting to Office resources while outside the Office physical environment.

D. Any personal equipment, including personal home computers, used to connect to the Office's information resources must meet Office remote access requirements, including having an approved antivirus program installed and configured with the latest updates.

E. Office confidential data is not to be stored (following usage) on any non-Office computers.

F. It is the responsibility of associates to ensure their access devices and remote connections are not used by unauthorized persons (including family members).

G. Employees may not change operating system configurations, install new software, alter equipment or add to it in any way (e.g., upgraded processors, expanded memory, or wireless cards), or download software from systems outside of the Office onto remote access computers.

H. To prevent unauthorized employees from accessing confidential Office information via open modem ports, Office employees must log out rather than hang up after completing a remote session. They must also wait until they receive a confirmation of their log-out command from the remotely connected Office machine before they leave the computer they are using.

I. The Office will adhere to References A. and B. and subsequent publications.

V. ENFORCEMENT

Violation of this protocol could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment or referral for criminal prosecution.

SUBJECT/POLICY NUMBER:

5.05.02.26 TELEPHONE SECURITY

PURPOSE/SCOPE:

Office telephony resources are subject to the same security requirements and protections as other information resources. This protocol establishes procedures and governs the use of telephones, modems, PBXs and other telephony resources at the Office.

I. REFERENCES

None.

II. DEFINITIONS

Analog - A method of transmitting information in a continuous fashion via energy waves.

Confidential Data/Information - Any data that is categorized as "confidential" under the Office's information resource classification protocol and framework.

ISDN - A type of communication line which can carry voice, digital network services and voice over internet protocol.

Modem - A device that enables a computer to transmit data over telephone lines by converting data between the computer's digital format and the phone line's analog format.

Private Branch Exchange (PBX) - A private telephone switchboard that provides on-premises dial service and may provide connections to public communications networks.

Telephony - The technology associated with the electronic transmission of voice, fax, or other information between distant parties using systems historically associated with the telephone.

III. ROLES AND RESPONSIBILITIES

A. The Information Systems Security Officer (ITSO) is responsible for auditing the use and management of Office telephony resources to ensure compliance with the Office Information Systems Security Program policy.

B. Information Custodians are responsible for assisting information owners with deploying, managing and protecting their telephony resources in compliance with the Office Information Systems Security Program policy.

C. Information owners are responsible for deploying, managing and protecting their telephony resources in compliance with the Office Information Systems Security Program policy.

D. Supervisors are responsible for ensuring their associates understand and comply with this protocol.

E. Employees are responsible for using Office telephony resources in an ethical, responsible and secure manner, in accordance with this protocol and existing the Office Information Systems Security Program policies.

V. POLICY AND GUIDELINES

Telephone services are intended to support the objectives and operations of the Office and are critical to fulfilling the Office's mission. These telephony resources are vulnerable to a variety of security threats and should be granted the same protection as other information resources.

When using the Office phone system or Office-issued cellular phones, employees should adhere to the following guidelines to protect the information communicated:

A. Understand that there should be no expectation of privacy when using these resources.

B. The Office may audit use of these resources.

C. It is possible for third parties to tap or redirect phone calls outside of the Office.

D. No confidential data should ever be discussed over a mobile phone because of the ease of intercepting such communications.

E. Make sure that the person on the other end of the conversation is who they say they are. Do not give out confidential information (including agency credit card information) unless you are sure of the identity of the person on the other end of the line.

F. Be cautious when discussing confidential information that the conversation cannot be overheard by unauthorized persons (such as visitors to the Office). Minimize use of speakerphone.

G. Obey relevant laws regarding the recording of phone conversations, including informing the other party that you are recording.

H. Follow the Office's Acceptable Use policy in using phone resources, just as you would with email or other information resources.

I. The Office's VOIP and other critical telephony components must be protected in the following manner:

1. This equipment should be stored in a secure, environmentally controlled location in accordance with the Office's physical security protocol.

2. Telephony equipment is subject to the same security policies as other computer equipment, including Access Control, Change Control, Auditing, Patch Management, Server Security, Network Security, etc.

3. Additional security threats and vulnerabilities applicable to telephony equipment must be analyzed and mitigated commensurate with the levels of risk and criticality/confidentiality of those resources.

J. Modems or other telephony equipment may not be installed without the explicit approval of the appropriate official (e.g., Business Unit Manager for requested area of installation, or deputy director's designate for modems and related telephony equipment).

K. Analog Phone Lines - As a rule, the following applies to requests for fax and analog lines:

1. Fax lines are to be approved for departmental use only. No fax lines will be installed for personal use.

2. A business unit workstation computer that is capable of making a fax connection is not to be allowed to use an analog line for this purpose, due to security violation that are created.

3. Exceptions for the preceding protocol on analog-as-fax lines will be delivered on a case-by-case basis after reviewing the business need with respect to the level of confidentiality and security posture of the request.

L. The use of an analog/ISDN fax line is conditional upon the requester's full compliance with the requirements listed below. These requirements are the responsibility of the authorized employee to enforce at all times:

1. The fax line is used solely as specified in the request.
2. Only persons authorized to use the line have access to it.
3. When not in use, the line is to be physically disconnected from the computer.
4. The line will be used solely for Office business and not for personal reasons.

M. Computer-to-Analog Line Connections -The general protocol is that requests for computers or other intelligent devices to be connected with analog or ISDN lines from within the Office will not be approved for security reasons. Analog and ISDN lines represent a significant security threat to the Office and active penetrations have been launched against such lines by hackers. Waivers to the protocol will be granted on a case-by-case basis.

N. Requesting an Analog/ISDN Line -Once approved by a manager, the individual requesting an analog/ISDN line must provide the following information to the Office IT Unit:

1. A clearly detailed business case of why other secure connections available at the Office cannot be used.
2. The business purpose for which the analog line is to be used.
3. The software and hardware to be connected to the line and used across the line.
4. The confidentiality of the data to be transferred over the line.
5. To what external connections the requester is seeking access.
6. Whether the machines that are using the analog lines will be physically disconnected from Office's internal network.
7. A description of where the analog line will be placed.
8. Whether dial-in from outside of the Office will be needed.
9. The number of lines being requested and the number of people that will use the lines.
10. The line must be terminated as soon as it is no longer in use.

