State of Rhode Island
Department of Administration / Division of Purchases
One Capitol Hill, Providence, Rhode Island 02908-5855
Tel: (401) 574-8100 Fax: (401) 574-8387

August 18, 2017

ADDENDUM #2

RFP # 7553502

Title: RI WIC Management Information System (MIS) Transfer and Implementation Project

Bid Closing Date & Time: September 6, 2017 at 10:00 AM Eastern Time (ET)

Notice to Vendors

ATTACHED ARE CLARIFICATIONS FOR VENDOR QUESTIONS 50, 55, 68, 80,86, AND 106 CONTAINED IN ADDENDUM 1, AS WELL AS THE REVISED APPENDIX B AND SECURITY POLICY FORMS. NO FURTHER QUESTIONS WILL BE ANSWERED.

David J. Francis
Interdepartmental Project Manager

Interested parties should monitor this website, on a regular basis, for any additional information that may be posted.

1. **Response Clarification for Question 55:**

   The original Q and A from RFP 7553502 Addendum 1
   "Question 55: According to WICTechnologyPartners, MIS Source Code is provided by procurement only per the instructions for the individual solicitations.
   Q: What are the instructions for obtaining Crossroads Source Code?

   Answer to question 55: Detailed specifications for the Crossroads system can be found by creating an account at http://www.wictechnologypartners.com/. Accounts require no special permissions or validations. Once logged in, click the "Resources" link on the home page, then "MIS Documentation", then "Access Crossroads Support Documentation"."

   Clarification Answer: Upon further evaluation and discussion with our federal agency, U.S. Department of Agriculture (USDA), Food and Nutrition Service (FNS), it has been determined that the documentation available through the WIC Technology Partners website is sufficient to meet the requirements of this solicitation.

2. **Response Clarification for Questions 50, 80, 86, and 106.**

   Clarification Answer: Please find the revised Appendix B in hard copy as well as electronically attached.

3. **Response Clarification for Questions 68.**

   Clarification Answer: Please find the State of Rhode Island Department of Administration/Division of Information Technology Security Policies attached.

Appendix B - Bid Worksheet REVISED 8/17/2017

RI WIC Management Information System (MIS) Transfer and Implementation Project

22-Month Transfer and Implementation Budget, Plus 3-5 Year Hosting Budget (Phase 7)

Task/Deliverable		# of Hours	Per Hour Rate	Total Cost
Phase 1: Project Planning and Initiation			**Cost:**	**$**
1.1	**Kickoff Meeting Agenda**			
	E.G. Project manager			
1.2	**Project Plan and Schedule**			
	E.G. Project manager			
1.3	**Monthly Status Reports**			
	E.G. Project manager			
1.4	**Planning Documents**			
	E.G. Project manager			
1.5	**Project Kickoff Meeting Summary**			
	E.G. Project manager			
Phase 2: Design			**Cost:**	**$**
2.1	**Gap Analysis Report**			
	E.G. Project manager			
2.2	**Configurations Management Plan**			
	E.G. Project manager			
2.3	**Master Decisions Documents**			
	E.G. Project manager			
2.4	**Configuration Requirements Document**			
	E.G. Project manager			
2.5	**Interface Design Document**			
	E.G. Project manager			
2.6	**Site Readiness Checklist and Recommendations**			
	E.G. Project manager			
Phase 3: Development			**Cost:**	**$**
3.1	**Hosting Site Support Requirements**			
	E.G. Project manager			
3.2	**Hosting Site Transition Out Plan**			
	E.G. Project manager			
3.3	**System and User Documentation**			
	E.G. Project manager			
Phase 4: Testing			**Cost:**	**$**
4.1	**UAT Test Scripts**			
	E.G. Project manager			
4.2	**Readiness for UAT**			
	E.G. Project manager			

4.3	**Self-Learning Modules**			
	E.G. Project manager			
4.4	**Training Materials**			
	E.G. Project manager			
4.5	**Training Evaluations**			
	E.G. Project manager			
4.6	**Training Materials Update**			
	E.G. Project manager			
4.7	**Pilot Readiness Certification**			
	E.G. Project manager			
Phase 5: Pilot			**Cost:**	**$**
5.1	**Training Guides**			
	E.G. Project manager			
5.2	**FAQ Document**			
	E.G. Project manager			
5.3	**Rollout Readiness Certification**			
	E.G. Project manager			
Phase 6: Rollout			**Cost:**	**$**
6.1	**Updated FAQ Document**			
	E.G. Project manager			
6.2	**Final System Documentation**			
	E.G. Project manager			
Phase 7: Maintenance and Operations			**Cost:**	**$**
7.1	**Six Month Warranty**			
	E.G. Project manager			
7.2	**Level 2 Help Desk (for three (3) years)**			
	E.G. Project manager			
7.2B	**Optional Level 2 Help Desk (for year four (4))**			
	E.G. Project manager			
7.2C	**Optional Level 2 Help Desk (for year five (5))**			
	E.G. Project manager			
7.3	**Transition Period**			
	E.G. Project manager			
7.4	**System Hosting (for three (3) years)**			
	E.G. Project manager			
7.4B	**Optional System Hosting (for year four (4))**			
	E.G. Project manager			
7.4C	**Optional System Hosting (for year five (5))**			
	E.G. Project manager			
7.5	**User Group Coordination (for three (3) years)**			
	E.G. Project manager			

7.5B	**Optional User Group Coordination (for year four (4))**			
	E.G. Project manager			
7.5C	**Optional User Group Coordination (for year five (5))**			
	E.G. Project manager			
			Total of 7 Phases:	
	Travel Expense to RI		**Cost:**	**$**
Project Initiation Meeting				
Design Sessions				
Interface Design Sessions				
Final Configuration Sessions				
eWIC Training				
Training Materials Walkthrough				
State Training				
UAT Training/UAT	Per week:		For eight (8) Weeks:	
Train the Trainer				
Pilot	Per week:		For eight (8) Weeks:	
Rollout				
			Total Project Cost:	

Offerors may add additional lines to this budget form to accommodate staffing patterns per task. All deliverables must be accounted for and a cost associated with each task at a fully loaded hourly rate.

	POLICY#	STATUS	ISSUED	LAST REVISED	PAGE
	10-01	Accepted	7/21/06	5/14/09	1 of 5
State of Rhode Island **Department of Administration** **Division of Information Technology**		TITLE	**Enterprise Password Security**		
		DRAFTED BY		Dmitry Kuchynski	

1.0 Policy Statement:

Employees and vendors accessing State of RI information resources who use password authentication shall use a password that complies with this policy.

2.0 Policy Objective:

Ensure that State of RI information resources are protected by passwords that are secure and selected to hinder unauthorized access to password-protected resources.

3.0 Definitions:

State User: any State employee, vendor, contractor within the executive branch of state government who uses state information resources including network, applications, web resources etc. within the State network..

State Agency: Any department, commission, board, office, or other agency that:
1) is in the executive branch of state government;
2) has authority that is not limited to a geographical portion of the state; and
3) was created by the constitution or a statute of this state.

4.0 Policy and Control Requirements:

4.1 Compliant Activities:

- Each employee shall have a unique user identification (User ID) and password.
- Employees shall assign their own passwords.
- Passwords shall be changed (at least) every 90 days.
- Passwords shall contain a minimum of 8 characters.
- Passwords shall include characters from 3 of the following 4 categories:
  English uppercase characters (A through Z)
  English lowercase characters (a through z)

Base 10 digits (0 through 9)
Non-alphabetic characters (for example, !, $, #, %)

- Complexity requirements are enforced when passwords are changed or created.
- Passwords shall be changed after first assignment or following a password reset.
- Passwords shall be encrypted while stored on the computer.
- Passwords shall be changed as soon as they expire.
- Accounts shall be locked out after three unsuccessful login attempts.
- Passwords shall not be duplicated within the last 15 occurrences (changes).
- Employees shall change passwords when advised of a potential security breach by the Chief Information Security Offer (CISO), CISO's designee or agency information security manager.

- Examples of acceptable passwords (not to be used as actual passwords)
  Lou1$ville (used "Louisville" as your base word, substitute 1 for i and replace the s with $)
  Msi8Y0ld (compressed a phrase "my son is 8 years old")
  g00ds3cur!tE (used "good security" as your based phrase, substitute o for zero, e for 3, i for ! and used uppercase E)

4.2 Permitted Activities:

- Password defaults can be used for initial hardware and software setup or configuration. Following initial activities, these defaults shall be changed.
- Expired passwords shall be used only to reset or to self-assign a new password.

4.3 Prohibited Activities

- Passwords shall not contain the User ID, user name, company name, replicated sequence of characters, or any complete dictionary words.
- Passwords and User IDs shall not be provided to others or shared.
- Passwords and User IDs shall not be posted or displayed where other individuals may have access.

5.0 Exceptions to Policy:

Exceptions to this policy may be granted solely by the CISO or the CISO's designee.

Examples of possible exceptions that may be permitted:

- Passwords for special use and restricted accounts such as training or service accounts may be defined to not expire, shared, etc.
- Passwords may be included in secured batch files only if no other acceptable alternative can be identified.
- Password complexity requirements may be adjusted to suit older legacy hardware and software in instances where meeting the full requirements of this policy would either be impossible or cost-prohibitive.

6.0 Password Resets

An employee can request to have his/her password reset for central administrative systems hosted and administered by Division of Information Technology in two ways.

6.1 Visit the Service Desk

6.1.1 The Service Desk will request the requesting party to verify their identity via a State Id or Drivers license.

6.1.2 Once verification has been completed the Service Desk will build a service ticket and will forward the ticket to the appropriate service queue for action. (24 hour response is guaranteed)

6.1.3 If the user is not present, service desk will reset the password to allow user access to the network. A message will be left on the user's voice mail with new password.

6.2 Telephone the Service Desk

6.2.1 The Service Desk will request the requesting party to verify their identity based on the information stored in the service desk database

6.2.2 Once verification has been completed the Service Desk will build a service ticket and will forward the ticket to the appropriate service queue for action. (24 hour response is guaranteed)

6.2.3 Service desk will reset the password to allow user access to the network. A message will be left on the user's voice mail with new password.

6.2.4 If the requesting party does not have a phone number on record, the email verification from the employee's supervisor will be required authorizing the password change.

7.0 Implementation Responsibility:

Each employee shall be responsible for selecting a secure password, maintaining password confidentiality, and promptly changing the password when any security breach is suspected. The RI DOIT member shall review security logs regularly to identify suspicious login attempts or recurring failures.

Any individual requesting an employee password shall be referred to this policy document, the agency manager, or to the CISO or the CISO's designee.

8.0 Compliance Responsibility:

State Agencies shall be responsible for implementing and enforcing the Enterprise Password Security Policy within their supported areas.
State Agency managers shall be responsible for ensuring that employees who report to them comply with this policy.

10.0 Policy Violations and Disciplinary Actions:

An employee found to be in violation of this policy may face disciplinary action up to and including dismissal from employment and/or criminal prosecution where the act constitutes a violation of law. A breach of contract, where applicable, may also be considered.

11.0 References:

HIPAA 164.310 Physical Safeguards
(c) Workstation Security
HIPAA 164.312 Technical Safeguards
(a) (1) Access Control
(2) Implementation Specifications
(i) Unique User Identification
(ii) Emergency Access Procedure
(iii) Automatic Logoff
HIPAA 164.312 (d) Person or Entity Authentication
Cross-reference Access Security Policy

12.0 Approvals:

Tom McConnell
Director of Operations

5/14/09
Date

John E. Landers
Chief Information Officer

5/3/2009
Date

Director, Department of Administration

5/13/09
Date

	POLICY#	STATUS	ISSUED	LAST REVISED	PAGE
	10-05	Accepted	6/30/06	6/30/06	1 of 49
State of Rhode Island Department of Administration Division of Information Technology		TITLE	IT Security Handbook Management Controls		
		DRAFTED BY		Jim Berard	

TABLE OF CONTENTS

1. MIS INFORMATION TECHNOLOGIES (IT) SECURITY POLICY

1.1. PURPOSE

1.1.1. This chapter provides policy guidance to the Department of Administration, Division of Information Technology (DoIT) for the implementation of Information Technology (IT) security policies and procedures. Security policies define lines of authority, primary points of contact, range of responsibilities, requirements, procedures and management processes that implement and sustain the framework of a compliant and cost effective security program

1.2. BACKGROUND

1.2.1. The Department of Administration, Division of Information Technology (DoIT)s goal is to provide ready access to essential, evidential information, including essential information in electronic format.

1.2.2. This electronically formatted information is created, collected, processed, stored, communicated and/or controlled in assemblies of computer hardware, software, and/or firmware known as information systems.

1.3. POLICY

1.3.1. The Division of Information Technology (DoIT) IT Security Policy. The Division of Information Technology (DoIT) will develop an overall State-wide IT security policy that will explain:

- Purpose and scope of the DoIT security policy
- Assignment of responsibilities for program implementation, as well as individual and other related offices' responsibilities (i.e. Human Resources)
- System compliance issues

1.4. RESPONSIBILITIES

1.4.1. **Chief Information Officer** (CIO) ensures that all departments create and implement a security policy.

1.4.2. **Chief Information Security Officer (CISO)** develops the department-wide IT security policy and is appointed by the Chief Security Officer.

1.4.3. **Department Directors** ensure the implementation of the IT security policy within their respective divisions.

1.4.4. **Managers** ensure that staff and other authorized personnel have access to a copy of the IT security policy and discuss relevant IT security issues with affected individuals.

1.4.5. **Staff** reviews and complies with policies and procedures as outlined in the department's IT security policy.

2. IT SECURITY PROGRAM MANAGEMENT

2.1. PURPOSE

2.1.1. The Department of Administration, Division of Information Technology's STATE-WIDE security program management provides the elements for establishing and managing an IT security program and the criteria to consider when designating a Chief Information Security Officer (CISO)

2.2. POLICY

2.2.1. All departments offices must develop and implement procedures to provide guidance and support for the IT security program. These procedures provide for the enforcement of IT security policy and for the documentation and transmission of important information and decisions relating to computer security.

2.2.2. Information security must be an integral part of each departments Strategic Planning process.

2.2.3. Each department's IT security program is subject to external review for compliance with the Department of Administration, Division of Information Technology requirements. A security review is required to ensure the IT security program actively encompasses each of the key program elements.

2.2.4. Security audit documentation, responses, and correspondence related to these reviews are considered sensitive data and treated in a manner that ensures the confidentiality and integrity of these documents.

- Security audits must be maintained at the Division of Information Technology (DoIT)'s location in a secure file and be available for review by the CIO and State CISO and other authorized individuals (e.g., Inspectors Office, Federal and State Law enforcement etc.).

2.3. RESPONSIBILITIES

2.3.1. **<u>Directors</u>** will:

- Fully support and integrate IT Security into the overall Department structure
- Ensure that each department division maintains an effective IT Security Program
- Ensure that appropriate resources are allocated to the IT Security Program
- Ensure the effectiveness of each divisions program by monitoring and evaluating on an annual basis
- Provide the departments policy and guidelines required to conduct an effective agency-wide IT security program.

2.3.2. **<u>State CSO</u>** will:

- Audit all administrative and technical aspects of the IT security program at least once every three years. These audits are scheduled in advance and will be conducted by, or under the auspices of the Division of Information Technology (DoIT) staff.
- Report deficiencies and corrective actions needed to the affected Division Head, for review and follow-up.
- Follow-up to insure that all corrective actions have been implemented.
- Provide support to Division IT security programs through IT security training, monthly teleconference calls, written and electronic communication, videos, brochures and on-site security audits.

2.3.3. **<u>Department, Unit and Office Heads, and Regional Facility Directors</u>** will:

- Ensure the office or facility IT Security Program is being followed in accordance with the Department's IT Security policy requirements.
- Provide the necessary resources to accomplish the goals and objectives of the IT Security Program.
- Select a CISO and ACISO who organizationally report to the Office Head or CIO and who would have the necessary skills to perform this job.
- Assume the security responsibility for each office IT system by signing an accreditation document authorizing its use by, or on behalf of the office.

2.3.4. **Designated Department/Unit/Office Information Security Officer** coordinates the IT security program for the respective area of responsibility. An effective OCISO must:

- Understand the overall business operation of the department.
- Grasp the importance of information security (InfoSec) in the context of the overall department mission.
- Understand concepts in administrative security, and system management to the extent needed to manage the office security program.
- Establish office InfoSec priorities.

2.3.5. **Office** CISO develops, implements, and manages a comprehensive IT security program as described in this section. The Alternate CISO assists the CISO and is responsible for all aspects of the security program in the absence of the CISO. Functions of the CISO include, but are not limited to the following:

- Coordinates, plans, directs, implements, and supports the IT security program for the office.
- Participates with all echelons of management in planning, implementing, establishing and monitoring system controls of the office IT Security Program.
- Ensures compliance with the requirements for safeguarding personal and other sensitive data pursuant to the Computer Security Act of 1987, the Privacy Act of 1974, Freedom of Information Act, the Departments IT Security Policy and Guidelines, and compliance with other Rhode Island General Laws and directives that protect the department’s electronic information systems from waste, fraud, or abuse.
- Develops and facilitates establishment of office-specific IT security policy and procedures as required, to ensure compliance with this policy.
- Ensures that all information security policies are accurate, reviewed annually, and updated as necessary.
- Ensures that the Alternate CISO(s) is/are kept current on all security policy, procedures and issues.
- Reviews the effectiveness of the locally established IT procedures as implemented.
- Coordinates the application of security policies and procedures to ensure the physical security of computer systems, terminal devices, and access controls to system software and data.
- Ensures that proper procedures are followed for the storage and disposition of forms or other printed outputs containing sensitive data.