O. Any connectivity between the telephone system and the host network must be approved by the Office's deputy director.

P. The Office will adhere to NIST guidance as set forth in Special Publication 800-24, PBX Vulnerability Analysis and other publications.

VI. ENFORCEMENT

Violation of this protocol could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment or referral for criminal prosecution.

SUBJECT/POLICY NUMBER:

5.05.02.28 SYSTEMS DEVELOPMENT

PURPOSE/SCOPE:

Security must be integrated into all phases of the System Development Life Cycle (SDLC). This protocol establishes procedures for security regarding System Development covers all systems at the Office, whether or not purchased or developed internally.

I. REFERENCES

A. National Institute of Standards and Technology (NIST), Security Considerations in the Information System Development Life Cycle, Special Publications 800-64.

B. National Institute of Standards and Technology (NIST), An Introduction to Computer Security: The NIST Handbook, Special Publication 80012.

II. DEFINITIONS

Confidential Data - Any data that is categorized as "confidential" under the Office's information resource classification protocol and framework.

Media - Physical objects on which data can be stored, such as hard drives, zip drives, floppy disks, compact disks, CD-ROMs, DVDs, flash drives and tapes.

System Development Life Cycle - The system development life cycle (SDLC) starts with the initiation of the system planning process and continues through system acquisition/development, implementation, operations and maintenance and ends with disposition of the system.

III. ROLES & RESPONSIBILITY

A. The Information Systems Security Officer (ITSO) is responsible for the following:

1. Assisting System Owners in addressing the security issues present in each life cycle phase.
2. Providing baseline security requirements to be used for Office systems.
3. Auditing to ensure all systems are in compliance with this protocol.

B. Information custodians are responsible for the following:

1. Assisting information owners with the development and implementation of security controls
2. Ensuring system security controls are implemented properly and operating as intended
3. Maintaining the system in accordance with all standard operating procedures and other approved security management processes
4. Assisting the ITSO with testing and auditing of the system

C. Information owners are responsible for the following:

1. Understanding the security requirements for each system life cycle phase
2. Implementing the life cycle security requirements for their systems

3. Ensuring security controls are incorporated in the design, development and testing of contractor-developed software

IV. POLICY AND GUIDELINES

Each information system passes through multiple phases during its lifetime (SDLC), as it is planned, developed, deployed, operated and retired. Specific security-related activities must occur in each phase to assure that the system is secure.

It is usually more cost-effective to include preventive security measures from the start rather than to deal with security breaches later on. By considering security early in the information SDLC, the Office will be able to avoid higher costs later on while also developing a more secure system from the start.

Any system development or implementation project, including system modifications, must consider security in all phases of the SDLC and treat security as an integral part of the project plan.

A. In each phase of the SDLC there are specific information security requirements that need to be met:

INITIATION PHASE:

1. Conduct confidentiality assessment (information, potential damage, laws and regulations, threats, environmental concerns, security characteristics, Office protocol and Guidelines).
2. Consider which laws, regulations or policies establish specific requirements for the availability, integrity and confidentiality of the system. The environmental (e.g., hazardous location) and public threats to the system or information should also be considered.
3. Perform preliminary Risk Assessment and incorporate the results into the decision-making process regarding the development/acquisition of the system.

DEVELOPMENT/ACQUISITION PHASE:

1. Develop security requirements at the same time system planners define the other requirements of the system.
2. Incorporate security requirements into design specifications along with assurances that the security features acquired can and do work correctly and effectively.
3. Document the system's security design.
4. Conduct design reviews at periodic intervals during the developmental process to assure the proposed design will satisfy the specified functional and security requirements.
5. Develop operational practices including standard operational procedures and system-specific security policies (e.g., account management, backups, employee training, etc.). Develop a system handbook reflecting these practices.

IMPLEMENTATION PHASE:

1. Configure and enable the system's security features.
2. Implement the system's security management procedures.
3. Test the system and authorize it for processing via the Office's Certification and Accreditation (C&A) process.

OPERATION/MAINTENANCE PHASE:

1. Perform the security activities outlined in the system security plan (e.g., performing backups, holding training classes, managing accounts.)
2. Any changes made, or maintenance performed, on the system must comply with the Office's Change Control and Patch Management policies and processes.

DISPOSAL PHASE:

1. Information may be moved to another system, archived, discarded, or destroyed in accordance with Florida Department of State Retention Schedules.
2. Dispose of any storage media as required by the Office's Media Management policies.
3. Dispose of software in keeping with its license or other agreements
4. Categorize each application as required by the Office's Information Resource Classification protocol and provide protection appropriate to its level of confidentiality and criticality.

SYSTEM TESTING:

1. Test all systems thoroughly prior to placement in the Office production operating environment.
2. Do not use confidential data to test applications software until software integrity has been reasonably assured by testing with non-confidential data or files.

B. Documentation of confidential systems must be provided the same degree of protection as that provided for the software.

C. Application software used at the Office must be obtained through authorized procurement channels and must comply with all licensing requirements.

D. Systems must comply with all Office information security policies and procedures (e.g., system hardening, access control, backup and recovery, etc.).

E. The Office must comply with References A. - B. and subsequent publications.

V. ENFORCEMENT

Violation of this protocol could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment or referral for criminal prosecution.

SUBJECT/POLICY NUMBER:

5.02.29 ELECTRONIC MAIL

PURPOSE/SCOPE:

Electronic mail must be protected from the threats and vulnerabilities that can cause system damage, data compromise and business disruption. , receive or store electronic mail, as well as use of any non-Office Email systems to transfer Office data.

I. REFERENCES

A. Office of Early Learning Use of Internet, Email and Computing Resources Policy 5.03.

B. Florida's Public Records Law, Chapter 119, Florida Statutes.

II. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), GUIDELINES ON ELECTRONIC MAIL SECURITY, SPECIAL PUBLICATION 800-45.

III. DEFINITIONS

Confidential Data - Any data that is categorized as "confidential" under the Office's information resource classification protocol and framework, or state or federal law.

Information Resources - The procedures, equipment, facilities, software and data that are designed, built, operated and maintained to collect, record, process, store, retrieve, display and transmit information.

Spam - Unauthorized and unsolicited electronic mass mailings.

IV. ROLES AND RESPONSIBILITIES

A. The Information Systems Security Officer (ITSO) is responsible for auditing email systems and usage to ensure compliance with the procedures and guidelines provided in this protocol.

B. Information custodians are responsible for assisting information owners in implementing the procedures and guidelines specified in this protocol.

C. Information owners are responsible for ensuring any email system they own and the data they own which is transmitted via email, adhere to this protocol and its associated procedures and guidelines.

D. Supervisors are responsible for ensuring their associates understand and adhere to the procedures and guidelines provided in this protocol.

E. Employees are responsible for adhering to the procedures and guidelines provided in this protocol.

V. POLICY AND GUIDELINES

Electronic mail is an essential tool used by Office to conduct its business. Email is a vital method of exchanging messages and data files over computer networks.

However, email is inherently insecure and presents many risks to Office information security. Email can be read, altered, or deleted by unknown parties without the permission of the person who sent or received the message. Email can also be used to distribute viruses and other harmful codes that pose a threat to Office resources. Employees might also send inappropriate, proprietary, or other confidential information via email,

thus exposing the Office to legal action or damage to its reputation. After web servers, an organization's mail servers are typically the most frequent targets of attack.

The Office of Early Learning must take prudent security precautions in administering and using email.

A. Employees must understand that email can be intercepted or altered without the knowledge of the sender or recipient when it is transferred over the Internet.

B. Confidential information will not be sent over the Internet (via email or other means) without being encrypted. Confidential information should be encrypted when transferred outside of the state's network.

C. To ensure data is adequately protected, Office personnel will only send official data via Office-owned or operated email systems.

D. Permission may be granted by Management to use an alternate system in the case of an emergency.

E. Office employees are not permitted to forward Office email or attachments to personal accounts managed by public email or Internet service providers where the information might be compromised.

F. Employees are prohibited from using any Office email systems (or any other email systems accessed from Office computers) for prohibited purposes, as outlined in Reference A.

G. Employees may not direct unauthorized or personal messages to the "All" Office distribution group or other large groups of users.

H. Emails should be deleted once no longer needed. Old emails that must be retained should be archived from the email server on a periodic basis. Email is generally subject to the Florida Public Records Law to the same extent as it would be on paper. For further guidance regarding confidentiality of records and Florida Public Records Law, see Reference B.

I. The following procedures should be used to avoid potential damage caused by email-borne computer viruses:

J. All incoming emails should be scanned for viruses in accordance with the antivirus protocol in place at the agency hosting the Office's email.

K. Employees should not open attachments or click on links in messages from senders they do not know.

L. Employees should report all suspicious emails to the ITSO.

M. Emails containing executable attachments should be filtered and quarantined from entering the Office's host network.

N. To minimize spam and avoid waste of Office resources, employees must avoid using their Office email addresses for personal correspondence on the Internet, particularly if they do not know or have a trust relationship with the other party. This especially includes giving out one's official email address to Internet shopping sites, bulletin boards and mailing lists.

O. Employees will have no expectation of privacy while using the Office's email system.

P. The Office must follow Reference C. and subsequent publications.

VI. ENFORCEMENT

Violation of this protocol could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment or referral for criminal prosecution.

SUBJECT/POLICY NUMBER:

5.05.02.30 DATABASE SECURITY

PURPOSE/SCOPE:

Securing information, so that it remains consistent, complete and accurate, is essential to the Office's reputation, mission and critical business objectives. This protocol establishes procedures for Database Security and applies to all Office databases.

I. REFERENCES

A. National Institute of Standards and Technology (NIST), Recommended Security Controls for Federal Information Systems and Organizations, Special Publication 800-53-Rev. 3.

II. DEFINITIONS

Availability - Assuring information and communications services will be ready for use when expected.

Confidentiality - Assuring information will be kept secret, with access limited to appropriate persons.

Confidential Data - Any data that is categorized as "confidential" under The Office's information resource classification protocol and framework.

Data - A representation of facts or concepts in an organized manner in order that it may be stored, communicated, interpreted, or processed by automated means.

Database - An organized collection of logically related information stored together in one or more computerized files.

Integrity - Assuring information will not be accidentally or maliciously altered or destroyed. Information has integrity when it is timely, accurate, complete and consistent.

Validation - The checking of data for correctness and/or for compliance with applicable standards, rules and conventions.

Verification - The process of ensuring information has not been changed in transit or in storage, either intentionally or accidentally.

III. ROLES AND RESPONSIBILITIES

A. The Information Systems Security Officer (ITSO) is responsible for the following:

1. Providing guidance to information owners and Custodians regarding database security.
2. Auditing Office databases, servers and applications to ensure compliance with this protocol.

B. Information Custodians are responsible for the following:

1. Assisting information owners with maintaining the confidentiality, integrity and availability of their data.
2. Assisting information owners with implementing the prescribed database security controls.
3. Immediately reporting breaches of database security to the Information Owner and the ITSO.

C. Information owners are responsible for the following for data that they own:

1. Ensuring the confidentiality, integrity and availability of the data.
2. Ensuring data integrity and validation controls are installed, operated and maintained.
3. Authorizing and limiting access to data they own.
4. Reporting database security incidents to the ITSO.

D. Supervisors are responsible for the following:

1. Ensuring their associates understand and comply with this protocol.
2. Reporting any suspected incidents to the ITSO and the Information Owner.

E. Employees are responsible for the following:

1. Not accessing data that they are not authorized to access and/or for which they do not have a legitimate business need to know;
2. Exercising due diligence to prevent accidental mis-entry, modification or deletion of data; and
3. Immediately reporting any security incidents to the Information Owner or Custodian.