- Develop and monitor procedures for controlling and authorizing movement of peripheral devices to off-site locations.
- Coordinates Office system IT Risk Analyses with the STATE/CSO system administrator on a scheduled basis or when changes occur in the office risk environment.
- Facilitates the development of sensitive system security plans for each Department’s IT system and reviews these plans with the STATE/CSO at least annually, ensuring they are updated as required.
- Ensures appropriate and timely action to protect electronic information assets from damage, destruction, alteration, and misappropriation, including fire, safety, and planning for contingencies.
- Coordinates the development of the office IT contingency plan for all office systems and reviews these plans at least annually, ensuring that they are updated as required.
- Ensures that at least one copy of the facility/unit contingency plan is maintained off-site and the facility’s copies are kept in a secure on-site area.
- Ensures that training and assistance is provided to facilitate the development and periodic testing of office-level contingency plans.
- Manages and coordinates contingency plan tests of office IT resources with the State CSO.
- Reviews and evaluates the results of contingency plan tests and reports findings with recommendations to CIO and the STATE/CSO.
- Provides all documentation required for the accreditation of each facility system to the office head or facility director.
- Establishes and implements procedures for identifying and reporting suspected or actual IT security breaches.
- Advises Department Human Resources in establishing appropriate Position Sensitivity Level designations for each staff position.
- Ensures that background investigations (related to IT security) for temporary employees and consultants occupying sensitive positions are requested in a timely manner.
- Provides guidance to Human Resources in updating of position descriptions and performance standards to reflect IT security responsibilities.
- Prepares training material and conducts facility/office training sessions involving sensitive IT security for office staff.

- Coordinates departmental continuing IT security awareness and training program by distributing applicable security training information to the staff as it becomes available and works closely with staff to facilitate the IT security awareness effort.
- Conducts IT security orientation during staff entry processing.
- Establishes procedures to ensure that the Central HR, is notified, prior to the transfer or termination of any employee who has system access privileges; and that all computer devices used by that employee are either returned to the Division of Information Technology (DoIT) or are otherwise identified.
- Coordinates secure delivery of passwords with the system administrator.
- Maintains documentation of all local staff members that are authorized users of remote systems. Maintains documentation of remote users of local systems.
- Ensures that access for users who are no longer authorized users of the State of Rhode Island's computer systems is terminated.
- Conducts routine reviews of the security access request files to ensure that the State of Rhode Island's IT user access forms are appropriately signed by each new user to establish authorized access. (Form TBD)
- Serves as the principal contact person for dealing with Department/unit/section violations of IT security policy.
- Maintains an historical file on IT security-related incidents.
- Coordinates the secure provision of IT access for audit/investigative team members.
- Performs initial investigation and reports information security incidents to STATE/CSO.
- Coordinates security reviews of office systems and operations.
- Provides advice and guidance to ensure procedures are established for identifying and reporting breaches of physical security to information systems.
- Reviews annually all office security procedures and makes recommendations as appropriate.
- Ensures that procedures are developed and implemented to protect data transmission and media storage from unauthorized access.
- Reviews and evaluates the impact of proposed office changes on IT security.
- Reports security incidents to the STATE/CSO.

3. SECURITY PLANS

3.1. PURPOSE

3.1.1. This chapter provides policy and guidance on completing security plans for the State of Rhode Island (IT) resources. All departments units and offices are required to provide adequate levels of security protection for each IT resource from its initial concept phase through the remainder of its life cycle.

3.1.2. The system security plan provides details of the security and privacy requirements of the designated system and the system owner's plan for meeting those requirements. The IT security plan is a tool for the system administrator to determine the sensitivity level and protection requirements for the system. It provides the following assistance:

- Describes the control measures currently in place and any planned controls that are intended to meet the protection requirements of the system.
- Assists in determining whether or not current security measures are adequate.
- Determines what additional action and/or resources are required to bring the system in line with operational and security requirements.
- Establishes the actual milestones for completing requirements and may serve as an internal management planning and decision-making tool.
- Contains detailed technical information about the system, its security requirements and the controls implemented to provide protection against any vulnerability.
- Serves as a structured process for planning adequate cost-effective security protection for a system.
- Reflects input from the CSO, system administrators, information owners, end users, and the Chief Privacy Officer.
- Provides the major component utilized by management in determining whether to accredit a system and is the first step in the accreditation process.

3.1.3. The policy and guidance contained in this chapter applies to all systems and covers all such IT resources maintained in-house or in the interest of the State of Rhode Island , and applies to all existing Information Technologies, Applications, Systems and any automated technology acquired in the future. Compliance with this policy and guidance is mandatory for all State of Rhode Island, staff, contractors, and others having access to, operating, or acting in behalf of the State of Rhode Island, on these unclassified resources.

3.2. POLICY

3.2.1. As defined by this policy, a system is any device that has the ability to process and store or retrieves electronic data. It is identified by constructing logical boundaries around a set of processes, communications, storage, and related resources.

3.2.2. The elements within these boundaries constitute a single system requiring a security plan. Each element of the system must:

- Be under the same direct management control;
- Have the same function or mission objective;
- Have essentially the same operating characteristics and security needs; and
- Reside in the same general operating environment.

3.2.3. All State of Rhode Island Departments, units, sections and commissions must identify all Information Technology (IT) systems being used by or on behalf of the State of Rhode Island, their department, Unit, Section or office, and any system used on behalf of a Department, whether housed at that Department or in a remote location, must be in a security plan, including the following:

- All servers
- All telecommunication systems.
- All standalone PCs.
- All LANs.
- Any system used to connect a department's information resources to a remote location.

3.2.4. Grouping systems, when logical, is acceptable and the systems may be covered under one security plan. However, each operating system must be uniquely identified and controls established and policy for each operating system in the plan. Here we have a situation where, what appears to be a single system, incorporates several servers, each using a different operating system. Obviously, security features, designs, and configurations are going to be different for each one. Let's examine the criteria established for a system:

Elements for Consideration		
1. Are the systems under the same direct management control?		
2. Do they have the same function or mission objective?		
3. Do they have essentially the same operating characteristics and security needs?		
4. Do they reside in the same general operating environment?		

If, in this case, only three of the four criteria meet the required elements for a single system plan, then each of the systems should either have a separate plan, or if not a separate plan, then one that discusses the unique differences between the two operating systems and provides separation in terms of the security features, risks, configuration, and safeguards used.

3.2.5. All component systems covered by a system security plan need not be physically connected. An example of this scenario is an office that has standalone PCs throughout several sites that are all primarily used for administrative purposes and all have Windows software installed. All standalone PCs in the office fall under the auspices of the Department’s IT unit and a single system administrator controls all software, hardware, and communication devices related to these PCs. As before, let’s examine the criteria for establishing security plans for this situation.

Elements for Consideration		
1. Are the systems under the same direct management control?		
2. Do they have the same function or mission objective?		
3. Do they have essentially the same operating characteristics and security needs?		
4. Do they reside in the same general operating environment?		

In this case, suppose that all of the four criteria meet the required elements for a single system plan. Although, the PCs are spread throughout the office, it is clear they have the same overall general working and operating environment. To qualify under this general category, the PC must have no network or remote connection capability.

3.2.6. Offices will consider what systems they own and how they may logically group or not group the identified systems. The most important consideration is that all office systems are covered under a security plan.

3.2.7. Security plans will be dated for ease of tracking modifications and approvals.Modifications shall be forwarded to the Division of Information Technology, attention Configuration Management Section, in order to update DoIt's Configuration Management Data Base. Dating each page of a security plan may be appropriate if updates are to be made through change pages.

3.2.8. Security plans must be updated annually to reflect changes in technical, operational and management issues.

3.3. RESPONSIBILITIES

3.3.1. Division of Information Technology (DoIT)

3.3.1.1. **Director, IT Operations:**

- Assures management is assigned for all IT resources.
- Assigns security responsibility for each system under her/his authority. The State of Rhode Island Information Technology systems outside the authority of the Department of Administration, Division of Information Technology, will be assigned security responsibility by the office responsible for their management.

3.3.1.2. **Departmental Chief Information Security Officer /Alternate Information Security Officer** (CISO/ACISO)**:**

- Serves as the central point of contact for Departmental IT security and coordinates security plan requirements with departmental/facility/units and the system administrators within the office or facility.
- Establishes and maintains a list of all IT systems within their Department.
- Ensures that, for each identified system, an individual has been assigned responsibility for the security of that system.
- Ensures preparation of IT security plans, in the approved format, for all systems owned and operated by or on behalf of the Department of Administration.
- Reviews all facility IT security plans. Comments on form or content will be sent to the originator for corrective action. /ACISO maintains a copy of the corrected plans.

- Maintains a tracking system for security plans to ensure plan completion, identification and correction of action items, and incorporation and documentation of changes to the system or environment into the plan.
- Ensures that system administrators review and update all plans annually.
- Works with all affected areas and appropriate staff in the preparation of a departments/facility/Unit IT Security Plan in the approved Division of Information Technology format for each individual system identified,
- Works with the appropriate staff to complete an action plan that identifies system vulnerabilities and establishes dates to complete necessary corrections.
- Ensures that all details of the official security plan are communicated to all individuals with a need-to-know.
- Ensures that all staff has a current copy of the department's official security plan and that all copies are securely stored.
- Updates the plan annually to incorporate any changes to the system status. Roll over any action items not completed from previous plans and forward to the CSO for review.
- Determines responsibility to define system boundaries and determine sensitivity levels.

4. RISK MANAGEMENT

4.1. PURPOSE

4.1.1. This chapter provides the Departments of the State of Rhode Island with policy and procedures necessary to establish and maintain a Risk Management Program. The program applies to all IT resources and helps to ensure the balance of risks, vulnerabilities, threats and countermeasures to achieve an acceptable risk level based on the sensitivity or criticality of the individual systems.

4.1.2. The policy includes all State of Rhode Island IT systems and resources and is mandatory for all organizational units, staff, contractors, and others having access to these resources, or operating on them in behalf of the State

4.1.3. This policy applies to all existing Information Technologies and any new systems acquired after the effective date of this policy.

4.2. BACKGROUND

4.2.1. Risk management is the total process of identifying, controlling, and eliminating or reducing risks that may affect all State of Rhode Island IT resources. It includes:

- Risk analysis;
- Determination of the appropriate levels of resources necessary to protect the IT;
- Management decisions to implement selected IT security safeguards based on the risk analysis, including accepting residual risk, if necessary; and
- Effectiveness reviews.

4.2.2. While formal risk analyses need not be performed, the need to determine adequate security requires that a risk-based approach be used. This risk analysis approach should include a consideration of the major factors in risk management and the effectiveness of current or proposed safeguards.

4.3. POLICY

4.3.1. The Department of Administration, Division of Information Technology, Director, IT Operations, will direct the DoIT Chief Security Officer, to establish and maintain, with all departmental CISOs, a program for conducting periodic risk analyses to ensure that appropriate, cost-effective safeguards are incorporated into existing and new installations of Information Technologies.

4.3.2. The CISO will conduct two general types of risk analyses, one for the overall department, and another for each IT resource operated by, or on behalf of the department.

4.3.3. The initial risk assessment is a measure of risks before they are corrected. Only residual risks should be considered during DoIT's CSO certification and accreditation of the system.

4.3.4. It is recommended that a team concept be utilized in completing risk analyses. Perform risk analyses:

- Prior to the approval of design specifications for new facilities and before the acquisition of new Information Technologies;
- Whenever there is a significant change to the facility or its Information Systems;
- On each system identified by the department; and
- Once every year, at a minimum.

4.3.5. The results of the individual system risk analysis and the office risk analysis must be policy.

4.3.6. The assessment team evaluates the results from these assessments and immediate action will be taken to reduce identified deficiencies. Those deficiencies that cannot be immediately reduced, the team shall provide suggested alternatives that must be presented to management.

4.3.7. Not all risk can be avoided. Budget constraints, staffing limitations, and cost-benefit considerations (controls can cost more than potential losses) may result in the acceptance of certain existing risks.

4.3.8. The Department Director must correct, or accept as uncontrolled risk, vulnerabilities found during any analysis. If the decision is to accept a risk, this decision must be policy as an uncontrolled risk and signed by the Departments Director. The DoIT Chief Security Officer will maintain this document and the risk analysis report and make them available for review by authorized reviewing organizations upon request (such as the Auditor General & Risk Management).

4.3.9. Consider all risk analysis reports sensitive documents, and therefore, label, handle and secure them appropriately.

4.4. RESPONSIBILITIES

4.4.1. **DoIT Chief Security Officer** must ensure that all Departments establish and maintain an effective risk management program.

4.4.2. **Department Director:**

- Ensure that a risk analysis and system risk analyses are performed and policy at least every year; and
- Ensure that vulnerabilities and risks found during any analysis are corrected, reduced to an acceptable level or accepted as uncontrolled risks.

4.4.3. **Facility, Unit, Section System Administrators** are responsible for ensuring that risk analyses are performed on all systems for which they have responsibility.

4.4.4. **Appropriate Office Information Security Officer (ISO):**

- Complete an office or unit IT risk analysis.
- Review the risk analyses for the office IT resources (both the office risk assessment and the system risk assessments) for completeness and assess the magnitude of the risks to the office or unit.
- Retain a copy of each system risk analysis.
- Develop a plan for correcting known vulnerabilities and risks identified from the system risk analyses.
- Document and forward recommendations to the departments CISO, copying the Department's Director and DoIT Chief Security Officer. The plans must include specific tasks, target dates for completion, and costs to implement, if applicable.

5. CONTINGENCY PLANS

5.1. PURPOSE

5.1.1. This chapter establishes requirements for business resumption and contingency planning within the Department of Administration. Each facility/unit office is responsible for the development, periodic testing and updating of a contingency plan for the section/unit/office and contingency plans for all IT resources within.

5.2. BACKGROUND

5.2.1. View Contingency Plans from two separate aspects:

- From the providers' perspective, individuals responsible for providing the resources necessary to conduct the office business need; and
- From the customers' viewpoint, individuals who must consider what to do until normal processing is restored.

5.2.2. The State of Rhode Island network is accessed for processing and storing information through the States wide area network (WAN), with departments having their own local area networks (LAN) that link the various personal computers and share various resources.

5.2.3. If a catastrophic event occurs that makes it impossible for the Department staff to use their respective LAN, the re-establishment of information systems and network functions is one part of the resumption plan. To restore both the information technology and the general office environment, consider the following interim processes:

- Hot sites (a reserved space already equipped with processing capability);
- Reciprocal agreements and arrangements with other agencies to provide restored capacity;
- Backup copies of critical files (critical data), previously processed on Local Area Network servers, required for continuing operations during the contingency period.

5.3. POLICY

5.3.1. All the State of Rhode Island IT systems require contingency plans. The contingency plan documents the specific methodology, structure, discipline, and procedures to be used for emergency response, backup operations, and post-disaster recovery. This planning ensures the availability of critical resources and facilitates the continuity of operations in an emergency situation.

5.3.2. **Department Directors** are responsible for the development and maintenance of contingency plans for these IT functions. The contingency planning process shall address the following activities:

- Backup and recovery of data and software;
- Emergency response actions to be taken to protect life and property and minimize the impact of the emergency;
- Selection of a backup or alternate operation strategy;
- Actions to be accomplished to initiate an effective recovery of business processes including a move to an alternate site, if necessary;
- Resumption of normal operations in the most efficient and cost effective manner.

5.3.3. All department offices develop and maintain current contingency plans for IT systems addressing disaster recovery that provide assurance that critical data processing support, based on the results of a thorough risk analysis, can be continued or resumed in a reasonable time frame. These plans include adequate coverage as described below.

- Emergency procedures in response to natural or manmade disasters (fire, flood, riot civil disorder, natural disaster, bomb threat, terrorist incident or any other activity which may endanger lives, property or the capability to perform essential functions) will be defined in the appropriate Emergency Preparedness Plan. Prominently display these emergency procedures in the areas to which they apply.
- Define and document arrangements, procedures and responsibilities to ensure that essential (critical) operations can be continued if normal processing or data communications are interrupted.
- Establish and document recovery procedures and responsibilities to facilitate the rapid restoration of normal operations at the primary site, or if necessary, at an alternate processing site.
- Identify and prioritize the minimally acceptable level of degraded operation of the essential (critical) systems or functions to guide implementation of recovery operations.

5.4. PROCEDURES

5.4.1. The following procedures outline the steps to be followed in the development and implementation of an effective IT contingency plan for all departments.

5.4.1.1. **Identify and Coordinate Mission-Critical Functions**. Identify and prioritize mission-critical functions in order of importance. Coordinate plans designed to continue essential missions and functions and appreciate the dependent nature of this process.

5.4.1.2. **Identify the Resources that Support Critical Functions**. Included in this analysis are the time frames when each resource will be needed and the effect on the mission if the resource is not available. One method used to identify mission-critical functions and their impact is called Business Impact Analysis. It includes the following reviews:

- Identify functions to understand the impact if they are not performed. A review is done of each function regarding its impact on operations, end users, interrelationships with other critical functions, as well as workload peaks and valleys;
- Additional expenses caused by overtime, the need for temporary employees, and other miscellaneous costs associated with recovery; and
- Inability to perform the facility's mission-critical functions. This needs to be evaluated and considered with regard to the impact within the organization.

Anticipating Potential Disasters. All resources associated with critical functions should be examined with likely problem scenarios. Form a department contingency planning team, and include representatives from three main areas: functional/business groups, facilities management, and technology management. Team members should also include staff from DoIT, system administrator, CISO/ACISO and other employees from financial management, personnel, and physical security. Assign legal advisors and other specialty groups to the team as needed.

5.4.1.3. **Selecting Business Resumption and Contingency Planning Strategies.** The primary purpose of this step is to plan how to restore needed resources. Consider alternative strategies and evaluate each for those controls necessary to prevent or minimize the disaster. A contingency planning strategy consists of three parts:

- Emergency response, the initial actions taken to protect lives and limit damage;
- Recovery, the steps that are taken to continue support for IT critical functions;
- Resumption, the return to normal IT operations. The relationship between recovery and resumption is important. The longer it takes to resume normal operations, the longer the department will be required to operate in the recovery mode.

5.4.1.4. **Strategy Selection** Base the selection of a strategy on practical considerations such as feasibility and cost. Risk analysis can be used to help estimate the cost of options to decide on an optimal strategy. The risk analysis should focus on areas where it is not clear which strategy is the best. Ask following questions as part of the risk analysis:

- Is it more expensive to purchase and maintain a generator or to move processing to an alternate site, considering the likelihood of losing electrical power for various lengths of time?
- Are the consequences of losing computer-related resources sufficiently high to warrant the cost of various recovery strategies?
- What categories of resources should each be considered? Some of these resources include human resources, processing capability, automated applications and data, computer-based systems, physical infrastructure, documents and papers.