IV. POLICY AND GUIDELINES

The Office has been entrusted with a variety of confidential data to accomplish its goals. The success of Office programs depends on the availability, integrity and confidentiality of this data. In order to protect this data, the Office implements the following data security measures, such as data validation and verification controls.

These controls are used to protect data from accidental or malicious alteration or destruction and to provide assurance to the employee that the information meets the expectations about its quality and that it has not been altered.

A. Data will be secured commensurate with its level of confidentiality and criticality.

B. Databases and applications that interface with databases, will be configured in accordance with security best practices:

1. Integrity verification programs, such as consistency and reasonableness checks, will be used to look for evidence of data tampering, errors and omissions.
2. Reconciliation routines (checksums, hash totals, record counts) will be used to ensure software and data have not been modified.
3. If employees are allowed to make updates to a database via a web page, these updates should be validated to ensure they are warranted and safe.
4. For databases containing confidential information, table access controls should be applied. Access to specific information within the database should be limited to only those personnel who need access to that information and access should be limited to only those functions (e.g., read, write, modify, etc.) required for the person to perform his or her duties.
5. Database servers should be configured to only allow connections from authorized, trusted sources (such as the specific web servers to which they supply information).

C. For confidential data, audit trails should be created and maintained within the database to track transactions and provide accountability.

D. Securing confidential information by selectively encrypting data within the database is encouraged.

E. Databases containing non-public information should never be on the same physical machine as a web server.

F. Databases (and database servers) that store public access information cannot be used to also store non-public (e.g., private, proprietary, confidential) information.

G. Integrity errors and unauthorized or inappropriate duplications, omissions and intentional alterations will be reported to the Information owner.

H. Database servers and database software must adhere to all Office information security policies and procedures pertaining to servers and systems, including patching, hardening, change control, authentication, etc.

I. The Office will follow Reference A. regarding database security.

V. ENFORCEMENT

Violation of this protocol could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment or referral for criminal prosecution.

SUBJECT/POLICY NUMBER:

5.05.02.31 MEDIA MANAGEMENT

PURPOSE/SCOPE:

Media must be handled, stored and disposed of properly in order to protect the confidential or critical Office data stored upon it. This protocol establishes procedures for Media Management and applies to all media that is used to store Office data.

I. REFERENCES

None.

II. DEFINITIONS

Confidential Data - Any data that is categorized as "confidential" under the Office's information resource classification protocol and framework.

Media - Physical objects on which data can be stored, such as hard drives, zip drives, floppy disks, compact disks, CD-ROMs, DVDs, flash drives and tapes.

Sanitization - To expunge data from storage media so that data recovery is impossible. The most common types of sanitization are destruction (e.g. burning or smashing), degaussing (i.e. demagnetizing) and overwriting.

III. ROLES AND RESPONSIBILITIES

A. The Information Systems Security Officer (ITSO) is responsible for developing media management standards and performing auditing to ensure media is being handled and disposed of in accordance with Office policies and procedures. This may include assisting in the development of procedures for media transfer to include tracking.

B. Information custodians are responsible for the following:

1. Assisting information owners with the proper handling of their media in accordance with Office policies and procedures.
2. Complying with Office policies and procedures for any media entrusted to them.
3. Reporting the loss, damage, or theft of any media entrusted to them that contains Office data.
4. Ensuring any media they own and media that contains data or applications that they own, are handled and disposed of in accordance with Office policies and procedures.

C. Supervisors are responsible for the following:

1. Ensuring their associates understand how to properly handle and dispose of media in accordance with Office policies and procedures.
2. Communicating changes in policies and procedures to their staff.

D. Employees are responsible for the following:

1. Protecting Office media in their possession from tampering or accidental damage.

2. Storing Office data only on approved media designated in the Office IT Operations Manual.
3. Backing up data that is stored on media in their physical possession.
4. Reporting the loss, damage, or theft of any media containing Office data.

IV. POLICY AND GUIDELINES

The Office has been entrusted with a variety of confidential data in order to accomplish its mission. This data, which is stored on a variety of media, must be protected from unauthorized disclosure, damage, fraud and abuse.

To protect the security and privacy of information, the Office will use a variety of security mechanisms that provide protections for media.

MEDIA HANDLING

A. Employees should take all reasonable steps to protect Office storage media in their possession from tampering or accidental damage.

B. Employees are responsible for making their own backups of any data that is not stored on Office servers.

C. Appropriate physical and environmental protection controls will be provided for stored media.

D. Handling media that contain confidential data:

1. Media should be marked with its classification level. Labeling will include any special handling instructions.
2. Media must be secured (such as kept in a locked drawer, cabinet, or safe) when not in use or unattended. Any media confidential information transported through the mail or courier/messenger service will be double-sealed, the second envelope will be appropriately marked with the confidentiality classification of the data.
3. The receipt and delivery of media containing confidential data must be monitored and accounted for to ensure data is not lost and potentially compromised while in transit.
4. Confidential information will be turned over or will be put out of sight when visitors are present.

MEDIA DISPOSAL:

A. Employees need to understand that simply deleting data from media does not completely or permanently remove the information. Deleted files are susceptible to unauthorized retrieval if not disposed of properly.

B. Media that contain confidential data must be sanitized when they are no longer needed to store the confidential data.

C. Before any Office-owned or managed computing equipment is transferred, donated, or otherwise disposed of, storage media associated with the equipment must be sanitized via the Office's IT Operations Manual.

V. ENFORCEMENT

Violation of this protocol could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment or referral for criminal prosecution.

SUBJECT/POLICY NUMBER:

5.05.02.32 PASSWORD MANAGEMENT

PURPOSE/SCOPE:

The Office will protect access to its information resources by ensuring any passwords used for authentication are properly assigned and protected. This protocol establishes procedures for Password Management and applies to all Office-owned or operated information systems, both operational and in development.

I. REFERENCES

A. National Institute of Standards and Technology (NIST), Recommendations for Electronic Authentication, Special Publication 800-63.