5.4.1.5. **Implementation:** Contingency planning, preparation, implementation, and procedures depend on the department's IT configuration (e.g., number of systems) and overall criticality and inter-relationships of systems being analyzed. Three of the most important issues are:

- How many plans are required. The number of actual plans needed depends upon the unique circumstances for each organization;
- Who prepares each plan. For small or less complex systems, the contingency plan may be incorporated into the computer security plan for that system. For larger complex systems, the computer security plan would contain a brief synopsis of the contingency plan. The contingency plan would be a separate document.; and
- Who executes the plan. At this point, coordination and cooperation between resource managers and functional managers is critical for success in implementing the plan.

5.4.1.6. Examples of preparations for implementing contingency plans include:

- Establish procedures for backing up files and applications and testing the backups on a regular basis;
- Establish contracts and agreements if the contingency strategy calls for them, re-negotiating existing contracts if necessary to reflect any changes;
- Purchase equipment to support a redundant capability. Maintain and periodically replace this equipment when no longer dependable or obsolete to an organization's architecture;
- Keep preparations, including documentation, up-to-date.

- Formally designate people who are responsible for various tasks in the event of a contingency. These people are often referred to as the contingency response team, which is often composed of members of the contingency planning team.

5.4.1.7. **Documentation:** Document and update the contingency plan regularly. A written plan is essential. It should clearly state, in simple language, the sequence of tasks to be performed in the event of an incident to enable someone with minimal knowledge to begin to execute the plan immediately. Store updated, electronic and printed copies of the contingency plan in several secure locations, such as alternate processing sites and secure off-site storage facilities. Members of the contingency plan response team must have 24-hour access to a copy of the plan.

5.4.1.8. **Contingency Plans** must include thoroughly policy procedures for restoring resources or for providing alternate processing. Remember that the system administrator may not be available during the disaster. Detailed, policy procedures that are readily available shorten recovery time and conserve resources.

5.4.1.9. **Training:** All Department personnel must be trained in, and continually practice and up-date, their contingency-related duties. New personnel must be trained as they join the organization. In an emergency there may be inadequate time to check a manual to determine correct procedures, and continuous training and practice promotes effective employee response during emergencies.

5.4.1.10. **Testing and Revising**

- Test the contingency plan yearly to identify and correct any problems in planning or implementation;
- Assign responsibility for keeping the contingency plan current; and
- Include reviews, analyses, and simulations of disasters.
- Use the results of contingency planning to improve the plan and detect and correct flaws.

5.4.1.11. **Review:** A review can be a simple test to check the accuracy of contingency plan documentation. The review will:

- Confirm that individuals listed are still in the organization;
- Confirm that individuals have the responsibilities that caused them to be included in the plan;
- Check home and work telephone numbers, organizational codes, and building and room numbers;
- Determine if files can be restored from backup tapes; and
- Confirm that employees know emergency procedures.

5.4.1.12. **Analysis:** An analysis may be performed on the entire plan or portions of it, such as emergency response procedures. The individual conducting the analysis should:

- By a staff member who did not participate in the development of the contingency plan but has a sound knowledge of the critical functions and supporting resources;
- Interview functional managers, resource managers, and their staff to uncover missing or unworkable sections of the plan.

5.4.1.13. **Simulations:** Disaster simulations provide information about flaws in the contingency plan and provide practice for a real emergency. These tests provide critical information that can be used to ensure the continuity of important functions. In general, the more critical the functions and the resources addressed in the contingency plan, the more cost-beneficial it is to perform a disaster simulation.

5.4.1.14. **Interdependencies**: Controls that support and compliment each other can prevent or reduce the effects of a disaster by lessening or eliminating the damage occurring as a result of the destruction, disclosure, or denial of critical resources. These controls include:

1. Risk analysis:
    - Analyzes vulnerabilities;
    - Weighs the benefits of various contingency-planning options; and
    - Identifies critical resources needed to support the organization and the local threats to those resources.
2. Physical, environmental, and logical access controls:
    - Help prevent the destruction of Information Technologies.
    - Address the most common threats: theft, unauthorized access, fires, loss of power, plumbing failures, and natural disasters.
3. ***Incident handling***, a subset of contingency planning, is the emergency response provided by a facility or organization to provide immediate assistance against active IT threats. A good incident response capability will:
    - Prevent incidents by incorporating preventive measures that guard against similar incidents;
    - Educate users about the incident, the circumstances, and the corrective action taken or needed. Examples of where incident response would be needed include a virus attack and a telephone social engineering attack. The first, a virus attack would require a technical solution to inoculate

systems against the virus and the second, a telephone social engineering attack, would depend more heavily on employee awareness of the issue.

4. IT Support and operations controls include:
   - ➢ Periodic backing up of critical files;
   - ➢ Prevention and recovery from more common contingencies, such as a disk failure or corrupted data files.
5. Policy creates and documents the organization's approach to contingency planning and assigns explicit responsibilities.

5.5. RESPONSIBILITIES

5.5.1. **<u>Department Director;</u>** ensures that all offices have business resumption and contingency plans for all IT resources.

5.5.2. **<u>Department IT Manager</u>**:

- Ensure the development, periodic testing and updating of contingency plans for all IT resources located at that office or facility.
- Ensure the establishment of a contingency planning team with representation from three main areas: functional/business groups, facilities management, and technology management.
- Identify all mission-critical systems and applications utilized by the office or facility.
- Ensure that all sensitive automated information required and controlled by the office or facility is adequately backed up and stored in a secure and readily available location.
- Notify the CISO of scheduled contingency tests and forward documentation of the results to the CISO after testing.
- Designate, in writing, an individual(s) to serve as the <u>Contingency Plan Project Coordinator</u> for the system and ensure this information is forwarded to the office or unit CISO.

5.5.3. ISO/AISO designated as the office IT <u>Contingency Plan Project Leader</u>:

- Provides guidance and coordination of the office IT contingency planning efforts;
- Defines requirements to develop and test system level contingency plans to ensure they align with the overall facility IT security policy and contingency plan;
- Develops plans and schedules for implementing the office IT contingency planning policy;

- Develops a planning methodology to ensure quality, consistency, and comprehensiveness of the completed contingency plans.
- Maintains a current listing of all IT Contingency Plan Project Coordinators and system administrators within the office.
- Provides training and support to the contingency planning team, and to the individuals appointed to develop and coordinate contingency plans.
- Monitors the contingency planning process and is prepared to report the progress to management as required.
- Establishes test schedules, monitors the tests, and evaluates the results.
- Reports the results of all IT contingency plan tests and critiques of their effectiveness to office management annually.
- Participates as a member of the Emergency Preparedness Committee or its equivalent.
- Evaluates all levels of contingency plans, determines the level of backup support, and identifies and prioritizes critical applications that will be supported. For example, based on these evaluations, it may be necessary to suspend non-critical applications until normal operations are restored.
- Maintains current copies of all contingency plans, tests, evaluations, and subsequent follow-up actions and makes this information available to external audit teams, as required.

5.5.4. <u>**Contingency Plan Project Coordinator**</u>:

- Develops and maintains the contingency plan(s) for the system, outlining the procedures for protection and recovery of physical files, personnel, and office equipment and manual procedures to be used in the event that IT systems are disrupted for an extended period of time.
- Coordinates with the CISO and State to ensure the plan is consistent with the overall disaster recovery plan.
- Communicates the plan to all users within the office.
- Clearly defines and communicates individual personnel, responsibilities, and authorities.
- Schedules and document tests of the system’s contingency plan and critiques their effectiveness.
- Coordinate the activation of the system’s contingency plan during an emergency.

5.5.5. **Departmental IT Manager/System Administrator**:

- Develop a comprehensive contingency plan to address adverse events that could impact Information Technology assets or State's/IT Units' ability to provide assistance to end users. This plan also addresses incident handling procedures. A boilerplate DoIT Contingency Plan is available on the CIO Information Security web site.
- Create and securely store copies of systems, utilities/support, and applications software, data files, and associated documentation for use in facility-wide backup and recovery operations. Store backups in an area that is secure and available to all key staff during an emergency.
- Evaluate all contingency plans and determine the level of backup support needed, and identify and prioritize those critical applications that you support.
- Evaluate the need to suspend applications or subsets of applications that are not Mission critical until normal operations are restored.
- Develop a strategy for providing adequate alternate processing capability based on the prioritization of critical applications identified within each. Strategies address support functions including transportation, telecommunications, and recovery operations (for example, cleaning companies specializing in electronic equipment, media recovery specialists, and equipment and protective device manufacturers).
- Maintain a list of the IT personnel involved in the disaster planning/recovery process. The roster provides adequate information to contact personnel both during scheduled work hours and during off-shift hours. It is critical that the roster of personnel be updated as personnel, addresses, telephone numbers, and responsibilities change.
- Maintain a current configuration diagram for all systems, networks, and telecommunications components.
- Communicate the plan to all users and units that will be affected by the plan(s). Clearly define and communicate individual personnel and their responsibilities and authority.
- Activate and coordinate established contingency plans during an emergency.

6. CERTIFICATION

6.1. PURPOSE

6.1.1. This chapter establishes the State of Rhode Island IT security policy for certification of all sensitive IT resources. Sensitive IT resources include both systems and applications that require some degree of protection for confidentiality, integrity or availability. This includes systems and data whose improper use or disclosure could adversely affect the ability of an office or unit to accomplish its Mission, proprietary data, Health Data, records about individuals requiring protection under the Privacy Act, HIPAA Regulation, and data not releasable under the Freedom of Information Act. The policy contained in this chapter covers all the State of Rhode Island IT resources, whether maintained in-house or in the interest of the State of Rhode Island. *NOTE: If the* system *or application is required for accomplishment of a departments* ***Mission*** *it is considered sensitive.*

6.1.2. Certification is a requirement for all IT resources. Existing IT, new IT resources and those not fully operational must complete all certification requirements and be accredited prior to full implementation.

6.2. BACKGROUND

6.2.1. Certification is a requirement of the Department of Administration, Division of Information Technology.

6.2.2. Certification testing requires a thorough technical evaluation that determines if all security requirements are met, including all applicable Department, State and Federal regulations, and standards. The results of tests will demonstrate that the installed security safeguards are adequate and appropriate for the system or application being tested. The certification process is the final step leading to DoIT accreditation (authorization for processing). Accreditation policy and procedures are included in a separate chapter of this Policy.

6.2.3. Certification of the system/application is based on the policy results of the design reviews, system tests, and the recommendations of the testing teams. All systems/applications must include security controls that reflect the true importance of the information processed and/or the government investment embodied in the components of the IT resource.

6.3. POLICY

6.3.1. Conduct certification evaluations on all IT resources owned or operated on behalf of the State of Rhode Island.

6.3.2. DoIT Applications Development Group certifies software; DoIT Operations Group certifies hardware, before releasing it to the field. Modifications made to the software at the Department, Unit and/or section level will require re-certification at the site making the modifications.

6.3.3. **Initial Certification:**

- Prior to accreditation, each IT resource is to undergo appropriate technical certification evaluations to ensure that it meets all Federal, State, DoIT policies, regulations and standards.
- All installed security safeguards are functioning properly and are appropriate for the protection requirements of the system/application. Certification of the system/application is based on the policy results of the design reviews (if available), system tests and the recommendations of the testing teams.
- All systems/applications must include security controls that reflect the true importance of the information processed on the system.

6.3.4. **Interim Certification:**

- The certification process must be flexible enough that it accommodates the need for operational efficiency, as well as adequate protection of the system.
- In a situation where the need for a system is sufficiently critical that it must be in operation before a full certification is possible, the DoIT Certifying Official can provisionally certify the system/application, documenting necessary restrictions, pending specific actions to be completed in a predefined time frame.
- This interim certification cannot exceed one year.
- These actions should also be included as milestones in the security plan for the system.

6.3.5. **Re-certification**: Systems/applications will be re-certified when:

- Changes in requirements result in the need to process data of a higher sensitivity.
- After the occurrence of a serious security violation, which raises questions about the validity of an earlier certification.
- No less frequently than three years after the previous certification.
- Substantial changes are made to the system. Examples of major changes include:
  - ➢ Changes in the system or software applications. These are substantial changes that alter the Mission, operating environment or basic vulnerabilities of the system. Examples are increases or decreases in hardware, application programs, or external users; hardware upgrades; addition of

telecommunications capability; dial-in lines; changes to program logic of application systems; or relocation of system to new physical environment or new organization.

  - ➢ Minor changes such as replacement of similar hardware when capacity does not significantly change, addition of two or three workstations on a network or small modifications to an application program (e.g., table headings are changed) would not require re-certification.

- Changes in protection requirements. These are changes in the sensitivity level of the data being processed, increase in the Mission criticality of the system or changes in Federal or the State policies.
- Occurrence of a significant security violation. These are violations or incidents that call into question the adequacy of the system security controls.
- Audit or evaluation findings. These are findings from any security review that identify significant unprotected risks. Such findings could include the system certification review, physical or information security inspection, internal control reviews, and external audits.
- Certification documentation for sensitive systems will be marked “For Official Use Only.” Sensitive systems are those in which the information included in the certification documentation contains details about the system that may identify weaknesses or vulnerabilities and requires protection against disclosure to persons without the need to know.

6.3.6. A Certification Review Team, established to conduct the technical evaluation of the system/application, obtains input from all who have been involved with the system/application, including: CISO, System Administrator, software development staff, the computer network operations staff, and users.

6.3.7. **Certification Testing of Security Controls:**

- The technical certification evaluation results are the basis for the system administrator’s certification statement in the accreditation request. The certification document should state what methods were used to perform the certification evaluation.
- The first step in the certification process is to determine what the protection requirements for the IT resource should be which are based on the sensitivity or criticality of the individual system/application.
- Once these requirements are defined, select and implement cost-effective controls to provide adequate protection to achieve an acceptable level of risk.
- The goal of the technical certification evaluation is to test existing controls to determine: (1) if controls function properly; (2) if controls satisfy performance criteria

and provide for availability, survivability and accuracy; and (3) if the controls can be easily defeated or circumvented.

6.3.8. The technical certification evaluation can be accomplished by two or more of the following:

- Evaluation and Testing. Security controls installed and implemented require testing to ensure they meet the defined security requirements for the system and they function as expected. System administrators should maintain documented results of these tests to be used as part of the certification review. In addition to specific tests of individual controls, evaluation of the overall system may also be performed. These evaluations may take the form of checklists or other methods that ensure consideration has been given to all security requirements and controls. Copies of evaluation results should be included in the certification documentation for the accreditation package.
- Other Internal Reviews. The results of any security related reviews performed by evaluation teams internal to the facility may be used as part of the certification evaluation. These reviews may include internal control reviews, physical or information security inspections, or CISO security reviews. Test and document corrective actions. Copies of review findings and corrective actions taken should be included in the certification documentation for the accreditation package.
- External Reviews. The results of any audits performed by independent external organizations may also be used as part of the certification evaluation. The Bureau of Audits or other audit groups may have performed these audits or reviews. Implementation of any corrective actions taken as a result of these audit findings should be tested and policy. Include copies of audit findings and corrective actions taken in the certification documentation for the accreditation package.
- Risk Analysis. Risk analysis can play a dual role in the evaluation process. It can be used to help determine important security requirements for the IT resource and to evaluate the existing and planned controls for cost-effective risk reduction. Since risk analysis must be performed throughout the life cycle of the system, it provides a method for reassessing the risks against system changes and determining additional controls required establishing an acceptable level of risk for the system/application.

6.4. PROCEDURES

6.4.1. Assemble a team.

- Assemble a team to gather the information and documentation needed to assess and demonstrate the adequacy of security measures used;
- Include representatives of IT security, application owners, software development staff if necessary, system administrators, computer support staff, and users. The DoIT

security staff provides an outside viewpoint to ensure that the best IT security practices are used in protecting sensitive systems.

6.4.2. Collect existing documents needed for the certification evaluation. These documents include, but are not limited to:

- System specifications and documentation
- System security plan
- Risk analysis
- Contingency and disaster recovery plans
- Staff records on personnel and the IT Security identification, training and position sensitivity levels
- Internal Control Reviews, security reviews, etc., if existing

6.4.3. Identify and describe the system/application to be certified and describe why it is sensitive.

- Create a written description of the purpose of the system;
- Include the hardware and software environment on which the system is operated; and
- Include a description of the sensitivity of the system, including any special applicable laws and regulations. This information is readily available in the Sensitive System Security Plan for the system being certified.
- If the certification is for a software application system that will be used by others, the hardware description should address the hardware needed to operate the system: however
- Focus the certification on the software application program.

6.4.4. Identify protection requirements and vulnerabilities.

- Review the description of the protection requirements for the system under the headings confidentiality, integrity, and availability in the Sensitive System Security Plan.
- Identify vulnerabilities for the system related to these protection requirements. Most vulnerabilities will be addressed in the existing documents collected in Step 2
- Ensure that all sensitive systems have a completed risk analysis. The risk analysis will identify vulnerabilities and their consequences, such as unauthorized disclosure of information, loss of data or other resources, denial of service, decisions based on erroneous information, etc. System documentation is another source of information

about the vulnerabilities. The security plan for the system being evaluated contains information about specific vulnerabilities and control measures addressed.

- Review any existing Internal Control, Bureau of Audits or security audit reports on the system, for additional information on system vulnerabilities.
- Interview managers in the user organization to ascertain their concerns about the sensitivity of the system and the level of protection required.

6.4.5. Identify security features needed.

- Review existing documents to identify the controls in place to address the vulnerabilities identified above. The risk analysis, security plans, and system documentation reviewed for vulnerabilities also contain information on controls used to reduce those vulnerabilities. System specifications, if they still exist, will also provide information on the controls designed into the system.
- Review the contingency and disaster recovery plans for the system. Staff training records will show the level of IT security training given to application and computer installation staff. Staff records should also show the sensitivity designation of staff positions and any personnel investigations, required and conducted, for staff in the affected positions.

6.4.6. Test adequacy of controls.

- Selectively check the adequacy of the controls once vulnerabilities and controls have been identified. Some live tests may be needed to ensure that identified controls actually work.
- Review other controls through other means. Previous system reviews and system acceptance tests may contain records of tests previously performed. It is not necessary to repeat these tests, if the system has not changed since they were done. The review of vulnerabilities and controls should identify any areas not adequately addressed.
- Use an Excel, DoIT Sensitive System Certification Worksheet to list the tests to be performed.
- Maintain a record of the results of the tests.

6.4.7. Evaluate the test results. The team will:

- Prepare a summary of the evaluation of the tests once all tests are completed. The team should then prepare recommendations about certification.
- Recommend certification with no further action required if the test results indicate that all protection requirements have been met.

6.4.8. If the Certification Review Team determines from the test results that the protection requirements were not met for the system:

- Explain the inadequacy of the controls in place in the evaluation discussion of test results.
- Alternatively certify that the basic protection requirements have been met, but recommend additional features be required. This latter form of certification is appropriate for certifying a software application system that must have certain operating system or hardware features in place for approved operation. This may also be used in recommending interim accreditation pending installation of some additional control not currently available.

6.4.9. **Certification:** The CIO or his designee signs the official Certification document.

6.4.10. If the need for a system is such that it must be put into operation before a full certification is possible:

- The Certifying Official can provisionally certify the system for operation, possibly with some restrictions, pending specific actions to be completed in a predefined time frame.
- This interim certification cannot exceed one year.
- These actions should also be included as milestones in the security plan for the system. The certification process must be flexible enough that it accommodates the need for operational efficiency as well as adequate protection of the system.

6.4.11. A Certification Guideline with the corresponding worksheets for certifying systems is available on the State's Information Security web site.

6.5. RESPONSIBILITIES

6.5.1. **Department Director** ensures that all systems within his area of control have been certified.

6.5.2. **Department IT Manager**: ensures that all systems operated at or on behalf of the department unit, section or commission are certified.

6.5.3. The **Chief Information Security Officer** will:

- Assemble the certification teams as required.
- Review the certification team's certification documentation and recommendation for each identified system/application.
- Sign the official certification statement for each system within the department.

6.5.4. **<u>Certification Team</u>** will:

- Perform all actions required for the certification review as outlined in the Process section of this chapter.
- Complete and sign the Evaluation and Recommendation certification document.
- Forward the certification document to the Agency Manager for review and final approval.

6.5.5. **<u>System Administrators</u>** will:

- Collect/prepare the necessary documentation required for system certification as described in this chapter.
- Participate in the certification process as a team member, as appropriate.
- Maintain the certification documentation of the system they manage.
- Include the certification evaluation in the accreditation package for the Director.

6.5.6. **<u>CISO/ACISO</u>** will:

- Ensure that system administrators are provided with information concerning the certification and accreditation of systems.
- Assist the system administrators in preparing and collecting the necessary documentation required for a system certification.
- Participate as a team member in the certification process.
- Maintain a copy of the certification documentation of each system.
- Ensure that the certification evaluation and recommendation document is included in the accreditation package for the Director's review.

7. ACCREDITATION

7.1. PURPOSE

7.1.1. This chapter establishes the State of Rhode Island's policy for accreditation of IT resources. The policy contained in this chapter covers all the State IT resources maintained in-house or in the interest of the State.

7.1.2. Accreditation is required for all the State of Rhode Island IT resources processing sensitive data. New IT resources or those not fully operational must complete all requirements and be accredited prior to full implementation.

7.2. BACKGROUND

7.2.1. Accreditation is a requirement of Department of Administration.

7.2.2. Accreditation or "authorization for processing" is the authorization and approval, granted to an IT resource to process, as an acceptable risk, in an operational environment. The term accreditation describes the process whereby information pertaining to the security of a system is developed, analyzed and submitted for approval to the appropriate senior management official.

7.2.3. The accreditation documentation includes a copy of the system security plan, risk analysis, contingency plan, security tests and results, and any residual risks known about the system.

7.2.4. The accreditation documentation provides the approving official with a clear understanding of a system's operational readiness and plans to correct any deficiencies noted. It should close by making specific recommendations for full, partial or denial of system accreditation.

7.3. POLICY

This policy defines the final step in the State of Rhode Island's IT security management process that ensures protection of the vital IT resources within the State.

7.3.1. **Initial Accreditation**

- All the State IT resources processing sensitive data will be accredited.
- The Office Head (approving official) will review the accreditation support documentation and will either concur, thereby declaring that a satisfactory level of

operational security is present or not concur, indicating that the level of risk has not been adequately defined or reduced to an acceptable level for operational requirements.

- The approving official must sign a formal accreditation statement declaring that the system appears to be operating at an acceptable level of risk, or defining any conditions or constraints that are required for appropriate system protection

7.3.2. Interim Accreditation

- Interim authority to operate can be granted, by the CIO, for a fixed period of time not to exceed one year. This authority is based on an approved security plan and is contingent on certain conditions being met. The interim authority to operate, while continuing the accreditation process, permits the IT resource to meet its operational Mission requirements while improving its security posture. If the approving official is not satisfied that the IT resource is protected at an acceptable level of risk, an interim accreditation can be granted to allow time for implementation of additional controls.
- An IT system administrator or the department CISO may make a recommendation or request for an interim accreditation.
- Interim authority to operate is not a waiver of the requirement for accreditation.
- The IT resource must meet all requirements and be fully accredited by the interim accreditation expiration date.

7.3.3. Re-accreditation

- Systems will be re-accredited when major changes occur to the system or every three years, whichever occurs first. Examples of major changes include:
- Changes in the system or software applications – Substantial changes that alter the Mission, operating environment or basic vulnerabilities of the system. Major changes include an increase or decrease in hardware, application programs, external users, hardware upgrades, addition of telecommunications capability, dial-in lines, changes to program logic of application systems, relocation of system to new physical environment or new organization. Minor changes such as, replacement of similar hardware when capacity does not significantly change, addition of two or three workstations on a network or small modifications to an application program (e.g., table headings are changed) would not require re-accreditation.
- Changes in protection requirements – Changes in the sensitivity level of the data being processed, increase in the Mission-criticality of the system or changes in Federal or State regulations.
- Occurrence of a significant violation – A violation or incident that questions the adequacy of the system security controls.

- Audit or evaluation findings – Findings from any security review that identify significant unprotected risks. These could include the system security verification review, physical or information security inspection, internal control reviews, Bureau of Audits and the DoIT Security Audits.

7.3.4. The information included in the accreditation package contains details about the system. These details may identify weaknesses or vulnerabilities that require protection against disclosure to persons without the need to know. Accreditation documentation for sensitive systems must be secured and marked, “For Official Use Only.”

7.4. PROCEDURES

7.4.1. The following documentation for each IT resource will be prepared and submitted in the accreditation package to the appropriate approving official (Unit, Section or Office Head or designee):

- Request for Accreditation. A written request that includes a certification statement that the IT resource has undergone adequate tests to ensure that it meets all State, Federal and the DoIT policies, regulations and standards and that all installed security safeguards appear to be adequate and appropriate for the sensitivity of the system.

- Approved IT Security Plan. The purpose of the system security plan is to provide a basic overview of the security and privacy requirements of the subject system and the IT resource owner’s plan for meeting those requirements. The plan may also be viewed as documentation of the structured process of planning adequate, cost-effective security protection for the system. Details about completing these plans are presented in Chapter 3. “Security Plans” of this document.

- Completed Risk Analysis. IT resource managers are responsible for having a risk analysis conducted for each IT resource to ensure that appropriate, cost effective safeguards are incorporated into existing and new systems. See Chapter 4. “Risk Management” of this Policy for guidance on performing the required risk analysis.

- Contingency/Disaster Recovery Plans. Each IT resource develops and maintains a contingency and disaster recovery plan which provides reasonable assurance that critical data processing can be continued, or resumed quickly, if normal operations are interrupted. Policy concerning contingency/disaster recovery planning is contained in Chapter 5, “Contingency/Disaster Recovery” of this Policy.

- Certification Evaluation and Recommendation. Prior to accreditation, each IT resource undergoes appropriate technical evaluations to ensure that it meets all Federal and the State policies, regulations and standards and that all installed security safeguards are functioning as designed and appropriate for the sensitivity of the data stored on the system. Chapter 6. “Certification” of this policy outlines the methodology for conducting certification testing.

7.5. RESPONSIBILITIES

7.5.1. **<u>CISO:</u>** ensures that all systems within the Department have been accredited.

7.5.2. **<u>Unit, Section and/or Office Managers:</u>**

- Ensure that all IT resources within their office or facility are officially accredited.
- Make the official accreditation decision based on review of the accreditation documentation presented to them and the recommendations of Agency Manager and the CISO.

7.5.3. **<u>Department IT Manager</u>** will:

- Review the accreditation package submitted to them by the system administrator.
- Make a recommendation to the Director for or against accreditation based on the documentation, the risks, the results of the certification, and the advice of the CISO.
- Submit the accreditation package to the Director for signature and forwarding to the DoIT Chief Information Officer.

7.5.4. **<u>System Administrators</u>** will:

- Complete, with the assistance of the CISO, an accreditation package.
- Take the corrective actions necessary to accredit the system if the system receives a partial accreditation or accreditation is disapproved.
- Maintains a copy of the accreditation package and ensures that the CISO has a current and complete accreditation package.
- Takes the necessary actions outlined in this policy to re-accredit the system if major changes are made to the system or at a minimum every three years.

7.5.5. **<u>CISO</u>:**

- Acts as the central point of contact for accreditation of IT resources within the office or unit.
- With the assistance of the CIO and the Agency Director, ensures that the security controls in place meet all applicable Federal and the State policies, regulations, and standards for the particular IT resource.
- Recommends, as appropriate, to the Agency Manager regarding accreditation of the system based on the accreditation package submitted by the system administrator.

- Maintains a copy of the accreditation packages for all the IT resources operated on or on behalf of the facility.
- Ensures that each IT resource is re-accredited every three years or when there is a major change to the system that may affect the security of the system.

8. APPENDIX A

8.1. ACRONYMS

IT	Information Technology
ACISO	Alternate Information Security Officer
CSO	Chief Security Officer
FOIA	Freedom of Information Act
CISO	Information Security Officer
LAN	Local Area Network
NIST	National Institute of Standards and Technology
PBX	Private Branch Exchange

9. APPENDIX B

9.1. GLOSSARY

Access Control

Security control designed to permit authorized access to an IT system or application.

Accreditation

A formal declaration by the Office Head that the IT is approved to operate in a particular security mode using a prescribed set of safeguards. Accreditation is the official management authorization for operation of IT and is based on the certification process, as well as other management considerations. The accreditation statement affixes security responsibility with the Office Head and shows that due care has been taken for security.

Authentication

Verification of the identity of a user, user device, or other entity, or the integrity of data stored, transmitted, or otherwise exposed to unauthorized modification in an IT.

Audit Trail

A record showing who has accessed a computer system and what operations he or she has performed during a given period of time. Audit trails are useful both for maintaining security and for recovering lost transactions.

Automated Information System(s) (AIS)

An assembly of computer hardware, software and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information.

Availability of Data

The state when data are in the place needed by the user, at the time the user needs them, and in the form needed by the user.

Backup

A copy of data and/or applications contained in the IT stored on magnetic media outside of the IT to be used in the event IT data are lost.

Certification

The comprehensive evaluation of the technical and non-technical security features of an IT and other safeguards, made in support of the accreditation process, that establishes the extent to which a particular design and implementation meet a specified set of security requirements.

Ciphertext Form of cryptography in which the *plaintext* is made unintelligible to anyone, who intercepts it by a transformation of the information itself, based on some key.

Confidentiality The concept of holding sensitive data in confidence limited to an appropriate set of individuals or organizations.

Configuration Management The process of keeping track of changes to the system, if needed, approving them.

Contingency Plan A plan for emergency response, backup operations, and post-disaster recovery maintained by an activity as a part of its security program that will ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation.

COTS Software Commercial Off The Shelf Software – software acquired by government contract through a commercial vendor. This software is a standard product, not developed by a vendor for a particular government project.

Data Integrity The state that exists when automated data is the same as that in source documents, or has been correctly computed from source data, and has not been exposed to alteration or destruction.

Degaussing Media Method to magnetically erase data from magnetic tape.

Default A value or setting that a device or program automatically selects if you do not specify a substitute.

Dial-up The service whereby a computer terminal can use the telephone to initiate and effect communication with a computer.

Encryption The process of making information indecipherable to protect it from unauthorized viewing or use, especially during transmission or storage. Encryption is based on an algorithm and at least one key. Even if the algorithm is known, the information cannot be decrypted without the key(s).

Facsimile A document that has been sent, or is about to be sent, via a fax machine.

Firewall A system or cination of systems that enforces a boundary between two or more networks.

Friendly Termination The removal of an employee from the organization when there is no reason to believe that the termination is other than mutually acceptable.

Gateway A bridge between two networks.

Hardware Refers to objects that you can actually touch, like disks, disk drives, display screens, keyboards, printers, boards, and chips.

Identification The process that enables recognition of a user described to an IT.

Internet A global network connecting millions of computers. As of 1999, the Internet has more than 200 million users worldwide, and that number is growing rapidly.

Intranet A network based on TCP/IP protocols (an internet) belonging to an organization, usually a corporation, accessible only by the organization’s members, employees, or others with authorization. An intranet’s Web sites look and act just like any other Web sites, but the firewall surrounding an intranet fends off unauthorized access.

Intrusion Detection Pertaining to techniques, which attempt to detect intrusion into a computer or network by observation of actions, security logs, or audit data. Detection of break-ins or attempts either manually or via software expert systems that operate on logs or other information available on the network.

CISO/ACISO The persons responsible to the Office Head or Facility Director for ensuring that security is provided for and implemented throughout the life cycle of an IT from the beginning of the concept development plan through its design, development, operation, maintenance, and secure disposal.

Issue-specific Policy Policies developed to focus on areas of current relevance and concern to an office or facility. Both new technologies and the appearance of new threats often require the creation of issue-specific policies (e.g., e-mail, Internet usage).

IT Security Measures and controls that protect an IT against denial of and unauthorized (accidental or intentional) disclosure, modification, or destruction of ITs and data. IT security includes consideration of all hardware and/or software functions.

IT Security Policy The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.

IT Systems An assembly of computer hardware, software and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information.

LDAP Short for Lightweight Directory Access Protocol, a set of protocols for accessing information directories. LDAP is based on the standards contained within the X.500 standard, but is significantly simpler. And unlike X.500, LDAP supports TCP/IP, which is necessary for any type of Internet access.

Least Privilege The process of granting users only those accesses they need to perform their official duties.

Local Area Network A short-haul data communications systems that connects IT devices in a building or group of buildings within a few square miles, including (but not limited to) workstations, front end processors, controllers, switches, and gateways.

Management Controls Security methods that focus on the management of the computer security system and the management of risk for a system.

Modem An electronic device that allows a microcomputer or a computer terminal to be connected to another computer via a telephone line.

Network Two or more systems connected by a communications medium; a network is composed of a communications medium and all components attached to that medium whose responsibility is the transference of information.

Operating System The most important program that runs on a computer. Every general-purpose computer must have an operating system to run other programs. Operating systems perform basic tasks, such as recognizing input from the keyboard, sending output to the display screen, keeping track of files and directories on the disk, and controlling peripheral devices such as disk drives and printers.

Operation Controls Security methods that focus on mechanisms that primarily are implemented and executed by people (as opposed to systems).

Overwriting media Method for clearing data from magnetic media. Overwriting uses a program to write (1s, Os, or a cination) onto the media. Overwriting should not be confused with merely deleting the pointer to a file (which typically happens when a “delete” command is used).

Password Protected/private character string used to authenticate an identity or to authorize access to data.

Parity The quality of being either odd or even. The fact that all numbers have parity is commonly used in data communication to ensure the validity of data. This is called parity checking.

PBX Short for private branch exchange, a private telephone network used within an enterprise. Users of the PBX share a certain number of outside lines for making telephone calls external to the PBX.

Peripheral Device Any external device attached to a computer. Examples of peripherals include printers, disk drives, display monitors, keyboards, and mice.

Port An interface on a computer to which you can connect a device.

Port Protection Device A device that authorizes access to the port itself, often based on a separate authentication independent of the computer’s own access control functions.

RADIUS Short for Remote Authentication Dial-In User Service, an authentication and accounting system used by many Internet Service Providers (ISPs). When you dial in to the ISP you must enter your username and password. This information is passed to a RADIUS server, which checks that the information is correct, and then authorizes access to the ISP system.

Real Time Occurring immediately. Real time can refer to events simulated by a computer at the same speed that they would occur in real life.

Remote Access The hookup of a remote computing device via communication lines such as ordinary phone lines or wide area networks to access network applications and information

Risk The probability that a particular threat will exploit a particular vulnerability of the system.

Risk Analysis The process of identifying security risks, determining their magnitude, and identifying areas needing safeguards. Risk analysis is a part of risk management.

Risk Management Process of identifying, controlling, and eliminating or reducing risks that may affect IT resources.

Router An interconnection device that is similar to a bridge but serves packets or frames containing certain protocols. Routers link LANs at the network layer.

Rules of Behavior Rules established and implemented concerning use of, security in, and acceptable level of risk for the system. Rules will clearly delineate responsibilities and expected behavior of all individuals with access to the system. Rules should cover such matters as work at home, dial-in access, connection to the Internet, use of copyrighted works, unofficial use of Federal Government equipment, the assignment and limitation of system privileges, and individual accountability.

Security Incident An adverse event in a computer system or the threat of such an event occurring.

Security Plan document that details the security controls established and planned for a particular system.

Security A detailed description of the safeguards required to protect a

Specifications system.

Sensitive Data Any information, the loss, misuse, modification of, or unauthorized access to, could affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, U.S. Code, but has not been specifically authorized under criteria established by an Executive order or an act of Congress to be kept classified in the interest of national defense or foreign policy.

Separation of Duties A process that divides roles and responsibilities so that a single individual cannot subvert a critical process.

Server The control computer on a local area network that controls software access to workstations, printers, and other parts of the network.

Smart Card A credit-card-sized device with embedded microelectronics circuitry for storing information about an individual. This is not a key or token, as used in the remote access authentication process.

Software Computer instructions or data. Anything that can be stored electronically is software.

Software Copyright The right of the copyright owner to prohibit copying and/or issue permission for a customer to employ a particular computer program.

SPAM To crash a program by overrunning a fixed-site buffer with excessively large input data. Also, to cause a person or newsgroup to be flooded with irrelevant or inappropriate messages.

System Set of processes, communications, storage, and related resources that are under the same direct management control, have the same function or Mission objective, have essentially the same operating characteristics and security needs, and reside in the same general operating environment.

System Availability The state that exists when required automated information s can be performed within an acceptable time period even under adverse circumstances.