II. DEFINITIONS

Authentication - The process of verifying that an employee is who he or she purports to be. Techniques are usually broken down into three categories: (1) something the employee knows, such as a password or PIN; (2) something the employee has, such as a smartcard or ATM card; and (3) something that is part of the employee, such as a fingerprint or iris.

Employee ID - Character string that uniquely identifies an employee or computer process.

Password - Any secret string of characters which serves as authentication of a person's identity and which may be used to grant or deny access.

III. ROLES AND RESPONSIBILITIES

A. System Developers must ensure their systems support the procedures and guidelines specified in this protocol document.

B. The Information Systems Security Officer (ITSO) will:

1. Provide advice to information owners and Custodians regarding system-specific password policies.
2. Audit systems to ensure compliance with this protocol.

C. Information custodians will:

1. Assist information owners with implementing measures to enforce protocol selection and management on their systems.
2. Instruct employees regarding system password protocol.
3. Assist the ITSO with auditing for compliance with this protocol.
4. Report any password compromises of Office information resources to the ITSO and the Information Owner.

D. Information owners will ensure the resources they own comply with the guidelines set forth in this protocol.

E. Supervisors will:

1. Ensure their personnel understand and comply with the guidelines contained in this protocol.

2. Report any suspected violations or password compromises to the ITSO and the Information Custodian.

F. Employees will understand their responsibilities for selecting and safeguarding their passwords and immediately notify a supervisor or the Information Custodian if they suspect that a password has been compromised.

IV. POLICY AND GUIDELINES

In order for passwords to be an effective tool for providing security, they must be selected, stored and administered appropriately. If passwords are poorly chosen, they can easily be guessed and then used by unauthorized persons. Likewise, passwords that are inappropriately stored are subject to disclosure and misuse by unauthorized persons.

The Office of Early Learning must incorporate password management guidelines in its IT Security Policy.

A. In systems that use passwords as their authentication method, every account (including newly issued accounts) will have a password.

B. Passwords must be changed:

1. Immediately upon initial employee logon.
2. At least every 90 days.
3. Individual systems may set a shorter expiration period for their employees.
4. Systems will have an automated mechaninism to ensure passwords are changed.
5. If it is suspected that the password has been compromised.
6. For administrator accounts, immediately upon the departure of personnel with access to those accounts, or upon suspected compromise of those passwords.

C. The following guidelines apply to password storage and visibility:

1. Passwords will not be visible on a screen, hardcopy or other output device.
2. Passwords will never be stored in a clear text file. This includes storage of passwords in configuration files, database files, application code and system directories. Any such passwords must be encrypted if they are required.
3. Passwords will not be sent via unsecured (i.e., unencrypted and unauthenticated) email.
4. Passwords will not be stored in written form (e.g. sticky notes) except if secured in an approved locked area.
5. Passwords are never to be lent or divulged to other persons, including individuals purporting to be system administrators.

D. A poorly chosen password could compromise the entire Office computer network. The object when choosing a password is to make it as difficult as possible for someone to guess what you have chosen. The following guidelines should be used to select strong, effective passwords:

E. Employees with multiple accounts on the same Office system (e.g. an administrative account and a regular employee account) must use completely different passwords for each account. Generic or group passwords will not be used.

F. Employees are not to use the same password at the Office that they use for any non-Office computer accounts (e.g. an account on an Internet website).

G. At a minimum, individuals creating passwords should use the following protocol:

1. Passwords should be at least eight (8) characters and contain a combination of letters, numbers and special characters.
2. Passwords cannot be reused for at least six (6) changes.
3. Never assign a login account a password that is the same string as the Employee ID or that contains the Employee ID (e.g., "bob123" is not an appropriate password for employee "bob").
4. Never set any password equal to the null string (i.e., a blank password), which is equivalent to no password at all.
5. Passwords should not be a dictionary word in any language.
6. Passwords should not contain any proper noun or the name of any person, pet, child, or fictional character.
7. Passwords will not contain any associate serial number, Social Security Number, birth date, telephone number, or any information that could be readily guessed about the creator of the password.
8. Passwords should not contain any simple pattern of letters or numbers, such as "xyz123."
9. Passwords should not share more than three (3) sequential characters in common with a previous password (i.e., do not simply increment the number on the same password, such as fido1, fido2, etc.).
10. Use a password that is easy to remember (e.g., a phrase, line from a song, or nonsense words) and that you can type quickly.

H. The assignment of passwords for specific Office systems should adhere to the following:

1. Each system should have its own password selection standard that adheres to the above guidelines while being commensurate with the level of security required by the level of confidentiality of the system.
2. The system will be configured to enforce the password selection criteria specified in the system criteria.
3. Employees should avoid using the "remember password" feature on web sites and other applications.
4. If SNMP is used, the community strings should follow the same selection guidance provided for passwords.

I. The Office must follow Reference A. and subsequent publications.

V. ENFORCEMENT

Violation of this protocol could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment or referral for criminal prosecution.

SUBJECT/POLICY NUMBER:

5.05.02.33 INFORMATION ASSET MANAGEMENT

PURPOSE/SCOPE:

All information assets must be tracked and managed to ensure they are not lost or misused. This protocol establishes procedures for Information Asset Management and applies to all Office information assets, including but not limited to workstations, servers, network devices, printers, personal digital assistants (PDAs), phones, software and licenses.

I. REFERENCES

A. Office of Early Learning (the Office) Use of Internet, Email and Computing Resources Policy 5.03.

II. DEFINITIONS

Information Asset - An information resource that has tangible value.

Information Resource - The procedures, equipment, facilities, software and data that are designed, built, operated and maintained to collect, record, process, store, retrieve, display and transmit information.

III. ROLES AND RESPONSIBILITIES

A. Information Systems Security Officer (ITSO) is responsible for auditing to ensure information assets are being tracked and managed in accordance with this protocol.

B. Information Custodians are responsible for assisting information owners with inventorying, tracking and protecting Office information resources in their care.

C. information owners are responsible for ensuring the inventorying, tracking and protecting the Office information resources that they own.

D. Supervisors are responsible for ensuring their associates understand their responsibilities regarding protection of information resources.