System Integrity The quality that a system has when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

System Administrator The individual responsible for defining the system's operating parameters, authorized functions, and security requirements. This individual is usually the person who maintains the system on a day-to-day basis.

System Owner The individual who is ultimately responsible for the function and security of the system.

TCP/IP Transmission Control Protocol/Internet Protocol. The Internet Protocol is based on this suite of protocols.

Technical Controls Security methods consisting of hardware and software controls used to provide automated protection to the system or applications. Technical controls operate within the technical system and applications.

Technical Security Policy Specific protection conditions and/or protection philosophy that express the boundaries and responsibilities of the IT product in supporting the information protection policy control objectives and countering expected threats.

Telecommunications Any transmission, emission, or reception of signals, writing, images, sound or other data by cable, telephone lines, radio, visual or any electromagnetic system.

Threat Any circumstance or event with the potential to cause harm to a system in the form of destruction, disclosure, modification of data, and/or denial thereof.

Trojan Horse Any program designed to do things that the user of the program did not intend to do, or that disguise its harmful intent. A program that installs itself while the user is making an authorized entry; and, then is used to break-in and exploits the system.

Unfriendly The removal of an employee under involuntary or adverse conditions. This may include termination for cause, RIF,

Termination involuntary transfer, resignation for "personality conflicts," and situations with pending grievances.

User Any person who is granted access privileges to a given IT.

User Interface The part of an application that the user works with. User interfaces can be text-driven, such as DOS, or graphical, such as Windows.

Virus A self-propagating Trojan horse (a program that surreptitiously exploits the security/integrity of a program), composed of a mission component, a trigger component, and a self-propagating component.

Vulnerability A weakness in automated system security procedures, technical controls, environmental controls, administrative controls, internal controls, etc., that could be used as an entry point to gain unauthorized access to information or disrupt critical processing.

Wide Area Network A physical or logical network that provides capabilities for a number of independent devices to communicate with each other over a common transmission-interconnected topology in geographic areas larger than those served by local area networks.

10. APPENDIX C

10.1. REFERENCES

POLICY#	STATUS	ISSUED	LAST REVISED	PAGE
10-06	Accepted	6/30/06	6/30/06	1 of 46

State of Rhode Island **Department of Administration** **Division of Information Technology**	TITLE	**IT Security Handbook** **Operational Controls**
	DRAFTED BY	Jim Berard

TABLE OF CONTENTS

1. PERSONNEL/USER SECURITY

1.1. PURPOSE AND SCOPE

1.1.1. This section provides policy and guidance on implementing minimum requirements concerning the staffing of positions that interact with all Information Technology (IT) System resources; the administration of users on a system, including considerations for terminating user access; and special considerations that may arise when contractors or other non-agency individuals have access to the Agency IT System resources.

1.1.2. The policy contained in this section is mandatory for all organizational units, employees, contractors, and others having access to and/or using the IT System resources of the Agency.

1.2. BACKGROUND

1.2.1. Many important issues in computer security involve users, designers, implementers, and managers. A broad range of security issues relates to how these individuals interact with computers and the access and authorities they need to do their job. No IT System can be secured without properly addressing these security issues.

1.2.2. DoIT security policy……. requires that each system establish a set of "Rules of Behavior". The security required by the rules is only as stringent as necessary to provide adequate security for the system and the information it contains.

1.3. POLICY

1.3.1. **Staffing:** The Agency's agency staffing process involves, at a minimum, the following steps which apply equally to all users of the Agency's IT System resources:

1.3.1.1. Position definition. Identify and address security issues early in the process of defining a position. Once a position has been broadly defined, the responsible supervisor determines the type of computer access needed for the position. There are two general security rules to apply when granting access:

- Separation of duties. **NOTE:** This phrase refers to dividing roles and responsibilities so that a single individual cannot subvert a critical function. For example, in financial systems, no single individual shall normally be given authority to issue checks. Rather, one person initiates a request for a payment and another authorizes that same payment.

- Least privilege. **NOTE:** This phrase refers to the security objective of granting users only those accesses they need to perform their official duties.

1.3.1.2. Determining position sensitivity:

- Supervisors, with assistance from the CISO and Human Resources Management analyze all positions, establish their sensitivity level designation, and document them with a Position Sensitivity Level Designation.
- The Office Head, or designee (e.g., Director, Human Resources Management), signs the appropriate form.

1.3.1.3. The following positions will be designated no lower than moderate risk:

- Office and unit CISO(s) and alternates
- Individuals having either programmer privileges or the ability to create and add users and/or menus to establish file access for IT System resources that process sensitive data

1.3.1.4. Position descriptions must be written or annotated to reflect specific security responsibilities and position sensitivity levels. Within this context, “specific security responsibilities” refer to employee obligations to protect sensitive data and to use such data and information derived from it only in the execution of official duties.

1.3.1.5. All other individuals with IT System resource access (e.g., contractors, volunteers) must meet the requirements of government employees performing similar duties.

1.3.1.6. Screening – Background screening helps determine whether a particular individual is suitable for a given position.

- The appropriate investigation will be requested by the office to ensure the screening of all individuals (including non-the Agency individuals, (e.g. contractors, volunteers, work-studies) before they are granted access to sensitive data or are allowed to participate in the design, operation or maintenance of sensitive information systems.
- The level of screening required varies from minimal checks to a full background investigation depending on the sensitivity of the information to be handled or the risk and magnitude of loss or harm that could be caused by the position.
- It is more effective to use separation of duties and least privilege to limit the sensitivity of the position, rather than relying on screening to reduce the risk to the organization.
- The Emergency Preparedness and Administration Security Office have issued a “Security and Risk Designation, Appendix A”, that establishes guidelines with regard to position sensitivity designation, risk levels and corresponding security investigation requirements.

1.3.1.7. Employee Training and Awareness

- Employees will be trained in the computer security responsibilities and duties associated with their jobs.
- For more training requirements, see Operations Handbook Section 3. “Education, Training, and Awareness”.

1.3.2. **User Administration:** The Agency agencies must ensure effective administration of users’ computer access to maintain system security, including user account management, auditing and the timely modification or removal of access.

1.3.2.1. User Account Management

- The Agency office management designates and records individuals authorized to issue access to IT System resources and data.
- The Agency Management, or their designee(s), sponsors user access for all users, including non Agency users and recommends access by the CIO. A written and signed request (electronic or paper form) for user access by management, or designee(s), constitutes management approval to initiate a request for access to any sensitive IT System resource. Management ensures that such requests meet the following criteria:
    - The request contains name, organization (or name of contracting company and contract number if applicable), location, purpose for access, and access requirements.
    - The individual must have an Agency need-to-know (i.e., access is an operational necessity) documented in the request.
    - The IT System security features have the capability to restrict the user’s access to only information and/or functions appropriate for the authorized activities.
- The office CISO or designee reviews all approved requests.
- Requests for access to remote systems and networks not under the agency management control (i.e., Automation Center) must be routed through the CISO prior to approval.
- Access requirements to information systems by auditors, consultants, representatives of hardware and software vendors, communication company employees, volunteers, work-study students, and other members of the general public must meet or exceed those requirements established for the Agency employees.
- Procedures will be established at the Agency agencies that require all users to sign an “Access Notice” (electronic or paper copy) before actual computer access is granted.

- The rules of behavior cited in Circular A-130, Appendix III clearly delineate responsibilities and expected behavior of all individuals with access to the system. The rules:
    - State the consequences of inconsistent behavior or noncompliance.
    - Should be in writing and form the basis for security awareness and training.
    - Will be available to every user prior to receiving authorization for access to the system.
    - Will be incorporated into the “access notice” for each system.
- Each agency will establish procedures for identifying, managing (adding and deleting users), recording, and monitoring who has access to sensitive IT System resources.
- The process of distribution of access codes will be controlled by the CISO and may be delegated to a designee.
- If access codes cannot be issued directly to users, a secure method for delivery will be established.

1.3.2.2. **Audit and Management Reviews:**

- The Agency IT offices ensure that user access and privileges are reviewed at least every 90 days for appropriate level of access/continued need.
- Reviews examine the levels of access of each individual, conformity with the concept of least privilege, whether all accounts are still active, whether management authorizations are up to date, and whether required training has been completed.

1.3.2.3. **Temporary Assignments, In-house Transfers, and Terminations:**

- Access authorizations are typically changed under two types of circumstances: (1) change in job role, either temporarily (e.g., while covering for an employee on sick leave or training a new employee) or permanently (e.g., in-house transfer) and (2) termination.
- Although necessary, temporary access authorizations should be granted sparingly and monitored carefully, consistent with the need to maintain separation of duties for internal control purposes. The access must be removed promptly when no longer required.
- Permanent changes are necessary when employees change positions within an organization. In this case, the process of granting account authorizations described earlier will occur again. The Agency offices must establish a procedure to ensure that access authorizations of the prior position be removed.

- Terminations of a user's system access generally can be characterized as either "friendly" or "unfriendly." Security issues must be addressed in both situations.
    - Friendly termination can occur when an employee is voluntarily transferred, resigns, or retires. Security issues must be addressed in all situations. Local "friendly" termination procedures will include:

        a. Removal of access privileges to all IT System resource accounts

        b. Control of keys

        c. Briefing on the continuing responsibilities for confidentiality and privacy

        d. Return of property

        e. Continued availability of data. In both the manual and the electronic worlds, this may involve documenting procedures or filing schemes, such as how documents are stored on the hard disk, and how are they backed up. Employees should be instructed whether or not to transfer important data from their PC to appropriate personnel before leaving. If cryptography is used to protect data, the availability of cryptographic keys to management personnel must be ensured.

    - Unfriendly termination may include situations when the user is being removed from duty or involuntarily transferred and there is a reasonable belief that IT System resources could be abused or misused. Local "unfriendly" termination procedures will include:

        a. Termination of system access at the same time (or just before) the employees are notified of their dismissal or upon receipt of resignation.

        b. When an employee notifies an organization of a resignation and it can be reasonably expected that it is on unfriendly terms, system access should be immediately terminated.

        c. If applicable, during the "notice of termination" period assign the individual to a restricted area and function. This may be particularly true for employees capable of changing programs or modifying the system or applications.

        d. In some cases, physical removal from the offices may be necessary.

1.4. RESPONSIBILITIES

1.4.1. **<u>The Agency IT Manager</u>** ensures that agencies within the network are in compliance with personnel security procedures as described in this section.

1.4.2. **<u>Office Heads, and Regional Agency Directors</u>**: ensure that ALL positions are assigned a proper sensitivity level designation based on information security criteria, such as computer related responsibilities, type of data to which the individual has access, a reasonable analysis of the risk, and principles of responsible management.

1.4.3. **<u>Senior Management/Human Resources</u>** analyze all positions, establish their sensitivity level designation, and document designation with a Position Sensitivity Level Designation. The Office Head or designee (e.g., Director, Human Resources) will sign the appropriate form.

1.4.4. **<u>Human Resources</u>**:

- Ensure that documentation for background investigations for identified positions are maintained in each employee's personnel file.
- Notify Agency CISO of all terminations and transfer of in-house employees.

1.4.5. **<u>Supervisor or designee(s)</u>**:

- Annually review the position description and performance standards with each employee occupying a position designated as sensitive.
- Discuss specific information security responsibilities with the employee.
- Discuss with the employee the consequences of noncompliance with those security responsibilities for the employee's particular position.
- Monitor temporary access authorizations and notify CISO when access should be terminated.

1.4.6. **<u>The Agency Information Security Officer(ISO)/Alternate ISO</u>**:

- Ensure access control procedures are in place for temporary access, permanent changes, and termination (friendly and unfriendly) of users. This will be confirmed by regular review and audit.
- Ensure that "rules of behavior" in accordance with DoIT policies and procedures have been established for all IT Systems.
- Ensure that "access notices/rules of behavior" have been reviewed and signed by all users prior to being granted access to the agency's IT Systems.

- Maintain “access notices/rules of behavior” for all individuals accessing the IT System resources.
- Maintain a list of all individuals granted system access, including remote access.
- Ensure that all positions have an established sensitivity level designation.

1.4.7. **Designee(s)** must distribute appropriate application menus and access privileges.

2. INCIDENT REPORTING

2.1. PURPOSE AND SCOPE

2.1.1. This section establishes mandatory procedures for IT Systems' security incident reporting within the Agency. It is designed to provide the Agency personnel the procedures for the proper response to an efficient and timely reporting of computer security related incidents, (e.g. major computer viruses, unauthorized user activity, and suspected compromise of the Agency data). These procedures are intended to meet required mandates of the Agency and to assist in the protection of the Agency IT System resources from unauthorized access, disclosure, modification, destruction, or misuse.

2.1.2. An IT System security incident reporting system is necessary to identify a violation or incident, assess damage as a consequence of a violation, record the violation or incident, investigate and report the incident, and use information to prevent future occurrences or violations. The reporting process outlined in these procedures is intended to detect and respond to IT System security incidents as they occur, assist in preventing future incidents through awareness, and when combined with existing IT System security procedures, augment the Agency IT System security controls.

2.1.3. The policy contained in this section covers all the Agency IT System resources whether maintained in-house or in the interest of the Agency. These policies are mandatory on all organizational units, employees, contractors, and others having access to and/or using the IT System resources of the Agency

2.2. BACKGROUND

2.2.1. Incident Response is a requirement of the Office of Management and Budget () Circular A-130, “Management of Federal Information Resources,” Appendix III. Responding to computer security incidents is generally not a simple matter. This activity requires technical knowledge, communication and coordination among staff responding to the incident, and adherence to applicable the Agency policy. Incidents over the last few years indicate that, if anything, responding to incidents is increasingly more complex. Intrusions into machines are a serious concern, and increasing sophistication and collaboration among network attackers pose a considerable threat to the integrity of computing resources. Viruses will continue to occasionally infect the Agency computers, despite widespread availability of virus detection and eradication software.

2.3. POLICY/PROCESS

2.3.1. <u>Security Incident Standards</u>

2.3.1.1. An incident refers to a computer security problem arising from a threat. Computer security incidents can range from a single virus occurrence to an intruder attacking many networked systems, or such things as unauthorized access to sensitive data and loss of mission-critical data.

2.3.1.2. IT System security incidents to be reported and tracked can be categorized as follows (these types of acts are not all-inclusive):

- Circumvention of IT System security controls, safeguards and/or procedures
- Unauthorized access, use, disclosure, alteration, manipulation, destruction, or other misuse of data and AIS
- Theft, fraud, or other criminal activity committed with the aide of IT System resources
- Theft, loss or vandalism of IT System hardware, software or firmware
- Issues affecting confidentiality, integrity and availability of data
- Unauthorized downloading or copying of sensitive Agency information

2.3.1.3. **<u>Examples</u>** of specific reportable incidents which are to be reported under the six categories of incidents include (but are not limited to):

- Unauthorized access to or use of sensitive data for illegal purposes
- Unauthorized altering of data, programs, and IT System hardware
- Loss of mission-critical data
- Environmental damage/disaster (greater than $10,000) causing loss of IT System services or data, or which may be less than $10,000 in damage yet have affected the Administration's or staff office's capabilities to continue day-to-day functions and operations
- Major infection of sensitive systems or software by malicious code, i.e. virus, Trojan Horse, etc
- IT System perpetrated theft, fraud and other criminal computer activity;
- Telecommunications/network security violations, i.e., networks (including local area networks (LANs) and wide area networks (WANs)) which experience service interruptions that cause an impact to an indefinite number of end users

- Theft or vandalism of IT System hardware, software or firmware whose loss did or may affect the organization's capabilities to continue day-to-day functions and operations
- Unauthorized access to data when in transmission over communications media (e.g. sniffers)
- Loss of system availability impacting the ability of users to perform the functions required to carry out day-to-day responsibilities (e.g. denial of service attacks)
- Unauthorized access to and/or unauthorized use of the Internet

2.3.2. Reporting Procedures

2.3.2.1. The person observing or discovering the incidents, as defined above, advises their supervisor or the office ISO as soon as possible. The office CISO is responsible for recording and reporting security incidents. Additionally, those incidents which are determined to affect a agency's capability to accomplish critical functions, restrict the availability of a system or communications medium, i.e. LAN, WAN, etc., or result in a monetary impact to the agency, will be reported within 48 hours of the occurrence to the Agency Information Security Officer. Depending on the severity and the nature of the incident, the Agency CISO may also contact the Agency General Counsel, and the Office of the Inspector General (OIG), and FedCIRC.

2.3.2.2. Reportable IT System security incidents are recorded on a security incident form or log as developed by the office. Essential information about the security incident will be identified in as much detail as possible, at the time of occurrence. Some information may need to be added at a later time based on the investigation/closure of the incident. The following minimum information about a security violation or incident will be entered on the IT System security violation/incident form:

- Location of incident and organization filing report
- Reported by (Name, Title and Organization)
- Date and time of report filing
- Date and time of incident
- Details of incident (include names of personnel involved and description of the who, what, when, where, how, and why)
- The name and title of the person to whom the incident initially was reported
- Identification of whether the Inspector General or appropriate law enforcement organization has been notified
- Incident impact on day-to-day operations

- Action taken to contain the incident and resources required to correct the incident (in cases of system outage note what vendors have been contacted)
- Short-range corrective action, such as immediately removing a terminated employee's access privileges
- Long-range corrective actions, as necessary
- Estimated monetary damage
- Additional information, as appropriate

2.3.2.3. The information collected on the IT System security incident form is reported to the Agency Information Security Officer (ISO) in a confidential manner.

- Initial reports of serious incidents or violations may be reported by telephone.
- Reports may be sent by U.S. mail using the double-envelope method, couriers, or secured electronic mail or facsimile.
- Follow-up contact will be established with the reporting unit or office by the CISO, and tracking for each incident will be continued until final closure.
- Each office or unit ISO will be responsible for making the determination of whether the IT System security incident at their level is reportable based on the definitions provided in this procedure and ensuring that reports are filed with the Agency ISO.

2.3.2.4. **Protection of Report Information**: IT System security incident report information will be treated as sensitive information and safeguarded as equivalent to Privacy Act information. Access to IT System security incident information must be restricted and stored in a secured area.

2.3.3. Tracking of IT System Security Incidents

2.3.3.1. The ISSO is responsible for tracking IT System security violations and incidents for the Agency. Tracking includes monitoring each incident through final closure and maintaining a copy of the incident report for a period of three (3) years. The ISSO reports those security violations and incidents which threaten critical organization functions to the office of the e Agency Information Security Officer (ISO).

2.3.3.2. **Reporting of Security Incidents and Violations to the Media:** The Agency offices must refer questions from the media (e.g., newspapers, television, and radio) concerning IT System security violations or incidents to the Agency Public Affairs Office.

2.4. RESPONSIBILITIES

2.4.1. **Agency ISO**:

- Ensures that the Agency policy, procedures, and standards meet the Agency requirements outlined in the Agency's corresponding Handbook.
- Provides guidance and assistance to the Agency offices in preparing their IT System Security Incident Reporting policy, procedures, and standards to comply with the Agency policy.
- Provides assistance, upon request, and as needed, to the Agency offices in dealing with both the administrative and technical aspects of reportable IT System security incidents. The Agency Information Security Officer (ISO) is the initial point of contact for each office.
- Organize an incident response team, as needed, to assist sites with IT System security incidents.
- Report incidents that are determined to affect the Agency's overall capability to accomplish critical functions; restrict the availability of a system or communications medium; or result in a monetary impact to the Agency' s Information Resources Security Officer (ISO).

2.4.2. **The Office of the General Counsel**:

- Interprets laws, regulations, and directives applicable to the Agency IT System security activities, and specific to IT System incident occurrences and reporting of those occurrences.
- Renders legal advice and other legal services with respect to IT System security incidents.

2.4.3. **The Office of the Inspector General**:

- Investigates and audits major IT System security incidents when appropriate, and conducts criminal investigations, as warranted.
- Provides advice on coordinating an investigative process for IT System security incidents and reconciliation of those incidents.

2.4.4. **The Agency CIO**: The Agency CIO ensures that the provisions of this section are implemented at all agencies within the Agency.

2.4.5. **<u>Office Heads, and Regional Agency Directors</u>**:

- Implement the IT System security requirements at their office or agency.
- Ensure that the office or unit ISO investigates, reviews, and records IT System security incidents and notifies the Agency Information Security Officer when a reportable incident, as defined above, occurs.

2.4.6. **<u>The Information Security Officer</u>(ISO)/Alternate ISO**:

- Establishes the office IT System security incident reporting system.
- Logs, investigates, and reviews IT System security incidents and reports the incidents to the appropriate the Agency Information Security Officer.
- Establishes contact with the Agency incident response team when a reportable incident occurs as defined earlier in this section.

2.4.7. **<u>Managers and Supervisors</u>**:

- Implement the requirements of the unit's IT System security incident reporting procedures within their assigned areas of management control.
- Ensure that IT System security violations/incidents, occurring within their assigned area of management control, are reported to the appropriate agency ISO.
- Ensure on a regular basis that all assigned employees, contractors and other individuals, who develop, operate, administer, maintain, or use the Agency IT System resources understand they are responsible for reporting actual or suspected IT System security incidents to their immediate supervisor or office ISO.

2.4.8. **<u>All the Agency Employees, contractors, and other individuals</u>** with access to sensitive areas or IT Systems are responsible for reporting IT System security violations or incidents to their supervisor and/or ISO.

3. EDUCATION, TRAINING AND AWARENESS

3.1. PURPOSE AND SCOPE

3.1.1. This section provides policy and guidance for offices in establishing their security awareness and training program. To protect the integrity, confidentiality, and availability of information, the Agency offices will ensure that each person involved understands their roles and responsibilities and is adequately trained to perform them.

3.1.2. The procedures and responsibilities described in this handbook apply to all the Agency organizational units, employees, contractors, and others having access to and/or using the IT System resources of the Agency.

3.2. BACKGROUND

3.2.1. The Computer Security Act of 1987 (Public Law 100-235) requires that “each agency must provide for the mandatory periodic training in computer security awareness and accepted computer practices of all employees who are involved with the management, use, or operation of each Federal computer system within or under the supervision of that agency”.

3.2.2. In accordance with the Computer Security Act of 1987, the National Institute of Standards and Technology (NIST) working with the U.S. Office of Personnel Management (OPM) was charged with developing and issuing guidelines for Federal computer security training. This requirement was satisfied by NIST’s issuance of “Computer Security Training Guidelines” (Special Publication 500-172).

3.2.3. In January 1992, OPM issued a revision to the Federal personnel regulations making these voluntary guidelines mandatory. This regulation, 5 CFR Part 930, is entitled “Employees Responsible for the Management or Use of Federal Computer Systems” and requires Federal agencies to provide IT System security training as set forth in NIST guidelines.

3.2.4. In 1998, the Office of Management and Budget () Circular A-130, “Management of Federal Information Resources,” Appendix III, “Security of Federal ITResources,” re-enforced these mandatory training requirements and added additional requirements.

3.2.5. Due to the revision of Circular A-130, Appendix III, NIST issued a new publication in April 1998, which superseded Special Publication 500-172. This new publication, NIST Special Publication 800-16, “Information Security Training Requirements: A Role- and Performance-Based Model” presents a new conceptual framework for providing IT System security training. This publication is available on the Agency Information Security web site.

3.3. POLICY

3.3.1. IT System Security awareness training is required for:

- New employees within 60 days of hire
- All users on an annual refresher basis
- Whenever there is a significant change in the IT System security environment or procedures
- When an employee enters a new position that deals with sensitive information

3.3.2. Initial User Awareness Training

3.3.2.1. Each employee (the Agency employee, contractors, and all other individuals using IT System resources) must attend or receive some form (e.g. computer based training [CBT] or video) of initial IT System security awareness training prior to being granted access to the Agency systems. The user must understand the basic purpose of the Information Security Program and its implementation before IT System access is granted. At a minimum, the users must understand the following IT System security components:

- IT System Security Policy
- Confidentiality
- Password Security; Logging Off; Multiple Sign-Ons
- Appropriate IT System Security Behaviors
- Identification of CISO
- Malicious Software
- Email hoaxes
- Back-ups (where appropriate)
- Internet Use
- Software licensing
- Email manners
- Expectations of privacy
- Incident reporting
- Telecommunication Security

- Network Overview
- Remote sign-on
- Physical security
- Disposal of Sensitive Information
- Repercussions of misuse of IT System resources

3.3.3. Attendance at all security training will be documented for each employee and placed in the employee's personnel file.

3.3.4. Continuing Training

3.3.4.1. As part of an effective information security training program, the office or unit will also provide an ongoing security awareness program for all users. Awareness activities may include:

- Distribution of IT System security pamphlets and flyers
- Viewing of IT System security videos
- Dissemination of security posters throughout the agency
- Security articles in the site's newsletters, daily bulletins, web pages, etc

3.3.4.2. Each user is required annually to review the station information security policy and/or procedures

3.3.5. In addition to the initial orientation awareness training and ongoing security awareness activities, the user (e.g., employee, trainee, contractor, volunteer, etc.) will receive continuing training annually in additional aspects of information security as it relates to the requirements of the duties of the individual. Depending upon an individual's responsibilities, the following is a list of possible training subjects:

- Laws and Regulations
- IT System Security Program
- System Environment
- System Interconnection
- Information Sharing
- Sensitivity
- Risk Management
- Management Controls

- Acquisition/Development/Installation/Implementation Controls
- Operational Controls
- Awareness, Training, and Education Controls
- Technical Controls
- Contingency Plans
- Internet/Intranet

3.3.6. The supervisor will assess the need for appropriate information security training as the employee's position changes or is revised. Employees will be solicited for ideas on how to improve information security in the agency. NOTE: *Everyone should be encouraged to view information security as a positive procedural tool ensuring the* confidentiality, *integrity, and availability of the Agency IT System systems.*

3.3.7. The Agency’s standard for developing and conducting IT System security awareness and training for the Agency employees is NIST’s Special Publication 800-16, “IT Security Training Requirements: A Role- and Performance-Based Model”.

3.4. RESPONSIBILITIES

3.4.1. **The Agency CIO:** Ensures that the provisions of this section are implemented at all agencies within the Agency.

3.4.2. **Office Heads, and Regional Agency Directors**:

- Ensure that their office has an information security training program that is effective, dynamically applicable, and documented.
- Ensure that information security is presented in a positive, cost-effective way.
- Participate in orientation and continuing education activities to emphasize support for the information security program.
- Ensure there is a method established office-wide to document IT System security training in each employee’s personnel folder.

3.4.3. **The DoIT Chief Security Officer (CISO)**:

- Provides assistance and support to the ISOs within the Agency,
- Reviews the site’s security awareness and training programs during scheduled security audits.

3.4.4. **Agency Information Security Officer(ISO)/Alternate Information Security Officer(AISO)**:

- Ensures that an information security orientation is presented during new employee entry processing.
- Maintains documentation of employee awareness and refresher training.
- Ensures that additional specialized training is provided as required. This will be accomplished by working with the supervisors, and with the assistance of the respective ISO, and the Agency.
- Monitors the Information Security Awareness Program and recommends policy and procedure. Specific information security responsibilities will be documented in each position description and consequences of noncompliance to information security procedures will be implemented according to current Human Resources directives concerning employee conduct.
- Distributes State provided information security training to the agency staff as it becomes available and works closely with supervisors to disseminate this information.

3.4.5. **Supervisors**:

- Ensure that employees who have functional responsibilities in information security areas (e.g., ISO and system administrators) are given the opportunity to attend security training lectures, courses, conferences, etc.
- Provide copies of the Agency IT system security policy and rules of behavior to the employee and discuss with the employee how they relate to the employee’s specific position.
- Assess the need for appropriate information security training of an employee as assignments change or as a position is revised.

3.4.6. **Agency employees and other users**:

- Attend security orientation training and any other specifically assigned IT System security training, as required, to fulfill their role.
- Annually review the information security policy and rules of behavior appropriate to the use of the Agency IT.

4. SECURITY CONSIDERATIONS IN COMPUTER SUPPORT OPERATIONS

4.1. PURPOSE

4.1.1. This section provides guidance for computer support and operations. The primary goal of computer support and operations is the continued and correct operation of a LAN/WAN computer system. The closely linked goals of computer security are the availability, confidentiality, and integrity of systems.

4.1 *BACKGROUND*

4.1.2. Computer support and operations refers to everything required to run a computer system to include both system administration and tasks external to the system that support IT operation (e.g., maintaining documentation). The support and operation of any computer system is critical to maintaining the security of a system. Support and operations are routine activities that enable computer systems to function correctly. These include fixing software or hardware problems, loading and maintaining software, and helping users resolve problems.

4.1.3. The failure to consider security as part of the support and operations of computer systems is, for many Agencies, their Achilles heel. Agencies often undermine their expensive security measures because of poor documentation, old user accounts, conflicting software, or poor control of maintenance accounts. Also, agencies' policies and procedures often fail to address many of these important issues.

4.1.4. The important security considerations within some of the major categories of support and operation are:

- User support
- Software support
- Hardware support
- Configuration management
- Backups
- Media Controls
- Documentation
- Maintenance

4.2. POLICY

4.2.1. <u>User Support</u>

- (User Support Services) provides Agency user support. An important security consideration for user support personnel is the ability to recognize which problems are security related.
- System support and operations staff must be able to identify security related problems, respond appropriately, and inform appropriate individuals. A wide range of possible security problems exists. Some will be internal to the Agency applications, while others apply to off-the-shelf products. Additionally, problems can be software or hardware based.
- User support must be closely linked to the organization's incident handling capability. In many cases, the same personnel perform these functions.

4.2.2. <u>Software Security and Support Elements</u>

4.2.2.1. Controlling what software is used on a system.

- All executable software used on sensitive the Agency IT System resources must be obtained through authorized channels.
- Each system installation of the Agency-developed or off-the-shelf software must be reviewed and approved for determination of need and system compatibility, prior to installation. This includes software acquired by any other means (e.g., public domain software, bulletin board services, personally owned software, Internet obtainable freeware).
- Executable software authorized to run on an Agency IT System resource must be identified in the system's security plan.

4.2.2.2. Ensuring that software has not been modified without proper authorization.

- There must be no local modification of security software features.
- Willful and intentional modification of the Agency software for illegal or disruptive purposes or for personal gain is a crime. There will be no modifications of these programs except through authorized channels.
- Safeguards must be in place to detect and minimize inadvertent or malicious modification or destruction, or attempts to do so, of the Agency's IT System application software, operating system software, and critical data files. The safeguards will achieve the integrity objectives and be documented in the system's security plan. The level of protection will be commensurate with the sensitivity of the information processed.

- All approved software, regardless of source, will be scanned for viruses prior to use. Virus and malicious code (software) prevention and control measures will be employed on every Agency IT System resource to protect the integrity of the software and data.

4.2.2.3. Ensuring that software is properly licensed.

- Use of copyrighted software will comply with copyright laws and license agreements. See the Agency 802, Appropriate Use of the Agency Office Equipment, and the Agency 815, New Desktop Software Requests.
- The Agency licensed software may not be taken home without management approval.

4.2.3. Hardware Security and Support Elements

4.2.3.1. Hardware support will be under the direction of Agency User Support (or its equivalent) or DoIT Service Desk.

4.2.3.2. Security measures must be taken by all users to protect against theft and unauthorized use of IT System peripheral and communications devices, computers, and related items such as printers, disks, and software.

4.2.3.3. The removal of peripheral or communication devices from an agency for use off-site must be controlled. Appropriate documentation will be maintained of all IT System equipment and software removed from the agency, including the individual responsible for the equipment and the date(s) the equipment was removed and returned to the agency. NOTE: Remote off-site (e.g., dial-in) access to a computer system must be authorized

4.2.3.4. All physical security requirements (e.g., key and cypher lock hardware, security surveillance television equipment, room intrusion detectors), as identified in the risk analysis, which may be deemed necessary by the agency ISO to protect peripheral devices and microcomputers, will be compatible with and, when possible, integrated into the agency's security system.

4.2.3.5. Locks and access control procedures will be used to protect storage media containing sensitive data.

4.2.3.6. For those systems where virus protection is applicable, such protection must be current and enabled.

4.2.4. Configuration Management

4.2.4.1. Agencies must practice configuration management. Configuration management:

- Manages changes made to a system's hardware, software, documentation, and tests throughout the life of a system.

- Identifies, documents, and verifies the functional and physical characteristics of an IT System, recording its configuration, and controlling changes to the System and its documentation.
- Ensures that changes to the system do not unintentionally or unknowingly diminish security.

4.2.4.2. Configuration management will provide a complete audit trail of decisions and design modifications.

4.2.4.3. A Configuration management plan will include:

- A baseline that includes the controls for changes to IT System resources, including hardware, software, administrative requirements, documentation, and connectivity to another IT System or LAN.
- A current list of all components of the IT System (hardware, software, and their documentation).
- The configuration of the peripherals (printers, modems) and interconnections to other IT Systems (shared printers, file servers) and LANs.
- Listing of version releases of current software, information on batch files, environmental settings such as paths, and switch settings of machine components.

4.2.4.4. All the Agency IT Systems will employ configuration management at a level appropriate with the size, complexity, and sensitivity of the system.

4.2.5. Backups

4.2.5.1. Backup of IT System resources must be done on a periodic basis.

- Support and operations personnel backup major systems’ software and data.
- Users of smaller systems are responsible for their own backups.
- Agencies may task support personnel with making backups periodically for smaller systems, either automatically (through server software) or manually.

4.2.5.2. Backups are critical to contingency planning and all users must be provided adequate awareness training on the importance of backing up data as well as the appropriate method for backing up their data, if this function is their responsibility.

4.2.5.3. Frequency of backups will depend upon how often data changes and how important those changes are.

4.2.5.4. Backup procedures must be periodically tested to ensure that copies work as intended..

4.2.5.5. Backups will be stored securely.

4.2.6. **Media Controls**. Media controls will be utilized to protect IT System resources. Media controls include a variety of measures to provide physical and environmental protection and accountability for tapes, disks, printouts, and other media. From a security perspective, media controls will be designed to prevent the loss of confidentiality, integrity, or availability of information, including data or software, when stored outside the system. This can include storage of information before it is input to the system and after it is output. The extent of media control depends upon many factors, including the type of data, the quantity of media, and the nature of the user environment. Physical and environmental protection is used to prevent unauthorized individuals from accessing the media. It also protects against such factors as heat, cold, or harmful magnetic fields.

4.2.6.1. **Marking/physical labeling**.

- Use labels to identify media with special handling instructions, to locate needed information, or to log media to support accountability. Identification is often by colored labels on diskettes or tapes or banner pages on printouts.

- If labeling is used for special handling instructions, users must be appropriately trained. The marking of IT System input and output is generally the responsibility of the user, not the system support staff. Typical markings for media could include Privacy Act Information or Joe's backup tape. In each case, the individuals handling the media must know the applicable handling instructions. For example, Joe's backup tape should be easy to find in case something happens to Joe's system. Also marking backup diskettes can help prevent them from being accidentally overwritten.

4.2.6.2. **Logging:** The logging of media will be used to support accountability. Logs can include control numbers (or other tracking data), the times and dates of transfers, names and signatures of individuals involved, and other relevant information. Periodic spot checks or audits may be conducted to determine that no controlled items have been lost and that all are in the custody of individuals named in control logs.

4.2.6.3. **Physical Access Protection**: As media can be stolen, destroyed, replaced with a look-alike copy, or lost, physical access protection must be utilized by agencies to protect their IT System resources. Physical access controls include locked doors, desks, file cabinets, or safes.

- If the media requires protection at all times, ensure the output data goes to a medium in a secure location (e.g., printing to a printer in a locked room instead of a general-purpose printer in a common area).

- Physical protection of media must be extended to backup copies stored offsite. Back-up copies will be accorded an equivalent level of protection to media containing the same information stored onsite. (Equivalent protection does not mean that the security measures need to be exactly the same. The controls at the off-site location are quite likely to be different from the controls at the regular site.)

4.2.6.4. **Environmental Protection:** Magnetic media, such as diskettes or magnetic tape, will be provided environmental protection, since they are sensitive to temperature, liquids, magnetism, smoke, and dust. Other media (e.g., paper and optical storage) will have different sensitivities to environmental factors and should be protected accordingly.

4.2.6.5. **Transmittal:** Media transferred within the agency and to outside elements must be secured during transmittal. Possible methods include sealed and marked envelopes, authorized messenger or courier, or U.S. certified or registered mail.