E. Employees are responsible for exercising due diligence in protecting information resources entrusted to them and immediately reporting the loss, theft or damage of any Office information resource.

IV. POLICY AND GUIDELINES

Each year, thousands of information assets are lost or stolen. Often agencies simply lose track of these items, resulting in exposing the Office to unnecessary risks.

Note: FDOE barcodes and manages the periodic inventory of the Office's real property. All Office associates should follow FDOE's protocol regarding the receipt, inventory and disposal of real property.

Not only would loss of information assets result in a financial impact on the Office, but it could also result in unauthorized access to data stored on or accessed through these assets and could have a detrimental effect. Additionally, the tracking and management of information assets is mandated by several federal regulations, such as the Clinger-Cohen Act.

A. The Office must keep a record of all information assets, including those mentioned in the scope above.

B. Information assets are to be added to the record upon receipt by the Office and assigned a barcode.

C. For each information asset, the Office will track at least the following information:

1. The brand, model and type of asset.
2. Serial number and the Office or DOE barcode.
3. The person to whom the asset is assigned.
4. The location of the asset.
5. Any maintenance agreements for the asset.
6. The date of receipt of the item.
7. Grant Number.
8. Date the record was last updated or inventoried.

D. Upon disposal of an information asset, the Office will track the date of disposal, the method of disposal (e.g., transfer, destruction, donation, etc.) and the name of the new owner (if there is one).

E. Periodic inventories are to be performed to verify records and account for all information assets.

F. Each asset is to be inventoried at least annually.

V. ENFORCEMENT

Violation of this protocol could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment or referral for criminal prosecution.

SUBJECT/POLICY NUMBER:

5.05.02.34 APPLICATION AND DATA SERVICES DISASTER RECOVERY

PURPOSE/SCOPE:

To define recovery objectives and to specify a set of procedures for achieving those objectives. This policy applies to all Office personnel and IT systems, networks and assets.

I. REFERENCES

A. The Public Company Accounting Reform and Investor Protection Act of 2002 (Sarbanes-Oxley, SOX).

B. ISO/IEC Standard 27002:2005 - Application and Data Services Code of Practice for Information Security Management, Clause 8.4.1 (Information Back-Up) http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50297.

C. Health Insurance Accountability and Portability Act (HIPPA)(Public Law 104-191(1996)) National Institute for Standards and Technology (NIST), Recommended Security Controls for Federal Infomratino Systems and Organizations, Special Publication 800-53.

D. Federal Emergency Management Agency Publication #141 - Emergency Management Guide for Business and Industry.

II. DEFINITIONS

Business continuity - The degree to which an organization may achieve uninterrupted stability of systems and operational procedures.

IT disaster - A sudden, significant event that may result in the loss or destruction of Office information and/or loss of service on the network used by Office associates.

III. ROLES AND RESPONSIBILITIES

A. The Office deputy director, Early Learning Program Initiatives (IT DRC) is responsible for chairing the IT Disaster Recovery Planning Committee, coordinating IT disaster response and recovery, reporting on disaster response and recovery and updating the Recovery Plan.

B. The Office deputy director, Early Learning Program Initiatives is responsible for conducting and/or supervising testing of the IT Disaster Recovery Plan.

C. The IT Disaster Recovery Planning Committee (IT DRPC, or "the Committee") is responsible for developing and reviewing the IT Disaster Recovery Plan.

D. The CIO, or designate, is responsible for backing up and restoring Office data.

E. Tech Support staff are responsible for various recovery tasks, such as installation and testing of replacement equipment, operations systems, applications software, communications, etc.

F. Office executive management is responsible for final approval of the IT Disaster Recovery Plan.

G. All Office employees are responsible for notifying the IT DRC in the event of an actual or suspected disaster that may affect any part of Office's IT systems, infrastructure, or assets.

IV. POLICY AND GUIDELINES

The IT Disaster Recovery Plan (DRP) will be an integral part of Office's overall DRP, just as Application and Data Services is an integral part of the Office.

A. The Office will implement the Plan, educating employees in their roles and responsibilities; test the Plan, to see if it will ensure rapid and full recovery; and fix flaws identified in testing, to better ensure the Plan will work when it is most needed.

B. The Office will establish an IT Disaster Recovery Planning Committee (IT DRPC), composed of key personnel from each functional area within the Office and the ITSO, who will chair the Committee.

THE IT DRPC

A. The IT DRPC chair, or designee, will obtain and analyze information for development of the IT Disaster Recovery Plan, such as:

1. Conducting a risk assessment of each of Office's IT systems.
2. Gathering IT industry information on best practices and technologies and identifying appropriate means of mitigating risk.
3. Identifying and assessing external resources and their capabilities.

B. The IT DRPC will meet to:

1. Analyze and discuss the information obtained by the IT DRPC chair.
2. Identify mission-critical systems and services, determining how long each business unit can survive without those systems/services in operation (conduct a business impact analysis).
3. Establish recovery priorities.
4. Develop the IT Disaster Recovery.
5. Submit to executive management for final approval.

C. The IT DRPC chair will:

1. Ensure the IT Disaster Recovery Plan is documented and communicated to all Office employees.
2. Coordinate IT disaster recovery training with the Human Resources Manager.

THE IT DISASTER RECOVERY PLAN

A. The IT DRPC chair, or designate, will work with FDOE IT will ensure periodic backups of Office information stores (databases, etc.).

B. In the event any employee knows of or suspects an IT disaster, the employee will contact the IT DRPC and the DRPC will begin the response and recovery process in accordance with the Plan.

IT DISASTER RECOVERY PLAN REVIEW

A. Subsequent to an actual disaster and recovery, the IT DRPC chair will prepare a response and recovery report and submit it to the IT Disaster Recovery Planning Committee for review. The committee may recommend revisions to the plan, based on the findings contained in the report.

B. The IT DRPC chair, or designate, will test IT disaster response and recovery at least once every 12 months. The IT DRPC chair, or designate, should also test response and recovery upon any changes to the Plan (see section 4.2).

C. The IT DRPC will review the IT Disaster Recovery Plan on a regular basis (every two years, at a minimum) to determine if it continues to meet the Office's, customers' and legal/regulatory requirements.

IT DISASTER RECOVERY PLAN REVISION

A. After any review of the IT Disaster Recovery Plan, the IT DRPC chair, or designate, will be responsible for updating the plan.

B. Within one month of any such update, the IT DRPC chair will verify that the update is capable of providing the desired results by conducting a response and recovery test.

V. ENFORCEMENT

Violation of this protocol could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment or referral for criminal prosecution.

POLICY NUMBER/SUBJECT:

5.05.02.35 INTERNET USAGE

PURPOSE/SCOPE:

The Internet provides a useful means of obtaining information pertinent to certain Office tasks. Unfortunately, certain Internet websites contain malicious software which damage computers and cause a significant reduction of employee productivity. This protocol defines acceptable use guidelines for Internet usage by authorized Office employees. This policy applies to all Office personnel and consultants.

I. REFERENCES

None.

II. DEFINITIONS

None.

III. ROLES AND RESPONSIBILITIES

All Office employees are responsible for adhering to the stated protocol and notifying Office management if inappropriate Internet usage is being conducted.

IV. POLICY AND GUIDELINES

Office employees will access Internet websites solely for Office-related matters and/or other uses as described within the associated procedures. Although it is intended that the Internet be used for business purposes, access to other acceptable sites is permitted before or after approved working hours and during approved lunchtime, but not during breaks.

Examples of acceptable Internet sites are: health matters, weather, news, business topics, community activities and career advancement. Under certain circumstances, such as emergency weather conditions, access to sites such as weather and news services may be appropriate within approved working hours.

Employees will be granted use of the Internet to carry out the mission of the Office and to promote efficiency and improved communications with our internal and external customers. It is intended that the Internet be used for business purposes.

A. The Office's Application and Data Services division will maintain detailed records of all Internet usage for use in detecting abuse or misuse of this resource with or without notice to the employee.

B. Unacceptable use of the Internet by employees includes, but is not limited to:

1. Access to sites that contain obscene, hateful, pornographic, unlawful, violent or otherwise illegal material
2. Sending or posting discriminatory, harassing, or threatening messages or images on the Internet.
3. Using computers to perpetrate any form of fraud and/or software, film or music piracy
4. Stealing, using, or disclosing someone else's password without authorization
5. Downloading, copying or pirating software and electronic files that are copyrighted or without authorization

6. Sharing confidential material, trade secrets, or proprietary information outside of Office.
7. Hacking into unauthorized websites
8. Sending or posting information that is defamatory to the Office, its products/services, colleagues and/or customers.
9. Introducing malicious software onto the company network and/or jeopardizing the security of the organization's electronic communications systems
10. Sending or posting chain letters, solicitations, or advertisements not related to business purposes or activities
11. Passing off personal views as representing those of the organization

C. The Office Application and Data Services division is tasked with protecting the Office's IT assets from malicious attacks. Certain Internet websites are known to spread viruses and spyware. The ITS division will provide due diligence in blocking access to websites determined by the division to potentially cause harm to Office IT assets.

D. If an Office employee is unable to access a specific website, the employee may contact Office's ITS's User Services group and request access. The request and reason for access will be logged.

V. ENFORCEMENT

Unauthorized or improper use of government information resources could result in loss or limitations of use of these resources, as well as disciplinary and/or legal action, including termination of employment or referral for criminal prosecution.

POLICY NUMBER/SUBJECT:

5.05.06 HELP DESK

Purpose:

Application and Data Services' desk is focused on diligently providing services desk (help desk) support for the office environment. This policy sets forth the duties and responsibilities of the services desk and employees and consultants associated with IT's Support Services.

I. REFERENCES

None.

II. DEFINITIONS

ADS - Application and Data Services

CIO - Chief Information Officer

IT Security Services Officer - IT Manager with additional responsibilities as deemed necessary by the Chief Information Officer

III. ROLES AND RESPONSIBILITIES

Help Desk Support - Single point of IT contact to all Office internal and external customers. This service provides initial analysis of incidents and requests for service, troubleshooting and resolution, assignment to second level support, performance accountability and tracking.

Help Desk Lead - The Help Desk Lead and technicians log user issues; provide technical guidance and training to employees; resolve user issues (Tier 1); problem escalation determination and routing (Tier 2); monitor user issues to resolution. Reports directly to the ADS Manager.

IV. POLICY AND GUIDELINES

POLICY

The Application and Data Services Help Desk will provide support services to assist Office employees with IT-related questions/issues.

GUIDELINES

Office employees and contractors contact the Help Desk by email to report IT related issues or request additional resources from the various IT service areas.

Help Desk contact information:

Email: Help.Desk@OEL.MyFlorida.com

Telephone: 850-717-8556

The Services Desk adheres to a specific process to remediate IT related issues as defined within this manual:

A. Each Service Area's procedures and standards must ensure compliance with security requirements set forth within the Agency's "IT Security/Risk Mitigation Services Policy" (5.05.02).

B. Any discrepancy between technology operations and stated security policies must be documented and brought to the immediate attention of the office Chief Information Officer (CIO) for review.

C. The CIO will determine whether corrective actions must be performed or an exception granted. Any exception must be documented and may require modification to policies, standards and procedures within this document.

V. ENFORCEMENT

Circumventing the security policy and/or procedures for Application and Data Service may result in disciplinary and/or legal action, including termination of employment or referral for criminal prosecution.

POLICY NUMBER/SUBJECT:

5.05.07 DESKTOP COMPUTING SERVICES

Purpose:

Application and Data Services Support Services' desktop computing service is focused on diligently providing desktop support services for the Office's environment. This policy sets forth the duties and responsibilities of the desktop computing services, and all Office employees and consultants.

I. REFERENCES

None.

II. DEFINITIONS

None.