4.2.6.6. **Disposition:** Ensure that information is not improperly disclosed when media is disposed. This applies both to media that is external to a computer system (such as a diskette) and to media inside a computer system, such as a hard disk. The process of removing information from media is called sanitization. One of the following three techniques must be used by agencies in disposing of their media:

- Overwriting. Overwriting uses a program to write (1s, Os, onto the media. Common practice is to overwrite the media three times. Overwriting should not be confused with merely deleting the pointer to a file (which typically happens when a *delete* command is used). Overwriting requires that the media be in working order.
- Degaussing. Degaussing is a method to magnetically erase data from magnetic media. Two types of degaussers exist: strong permanent magnets and electric degaussers.
- Destruction. Destruction is shredding or burning.

4.2.6.7. **Documentation:** Documentation of all aspects of computer support and operations must be maintained to ensure continuity and consistency. Formalizing operational practices and procedures with sufficient detail helps to eliminate security lapses and oversights, gives new personnel sufficiently detailed instructions, and provides a quality assurance function to help ensure that operations will be performed correctly and efficiently.

- The security of a system must be documented. This includes many types of documentation, such as security plans, contingency plans, risk analysis, and security policies and procedures. Much of this information, particularly risk and threat analyses, has to be protected against unauthorized disclosure. Security documentation needs to be both current and accessible. Accessibility should take special factors into account (such as the need to find the contingency plan during a disaster).
- Security documentation must be designed to fulfill the needs of the different types of people who use it. Agencies should have locally developed *policy* and *procedures*. Policy is outlined in Section 1 of the the Agency IT System Handbook – Management Controls. Security procedure manuals are written to inform various system users how to do their jobs securely. A security procedures manual for

systems operations and support staff will address a wide variety of technical and operational concerns in considerable detail.

4.2.6.8. **Maintenance:** System maintenance requires either physical or logical access to the system. If someone who does not normally have access to the system performs maintenance, then a security vulnerability is introduced.

- Procedures must be developed to ensure that only authorized personnel perform maintenance. IT System technical support and maintenance work performed at the Agency agencies (on-site) must be supervised by or under the control of the Agency personnel knowledgeable in appropriate IT System operations.
- Automated (i.e., computer-connected) dial-up diagnostic maintenance of sensitive the Agency systems via remote communications between vendors and the Agency IT System resources is prohibited unless authorized by management in the system's accreditation. If authorized, authentication of the maintenance provider by the system prior to access is required.
- If a system has a maintenance account, it is critical to change factory-set passwords or otherwise disable the accounts until they are needed.

4.3. RESPONSIBILITIES

4.3.1. **Agency CIO:** Ensures that the provisions of this section are implemented at all agencies within the Agency.

4.3.2. **Agency ISO**: Ensures that the Agency policy, procedures, and handbooks reflect the Agency, Federal and generally accepted principles and practices for security IT Systems.

4.3.3. **Office Heads, and Regional Agencies Directors**: Ensure that adequate support and funding are provided to support their IT System functions and are ultimately responsible for the security for systems under their management control.

4.3.4. **Office, Library, and Regional CIOs**: Implement adequate computer support to the unit's systems and to the users.

4.3.5. **System Administrators:** Ensure that the controls described above are maintained for their assigned systems and are responsible for day-to-day operations.

4.3.6. **Information Security Officer (ISO)/Alternate Information Security Officer (AISO)**: Assist the support and operations staff in performing their duties and responsibilities as outlined in this section.

5. PHYSICAL/ENVIRONMENTAL SECURITY

5.1. PURPOSE AND SCOPE

5.1.1. This section provides policy and guidance to implement minimum requirements that will reduce the exposure of computer equipment to physical and environmental damage and assist in achieving an optimum level of protection for the Agency IT Systems.

5.1.2. The policy contained in this section covers all the Agency IT System resources maintained in-house or in the interest of the Agency. These policies are mandatory and apply to all organizational units, employees, contractors, and others having access to and/or using the IT System resources of the Agency.

5.1.3. This policy applies to all IT Systems currently in existence and any new automated technology acquired after the effective date of this policy document.

5.2. BACKGROUND

5.2.1. In the early days of computer technology, securing the system in a controlled environment with very limited access protected the computers and the information they processed. Although major changes in computer environments have occurred, physical security is still vitally important. Physical security measures are a tangible defense that must be taken to protect the agency, equipment, and information from theft, tampering, careless misuse, and natural disasters.

5.3. POLICY

5.3.1. Staff and equipment require a safe, secure, and technically sound physical environment. While it is necessary to comply with each of the areas addressed, appropriate adjustments or allowances may be made for the organization, physical plant, and any special requirements of the individual office or agency. Deviation from the minimum requirements must be annotated on the system risk assessment and the Office Head or Agency Director must be aware and acknowledge this deviation in the accreditation of the system.

5.3.2. There must be, at a minimum, a cipher lock or suitable substitute on each door to the computer room.

5.3.3. Only personnel who require access to perform their official duties will be permitted in the computer room.

5.3.4. A log will be kept of all personnel who were issued the combination/key to the computer room and the person will be required to sign for that combination/key.

5.3.5. The combination of a cipher lock will be changed frequently, especially when a person who was previously given the combination leaves the organization.

5.3.6. Keys or card keys will be returned to the Agency upon separation, transfer, or termination.

5.3.7. Loss of keys or disclosure of cipher key code will be reported to the ISO immediately.

5.3.8. A computer room access roster will be established.

5.3.9. There will be signs posted designating the room as a “Restricted Area”.

5.3.10. Contract maintenance personnel and others not authorized unrestricted access but who are required to be in the controlled area, will be escorted by an authorized person at all times when they are within the controlled area.

5.3.11. All access to the computer room will be logged, and logs reviewed monthly by the ISO to determine if access is still required.

5.3.12. There shall be no signs to indicate that an information system is located in any particular building or area.

5.3.13. The main computer room should have certain structural physical security features. The computer room:

- Should be located in the center of the building
- Should not have windows
- The computer room walls should extend from true floor to true ceiling
- Failure to meet these requirements must be annotated in the risk assessment

5.3.14. Media used to record and store sensitive software or data will be labeled, protected, controlled and secured when not in use.

5.3.15. Physical access controls will also be implemented not only in the area containing system hardware, but also locations of wiring used to connect elements of the system, supporting services (such as electric power), backup media, communications closets, and any other elements required for the system’s operation.

5.3.16. It is important to review the effectiveness of physical access controls in each area, both during normal business hours and at other times – particularly when an area may be unoccupied.

5.3.17. A computer room will have appropriate environmental security controls implemented, which include measures implemented to mitigate damage to IT System resources caused by fire, electrical surges and outages, water, and climate control failure.

5.3.17.1. **Fire and Smoke**

- Install smoke detectors near computer equipment – and check them periodically.
- Keep fire extinguishers in and near your computer rooms, and be sure all those with authorized access know where they are and how to use them.
- Enforce no smoking, no eating, and no drinking policies.
- Periodically hold fire drills.

5.3.17.2. Climate

- Keep all rooms containing computers at reasonable temperatures, following manufacturers recommendations.
- Keep the humidity level at 20-30 percent.
- Install gauges and alarms that warn you if the environmental controls are getting out of range. These alarms will be monitored at all times.
- Equip all heating and cooling systems with air filters to protect against dust and other particulate matter.

5.3.17.3. Water

- Protect your systems from the various types of water damage. Flooding can result from rain or ice buildup outside, toilet or sink overflow inside, or water from sprinklers used to fight a fire. Maintain plastic sheeting to protect the equipment if the sprinklers go off.
- Avoid locating computer rooms in the basement.

5.3.17.4. Electricity

- Connect all IT System resources to a non-interruptible power supply (UPS) that is tested periodically.
- Connect all critical IT System equipment to backup emergency generators.
- Install anti-static carpeting in each agency.

- Install a line filter on your computer’s power supply. A voltage spike can destroy your computer’s power supply.

5.4. RESPONSIBILITIES

5.4.1. **__Agency ISO:__** Ensures that the Agency policy, procedures, and handbooks reflect the Agency, Federal, and generally accepted principles and practices for the security of IT Systems.

5.4.2. **__Agency CIO:__** Ensures that the provisions of this section are implemented at all agencies within the Agency.

5.4.3. **__Office Heads, and Agency Directors:__**

- Ensure procedures are established for identifying and reporting suspected or actual breaches of physical security.
- Ensure that adequate funding is available for IT System physical and environmental controls for elements under their administrative control.
- **__User Support__**. Helps to develop, in cooperation with the ISO, physical access control procedures for the computer room and other restricted areas. Trains staff on the procedures established.
- **__System Administrators.__** Comply with access control procedures established for the computer room.
- **__ISO/AISO__**. Monitors access to the computer room and ensures that the physical access control procedures are established and followed.

6. CONTRACTOR/VENDOR/PARTNER SECURITY

6.1 *PURPOSE*

6.1.1. This section provides policy and guidance on implementing minimum security requirements for conducting the Agency business utilizing contracts, sharing agreements, and memorandums of understanding (MOUs) with companies, vendors, and other federal agencies.

6.1.2. The policy contained in this section covers all the Agency IT System resources maintained in-house or in the interest of the Agency. These policies are mandatory on all organizational units, employees, contractors, and others having access to and/or using the IT System resources of the Agency.

6.1.3. This policy applies to all IT Systems currently in existence and any new automated technology acquired after the effective date of this policy document.

6.1. BACKGROUND

6.1.1. The Agency is increasing the use of contractors and their services as well as entering into inter-agency agreements. This section covers in further detail some of the security requirements and controls that need to be addressed to ensure the confidentiality, integrity, and availability of the Agency's sensitive data and resources.

6.2. POLICY

6.2.1. **<u>Contractor Personnel Security:</u>**

6.2.1.1. Security requirements and specifications for hardware and software maintenance personnel contracted from commercial sources must be defined and approved prior to signing of contractual agreements.

6.2.1.2. Such requirements will vary depending upon the level of trust associated with the equipment or system to be maintained.

6.2.1.3. Maintenance contractors and their employees will be granted limited and controlled access to computer equipment and systems consistent with established security requirements. The access provided must be the MOST restrictive set of capabilities and privileges required to perform the work.

6.2.1.4. Access of contractors to the Agency's sensitive systems must be in the interest of the Agency.

6.2.1.5. Access must be limited to a specified timeframe appropriate to the task and then reviewed for possible termination.

6.2.1.6. The Agency management or their designees must officially sponsor all non-the Agency personnel accessing the Agency resources.

6.2.1.7. All contractors that have access to the Agency’s sensitive systems and data must be required to meet the minimum the Agency security requirements outlined in Section 1 “Personnel Security”.

6.2.1.8. Contractors must receive the same security training required for the Agency employees, including orientation and periodic security updates.

6.2.1.9. Contractors must indicate in writing that they have read and understand the Agency security requirements applicable to them.

6.2.1.10. Contract personnel who access the Agency IT System resources or data must have a background investigation. For questions concerning approval of contractor investigations, contact the Agency Security Office.

6.2.1.11. The following language is recommended for inclusion in contracts concerning background investigations:

“The investigative history for contract personnel working under this contract must be maintained in the databases of either the Office of Personnel Management (OPM) or the Defense Industrial Security Clearance Organization (DISCO). Should the contractor use a vendor other than those identified by OPM or Defense Security Service (DSS) to conduct investigations, the investigative company must be certified by OPM/DSS to conduct contractor investigations.

All costs associated with obtaining clearances for contractor provided personnel are the responsibility of the contractor. Further, the contractor will be responsible for the actions of all individuals they employ to work for the Agency under this contract. In the event that damages arise from work performed by contractor provided personnel, under the auspices of this contract, the contractor will be responsible for all resources necessary to remedy the incident.”

Contract personnel performing work under this contract shall satisfy all requirements for appropriate security eligibility in dealing with access to sensitive information and information systems belonging to or being used on behalf of the Agency. To satisfy the requirements of the Agency, a Minimum Background Investigation shall be conducted prior to performing work under this contract. The level of access and the individual's capability to perform work under this contract will be the determining factor in deciding if a higher investigative requirement is needed. The contractor shall ensure that those requirements are fully satisfied within 30 days of initiation of such investigations."

6.2.2. **Contracts/Sharing Agreements/Memorandum Of Understanding (MOU)**

6.2.2.1. All management, operational and technical security requirements outlined in the Agency's IT System Security Handbooks shall be included in contract specifications, as applicable, for the acquisition, maintenance, or operation of the Agency IT System resources.

6.2.2.2. All requirements outlined in Circular A-130, Appendix III, will be implemented.

6.2.2.3. Contracts, sharing agreements, and MOUs pertaining to IT System resources will be reviewed by the ISO for security implications prior to initiation of the contract. A separate section in the contract dealing with security issues will be incorporated, where appropriate.

6.2.2.4. If a potential risk to the Agency information resources exists, the ISO must be contacted for advice and documentation of risk.

6.2.2.5. Each the Agency office and agency must ensure that IT System contracts/agreements/MOUs documents include a written requirement that they (e.g., contractor) meet the minimal security clearance levels as outlined in the Agency's IT Systems Security Operations Handbook, Section 1 "Personnel Security".

6.2.2.6. Contracts must stipulate that the contractor will be held responsible for the cost of background investigations. Contractor personnel's background information must be maintained in the databases of either the Office of Personnel Management (OPM) or the Defense Industrial Security Clearance Organization (DISCO). Should the contractor use another vendor other than OPM or Defense Security Service (DSS) to conduct investigations, the investigative company must be certified by OPM/DSS to conduct contractor investigations.

6.2.2.7. Access to the Agency's network in the performance of contract duties and agreements must be outlined in the statement of work and included in the contract. Inbound access to the Agency's network must be secure and meet all requirements as outlined in the Agency's IT System Technical Handbook, Section 3, "Network and Communication Security". Additional costs for implementing a secure connection must be included in the contract, agreement, or MOU.

6.2.2.8. Following are paragraphs of contracting language that may be added to contracts, as required, to ensure that certain areas of security are addressed:

Records:

(Clause to be added if the contractor will have access to records protected by 38 U.S.C.

"Contractor personnel who obtain access to hardware or media which may manipulate or store any sensitive information protected under 38 USC, as defined by the Agency, must not access information unless absolutely necessary to perform their contractual duties. Disclosure of any sensitive data obtained during the performance of the particular contractual duty is prohibited. Violation of these statutory provisions may involve imposition of criminal penalties."

System of Records:

"The Agency system(s) of records to which the contractor personnel will have access in order to maintain ________(system(s) to be deployed or maintained) is/are (insert title and identity code of the Agency system(s) of records involved).

System Security:

"The Contractor shall provide the Agency with full assurance that security measures have been implemented which are consistent with all the Agency, and other Federal standards and guidelines."

Procedures for User Access:

"Access requirements to the Agency information systems by contractors and contractor personnel shall meet or exceed those requirements established for the Agency employees as described in the Agency's IT System Security Policy the IT System Security Handbooks."

6.3. RESPONSIBILITIES

6.3.1. **Agency ISO:** Ensures that the Agency policy, procedures, and handbooks reflect the Agency, federal and generally accepted principles and practices for security IT Systems.

6.3.2. **Agency CIO**: Ensures that the provisions of this section are implemented at all agencies within the Agency.

6.3.3. **Office Heads, and Agency Directors**: Ensure that adequate contractual controls are implemented for all contracts, agreements, and procurements for which they hold responsibility and are ultimately responsible for the information security for systems in the area under their administrative control.

6.3.4. **CIO//ISO/AISO**

6.3.4.1. Ensures that all IT System security requirements (management, operational, and technical) are reviewed and documented prior to negotiating a contract, agreement, or MOU.

6.3.4.2. Provides security requirements to the procurement official for inclusion into the contract, agreement, or MOU.

6.3.5. **Procurement Official**

6.3.5.1. Ensures that the ISO reviews any contracts, agreements, MOUs pertaining to IT System resources for adequate security specifications and requirements.

6.3.5.2. Ensures the inclusion of a separate section in the contract dealing with information security issues, where appropriate.

6.3.6. **Contractors**

6.3.6.1. Comply with all the Agency and Federal security requirements.

6.3.6.2. Protect access codes from improper disclosure.

6.3.6.3. Access only authorized IT System applications and data necessary to perform approved activities. Access capability does not equate to authority (e.g., casual browsing of data is not permitted).

6.3.6.4. Notify the Agency contact when access or authority is no longer required for approved tasks.

6.3.6.5. Attend IT System security training as required by the Agency policy, regulations, MOUs, or sharing agreements.

6.3.6.6. Fund and obtain background investigations as required.

7. APPENDIX A

7.1. ACRONYMS

AISO	Alternate Information Security Officer
CIO	Chief Information Officer
DISCO	Defense Industrial Security Clearance Organization
DSS	Defense Security Service
NHT	Information Technology Services Division
ISO	Information Security Officer
LAN	Local Area Network
MOU	Memorandum of Understanding
NIST	National Institute of Standards and Technology
OIG	Office of the Inspector General
	Office of Management and Budget
OPM	Office of Personnel Management
ISO	Information Security Officer
WAN	Wide Area Network

8. APPENDIX B

8.1. GLOSSARY

Access Control

Security control designed to permit authorized access to an IT system or application.

Accreditation

A formal declaration by the Office Head that the IT is approved to operate in a particular security mode using a prescribed set of safeguards. Accreditation is the official management authorization for operation of IT and is based on the certification process, as well as other management considerations. The accreditation statement affixes security responsibility with the Office Head and shows that due care has been taken for security.

Authentication

Verification of the identity of a user, user device, or other entity, or the integrity of data stored, transmitted, or otherwise exposed to unauthorized modification in an IT.

Audit Trail

A record showing who has accessed a computer system and what operations he or she has performed during a given period of time. Audit trails are useful both for maintaining security and for recovering lost transactions.

Automated Information System(s) (AIS)

An assembly of computer hardware, software and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information.

Availability of Data

The state when data are in the place needed by the user, at the time the user needs them, and in the form needed by the user.

Backup

A copy of data and/or applications contained in the IT stored on magnetic media outside of the IT to be used in the event IT data are lost.

Certification

The comprehensive evaluation of the technical and non-technical security features of an IT and other safeguards, made in support of the accreditation process, that establishes the extent to which a particular design and implementation meet a specified set of security requirements.