III. ROLES AND RESPONSIBILITIES

ROLES

ADS - Application and Data Services

CIO - Chief Information Officer

IT Management - Chief Information Officer and other IT Management as deemed necessary by the Chief Information Officer

Desktop Support - Installation, configuration, support and maintenance of end user desktop and laptop hardware, software, conference and training facility computing and electronic (audio / visual) systems support, application software management, PC deployment, updates, printer support and virus protection.

Remote Desktop Services - Installation, configuration, support and maintenance of remote access to Microsoft Office and Intranet/Internet sites. Access to other applications requires a service or project initiation request.

Desktop Security Services - Hard disk encryption and security for external devices.

RESPONSIBILITIES:

The Office's Desktop Computing service technicians install, test, troubleshoot and maintain hardware and software; implement and monitor PC standards and procedures; maintain service logs; coordinate vendor updates pertaining to desktop components; provide technical guidance and training to employees; monitor problem/change activities and coordinate the involvement of staff, clients and vendors to ensure effective resolution of user problems. Reports directly to the Information Support Services Manager.

IV. POLICY AND GUIDELINES

POLICY

The Office's ADS Desktop Computing service area will provide desktop support services to enhance the Offices's IT endpoint device capabilities.

GUIDELINES

Office employees and contractors may contact the Help Desk to report IT related issues or request additional resources from Desktop Computing.

Help Desk contact information:

Email: Help.Desk@OEL.MyFlorida.com

Telephone: 850-717-8556

The Help Desk adheres to a specific process to remediate IT related issues as defined within this manual. Each Service Area's procedures and standards must ensure compliance with security requirements set forth within the Agency's "IT Security / Risk Mitigation Services Policy" (5.05.02).

Any discrepancy between technology operations and stated security policies must be documented and brought to the immediate attention of the Agency's Chief Information Officer (CIO) for review.

The CIO will determine whether corrective actions must be performed or an exception granted. Any exception must be documented and may require modification to policies, standards and procedures within this document.

V. ENFORCEMENT

Circumventing the security policy and/or procedures for Application and Data Service may result in disciplinary and/or legal action, including termination of employment or referral for criminal prosecution.

POLICY NUMBER/SUBJECT:

5.05.08 DATA SERVICES

Purpose:

Application and Data Services' organization is charged with providing security, maintenance, database design, performance tuning and extensive monitoring of all the office's mission critical data residing on various relational database environments. This policy sets forth the duties and responsibilities of all Data Services organization and all Office employees, consultants and vendors.

I. REFERENCES

None.

II. DEFINITIONS

ADS - Application and Data Services

CIO - Chief Information Officer

ITSO – Information Systems Security Officer

III. ROLES AND RESPONSIBILITIES

ROLES

SQL Database Administration - Installation, configuration, support and maintenance of SQL database management software, full development lifecycle support, including storage management, performance tuning, monitoring, backup/recovery, middleware support and requisite management of servers and storage software.

Oracle Database Administration - Installation, configuration, support and maintenance of Oracle database management software, full development lifecycle support, including storage management, performance tuning, monitoring, backup/recovery, middleware support and requisite management of servers and storage software.

Data Warehouse Administration and Reporting - Installation, configuration, support and maintenance of data warehouse environment and reporting tools. Service includes data replication, extraction and load processes.

Data integration and interface Services - Development, support and maintenance of data integration and interface processes. Service includes data extraction, transmission, import/export files, batch management, integration with applications, monitoring and file transfer processes.

Backup/Recovery - Stand-alone file and data backup/recovery services not included in other Office services.

RESPONSIBILITIES:

A. The ITSO is responsible for reviewing the Data Services procedures with the Data Services supervisor to ensure the Office's critical data residing within its relational databases is properly controlled. The ITSO will provide direction to the Data Services organization to ensure all activities conform to the Offices's stated goals and objectives.

B. The Data Services supervisor is responsible for overseeing database administration, data administration and ownership of data interfaces used to view and/or manipulate data residing within the Offices's relational databases.

IV. POLICY AND GUIDELINES

POLICY

The ADS Operations' Data Services technicians and analysts-programmers will be responsible for the day-to-day monitoring and management of the Office's critical data residing within approved relational databases. The Data Services supervisor will guide personnel in the performance of the following services:

A. Data Services: Deals with the modeling of the data and treats data as an organizational resource. Analysts-programmers use knowledge of data design, data analysis, classification and maintenance of the Offices's data and data relationships to provide direct fact-based data for the Office's day-to-day administration of early learning services. The Data Services analysts programmers develop data models and data dictionaries, which, combined with transaction volume, are the raw materials for database design.

B. Database Administration: Works with the ADS technicians and analyst-programmers in the implementation of the various types of databases (i.e. SQL Server, Oracle) used by the Office to secure, manipulate and control critical data. This includes:

1. Database installation, configuration, integration, maintenance, and performance management,
2. Data management,
3. Data security management,
4. Database Administration includes
5. the development and design of database strategies,
6. monitoring and improving database performance and capacity planning for future expansion requirements.
7. planning, coordinating and implementation of security measures on new and existing database systems to safeguard the data.

C. Data Interface Analysis/Support. The Office uses several methods of extracting/manipulating data stored within the relational databases. Data Services works with ADS technicians to evaluate, certify and support several middleware products used to extract useful information from the Offices's databases.

GUIDELINES

A. Currently, the Office has two relational databases overseen and used by the Data Services group:

1. SQL Server Database
2. Oracle Database

Support for any other relational database environments must be formally requested stating reasoning for non-conformance to above standards to the ITSO for review. Exceptions will be granted solely based upon ITSO's analysis and the CIO's final approval.

B. Office employees and contractors may contact the Data Services Request Line by email to request ad hoc data provision reports and analysis to support the Office's mission. Email equests should be

specific, and contain: the period of review for the data requested; the purpose or audience for the data request; the desired format for the output of data results; the specific research question the data is intended to answer; and the priority of the request.

Data Services contact information:
Email: DataServices.Request@OEL.MyFlorida.com
Telephone: 850-717-8565

V. ENFORCEMENT

Circumventing the security policy and/or procedures for Application and Data Services may result in disciplinary and/or legal action, including termination of employment or referral for criminal prosecution.