Ciphertext Form of cryptography in which the *plaintext* is made unintelligible to anyone, who intercepts it by a transformation of the information itself, based on some key.

Confidentiality The concept of holding sensitive data in confidence limited to an appropriate set of individuals or organizations.

Configuration Management The process of keeping track of changes to the system, if needed, approving them.

Contingency Plan A plan for emergency response, backup operations, and post-disaster recovery maintained by an activity as a part of its security program that will ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation.

COTS Software Commercial Off The Shelf Software – software acquired by government contract through a commercial vendor. This software is a standard product, not developed by a vendor for a particular government project.

Data Integrity The state that exists when automated data is the same as that in source documents, or has been correctly computed from source data, and has not been exposed to alteration or destruction.

Degaussing Media Method to magnetically erase data from magnetic tape.

Default A value or setting that a device or program automatically selects if you do not specify a substitute.

Dial-up The service whereby a computer terminal can use the telephone to initiate and effect communication with a computer.

Encryption The process of making information indecipherable to protect it from unauthorized viewing or use, especially during transmission or storage. Encryption is based on an algorithm and at least one key. Even if the algorithm is known, the information cannot be decrypted without the key(s).

Facsimile A document that has been sent, or is about to be sent, via a fax machine.

Firewall A system or cination of systems that enforces a boundary between two or more networks.

Friendly Termination The removal of an employee from the organization when there is no reason to believe that the termination is other than mutually acceptable.

Gateway A bridge between two networks.

Hardware Refers to objects that you can actually touch, like disks, disk drives, display screens, keyboards, printers, boards, and chips.

Identification The process that enables recognition of a user described to an IT.

Internet A global network connecting millions of computers. As of 1999, the Internet has more than 200 million users worldwide, and that number is growing rapidly.

Intranet A network based on TCP/IP protocols (an internet) belonging to an organization, usually a corporation, accessible only by the organization's members, employees, or others with authorization. An intranet's Web sites look and act just like any other Web sites, but the firewall surrounding an intranet fends off unauthorized access.

Intrusion Detection Pertaining to techniques, which attempt to detect intrusion into a computer or network by observation of actions, security logs, or audit data. Detection of break-ins or attempts either manually or via software expert systems that operate on logs or other information available on the network.

ISO/AISO The persons responsible to the Office Head or Agency Director for ensuring that security is provided for and implemented throughout the life cycle of an IT from the beginning of the concept development plan through its design, development, operation, maintenance, and secure disposal.

Issue-specific Policy Policies developed to focus on areas of current relevance and concern to an office or agency. Both new technologies and the appearance of new threats often require the creation of issue-specific policies (e.g., e-mail, Internet usage).

IT Security Measures and controls that protect an IT against denial of and unauthorized (accidental or intentional) disclosure, modification, or destruction of ITs and data. IT security includes consideration of all hardware and/or software functions.

IT Security Policy The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.

IT Systems An assembly of computer hardware, software and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information.

LDAP Short for Lightweight Directory Access Protocol, a set of protocols for accessing information directories. LDAP is based on the standards contained within the X.500 standard, but is significantly simpler. And unlike X.500, LDAP supports TCP/IP, which is necessary for any type of Internet access.

Least Privilege The process of granting users only those accesses they need to perform their official duties.

Local Area Network A short-haul data communications systems that connects IT devices in a building or group of buildings within a few square miles, including (but not limited to) workstations, front end processors, controllers, switches, and gateways.

Management Controls Security methods that focus on the management of the computer security system and the management of risk for a system.

Modem An electronic device that allows a microcomputer or a computer terminal to be connected to another computer via a telephone line.

Network Two or more systems connected by a communications medium; a network is composed of a communications medium and all components attached to that medium whose responsibility is the transference of information.

Operating System The most important program that runs on a computer. Every general-purpose computer must have an operating system to run other programs. Operating systems perform basic tasks, such as recognizing input from the keyboard, sending output to the display screen, keeping track of files and directories on the disk, and controlling peripheral devices such as disk drives and printers.

Operation Controls Security methods that focus on mechanisms that primarily are implemented and executed by people (as opposed to systems).

Overwriting media Method for clearing data from magnetic media. Overwriting uses a program to write (1s, Os, or a cination) onto the media. Overwriting should not be confused with merely deleting the pointer to a file (which typically happens when a “delete” command is used).

Password Protected/private character string used to authenticate an identity or to authorize access to data.

Parity The quality of being either odd or even. The fact that all numbers have parity is commonly used in data communication to ensure the validity of data. This is called parity checking.

PBX Short for private branch exchange, a private telephone network used within an enterprise. Users of the PBX share a certain number of outside lines for making telephone calls external to the PBX.

Peripheral Device Any external device attached to a computer. Examples of peripherals include printers, disk drives, display monitors, keyboards, and mice.

Port An interface on a computer to which you can connect a device.

Port Protection Device A device that authorizes access to the port itself, often based on a separate authentication independent of the computer’s own access control functions.

RADIUS Short for Remote Authentication Dial-In User Service, an authentication and accounting system used by many Internet Service Providers (ISPs). When you dial in to the ISP you must enter your username and password. This information is passed to a RADIUS server, which checks that the information is correct, and then authorizes access to the ISP system.

Real Time Occurring immediately. Real time can refer to events simulated by a computer at the same speed that they would occur in real life.

Remote Access The hookup of a remote computing device via communication lines such as ordinary phone lines or wide area networks to access network applications and information

Risk The probability that a particular threat will exploit a particular vulnerability of the system.

Risk Analysis The process of identifying security risks, determining their magnitude, and identifying areas needing safeguards. Risk analysis is a part of risk management.

Risk Management Process of identifying, controlling, and eliminating or reducing risks that may affect IT resources.

Router An interconnection device that is similar to a bridge but serves packets or frames containing certain protocols. Routers link LANs at the network layer.

Rules of Behavior Rules established and implemented concerning use of, security in, and acceptable level of risk for the system. Rules will clearly delineate responsibilities and expected behavior of all individuals with access to the system. Rules should cover such matters as work at home, dial-in access, connection to the Internet, use of copyrighted works, unofficial use of Federal Government equipment, the assignment and limitation of system privileges, and individual accountability.

Security Incident An adverse event in a computer system or the threat of such an event occurring.

Security Plan Document that details the security controls established and planned for a particular system.

Security Specifications A detailed description of the safeguards required to protect a system.

Sensitive Data Any information, the loss, misuse, modification of, or unauthorized access to, could affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, U.S. Code, but has not been specifically authorized under criteria established by an Executive order or an act of Congress to be kept classified in the interest of national defense or foreign policy.

Separation of Duties A process that divides roles and responsibilities so that a single individual cannot subvert a critical process.

Server The control computer on a local area network that controls software access to workstations, printers, and other parts of the network.

Smart Card A credit-card-sized device with embedded microelectronics circuitry for storing information about an individual. This is not a key or token, as used in the remote access authentication process.

Software Computer instructions or data. Anything that can be stored electronically is software.

Software Copyright The right of the copyright owner to prohibit copying and/or issue permission for a customer to employ a particular computer program.

SPAM To crash a program by overrunning a fixed-site buffer with excessively large input data. Also, to cause a person or newsgroup to be flooded with irrelevant or inappropriate messages.

System Set of processes, communications, storage, and related resources that are under the same direct management control, have the same function or Mission objective, have essentially the same operating characteristics and security needs, and reside in the same general operating environment.

System Availability The state that exists when required automated information s can be performed within an acceptable time period even under adverse circumstances.

System Integrity The quality that a system has when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

System Administrator The individual responsible for defining the system's operating parameters, authorized functions, and security requirements. This individual is usually the person who maintains the system on a day-to-day basis.

System Owner The individual who is ultimately responsible for the function and security of the system.

TCP/IP Transmission Control Protocol/Internet Protocol. The Internet Protocol is based on this suite of protocols.

Technical Controls Security methods consisting of hardware and software controls used to provide automated protection to the system or applications. Technical controls operate within the technical system and applications.

Technical Security Policy Specific protection conditions and/or protection philosophy that express the boundaries and responsibilities of the IT product in supporting the information protection policy control objectives and countering expected threats.

Telecommunications Any transmission, emission, or reception of signals, writing, images, sound or other data by cable, telephone lines, radio, visual or any electromagnetic system.

Threat Any circumstance or event with the potential to cause harm to a system in the form of destruction, disclosure, modification of data, and/or denial thereof.

Trojan Horse Any program designed to do things that the user of the program did not intend to do, or that disguise its harmful intent. A program that installs itself while the user is making an authorized entry; and, then is used to break-in and exploits the system.

Unfriendly Termination The removal of an employee under involuntary or adverse conditions. This may include termination for cause, RIF, involuntary transfer, resignation for "personality conflicts," and situations with pending grievances.

User Any person who is granted access privileges to a given IT.

User Interface The part of an application that the user works with. User interfaces can be text-driven, such as DOS, or graphical, such as Windows.

Virus A self-propagating Trojan horse (a program that surreptitiously exploits the security/integrity of a program), composed of a mission component, a trigger component, and a self-propagating component.

Vulnerability A weakness in automated system security procedures, technical controls, environmental controls, administrative controls, internal controls, etc., that could be used as an entry point to gain unauthorized access to information or disrupt critical processing.

Wide Area Network A physical or logical network that provides capabilities for a number of independent devices to communicate with each other over a common transmission-interconnected topology in geographic areas larger than those served by local area networks.

9. APPENDIX C

9.1. REFERENCES

Computer Security Act of 1987 (PL 100-235)

Circular A-123, Internal Control Systems

Circular A-130, Management of Federal Information Resources, Appendix III, "Security of Federal IT Systems".

Privacy Act of 1974 (PL-93-579) and Amendments

NIST SP 800-12, An Introduction to Computer Security; The NIST Handbook

NIST SP 800-14, Generally Accepted Principals and Practices for Securing IT Systems.

NIST SP 500-172, Computer Security Training Guidelines. This was replaced by 800-16. Should it be here instead?

the Agency IT Systems Security Handbook

the Agency Directive XXX, IT Systems Security Policy

	POLICY#	STATUS1	ISSUED	LAST REVISED	PAGE
	10-07	Accepted	6/30/06	4/01/08	1 of 46
State of Rhode Island Department of Administration Division of Information Technology	TITLE	IT Security Handbook Technical Controls			
	DRAFTED BY		Jim Berard		

TABLE OF CONTENTS

1. TECHNICAL SECURITY

1.1. PURPOSE

1.1.1. This chapter provides policy and guidance to implement technical controls that will reduce the exposure of computer equipment and assist in achieving an optimum level of protection for the State of Rhode Island information technology (IT) systems.

1.1.2. The policy contained in this chapter covers all the State IT resources maintained in-house or in the interest of the State. These policies are mandatory on all agencies, organizational units, employees, contractors, and others having access to and/or using the IT resources of the State.

1.1.3. This policy applies to all automated information systems currently in existence and any new automated technology acquired after the effective date of this policy document.

1.2. BACKGROUND

1.2.1. The issues that will be covered in this chapter under technical security are:

- Identification and Authentication
- Authorization/ Access Control
- Audit Trails

1.2.2. Identification and Authentication are critical building blocks of computer security since they are the basis for most types of access control and for establishing user accountability. Identification and Authentication are technical measures that prevent unauthorized people (or unauthorized processes) from entering an automated information system. Access control usually requires that the system be able to identify and differentiate among users. Access control is based on least privilege, which refers to the granting to users of only those accesses minimally required to perform their duties. User accountability requires the linking of activities on a system to specific individuals and therefore, requires the system to identify users.

1.2.3. Access to the State's IT resources must be managed by a combination of technical and administrative controls. Uniform policy for access control across all the State's systems and networks is needed to support today's highly inter-connected environment and ensure that weaknesses at one agency do not place all the State information assets at unnecessary risk.

1.2.4. These controls will ensure that only authorized individuals gain access to information systems resources, that these individuals are assigned an appropriate level of privilege and that they are individually accountable for their actions. Access will be controlled and limited based on positive identification and authentication mechanisms.

1.3. POLICY

1.3.1. Identification is the means by which a user provides a claimed identity to the system. The most common form of identification is the user ID.

1.3.1.1. Unique Identification. Every State information system must ensure that users are uniquely identified before being allowed to perform any actions on the system.

1.3.1.2. Correlate Actions to Users. Each system must internally maintain the identity of all active users and be able to link actions to specific users.

1.3.1.3. Maintenance of User IDs:

- Offices and facilities must ensure that all user IDs belong to currently authorized users
- Identification data must be kept current by adding new users and deleting former users
- Inactive User IDs. User IDs that are inactive for 90 days must be disabled

1.3.2. Authentication is the means of establishing the *validity* of this claim. There are three means of authenticating a user's identity *which can be used alone or in combination*: something the individual knows (a secret –e.g., a password, Personal

Identification Number (PIN), or cryptographic key); something the individual *possesses* (a token – e.g., a bank's ATM card or a smart card); and something the individual *is* (a biometric – e.g., characteristics such as a voice pattern, handwriting dynamics, or a fingerprint).

1.3.2.1. Require Users to Authenticate. Users must authenticate their claimed identities on all IT resources.

1.3.2.2. Limit Log-on Attempts. The State IT Organizations must limit the number of log-on attempts to five (5). This helps to prevent guessing of authentication data. Where round-the-clock system administration service is available, system administrator intervention will be required to clear a locked account. Where round-the-clock system administration service is not available, accounts will remain locked out for at least ten (10) minutes.

1.3.2.3. Administer Data Properly. The State IT Organizations must have procedures to disable lost or stolen passwords and must monitor systems to look for stolen or shared accounts.

1.3.2.4. Passwords - Acceptable passwords must be carefully chosen by the user and enforced by the system. Controls must be implemented to require strong passwords.

1.3.2.5. Acceptable passwords must include each of the following characteristics:

- Letters - Upper or Lower Case Letters (A, B, C,.....Z, a, b,c,......z)
- Westernized Arabic Numerals (0, 1, 2.....9)
- Non-alphanumeric "special characters." For example, punctuation or symbols. ([};"!$=)

1.3.2.6. At a minimum, user passwords must be at least **8** characters long.

- The password must not contain the user's e-mail name, user ID or the full name as shown in the domain registry.
- New passwords shall never be the same as any of the last 3 passwords.
- The password must not contain dictionary words from any language because numerous password-cracking programs exist that can run through millions of possible word combinations in seconds. Simply adding a

number onto the end of a word is not sufficient. The numeric and/or special characters should be integrated into the password. However, a complex password that cannot be broken is useless if you cannot remember it. For security to function, you must choose a password you can remember and yet is complex. For example, Msi5!Yold (My son is 5 years old) or IhliCf5#yN (I have lived in California for 5 years now).

- Passwords must be stored in irreversible encrypted form and the password file cannot be viewed in unencrypted form.
- A password must not be displayed on the data entry/display device.
- Operating systems, systems software, and other systems at high risk of compromise are sometimes installed with a standard set of default accounts and associated standard passwords. Like all accounts, these access routes must be protected by strong passwords. Additional measures, such as disabling, renaming, or decoying these standard accounts, will be employed.
- During the first instance of access with a new account, the initial password must be changed by the individual responsible for the account, in compliance with the password controls defined in this policy.
- The proper and secure use of passwords must be included in user training.

1.3.2.7. If system-supplied password generation is available, it must enforce the above requirements and also include the following additional features:

- The system will give the user a choice of alternative passwords from which to choose.
- Passwords will be reasonably resistant to brute-force password guessing attacks.
- The generated sequence of passwords will have the property of randomness (i.e., consecutive instances shall be uncorrelated and the sequences shall not display within a predictable time period).

1.3.3. **Access Control/Authorization_**- Access is the ability to perform a function with a computer resource (e.g., use, change, or view). Access controls are the system-based means by which the ability is explicitly enabled or restricted in some way. Access controls can prescribe not only who (a user) or what (a process) is to have access to a specific system resource, but also the level of access that is permitted.

1.3.3.1. The Division of Information Technology must establish a process to authorize and document access privileges based on a legitimate and demonstrated need to have system access.

1.3.3.2. Access privilege documentation must be maintained in a manner that makes it easily retrievable by individual user account.

1.3.3.3. Prior to initial account distribution, positive identification of individuals receiving accounts must be conducted. Positive physical identification can be done by anyone the system administrator can trust to perform this task. For example, if an employee needs access to a system located off-site, the employee's supervisor can make positive physical identification of the employee and request access via electronic mail. During the first instance of access with a new account, the initial password must be changed by the individual responsible for the account, in compliance with the password controls defined in this policy.

1.3.3.4. When system users are no longer part of an organization, or their duties change, their account access must be appropriately modified or terminated. Requests to change access privileges must be signed and forwarded to the appropriate designated individual by the responsible manager.

1.3.3.4.1. The default "Guest" account on servers and workstations will be disabled. Use of Guest-type accounts is strongly discouraged but, if needed, these accounts must conform to the naming conventions and the password policy established in this policy.

1.3.3.4.2. The State IT organization must control access to resources based on the following access criteria, as appropriate:

- *Identity* (user ID). The identity must be unique in order to support individual accountability.
- *Roles.* Access to information must also be controlled by the job assignment or function (i.e., the role) of the user who is seeking access.
- *Location.* Access to particular system resources will be based upon physical or logical location.

- Access would be denied for a sixth user, even if the user were otherwise authorized to use the application.

- *Access Modes.* The State IT Organizations will consider the types of access, or access modes. Common access modes, which can be used in both operating and application systems, include read, write, execute, and delete.

1.3.3.5. **Access Control Mechanisms:** The State IT Organization must implement both internal and external access control mechanisms. *Internal* access controls are a logical means of separating what defined users (or user groups) can or cannot do with system resources. *External* access controls are a means of controlling interactions between the system and outside people, systems, and services. When setting up access controls, the State IT organization shall incorporate the following mechanisms where appropriate and applicable:

- *Access Control Lists (ACLs).* ACLs are a register of users (including groups, machines, and processes) who have been given permission to use a particular system resource and the types of access they have been permitted. The State IT Organizations will maintain Access Control Lists and establish a procedure to identity and remove users who have left the organization or whose duties no longer require access to the application. Access Control Lists will be reviewed regularly.

- *Constrained User Interfaces.* The State IT Organizations will restrict access to specific functions by never allowing users to request information, functions, or other resources for which they do not have access.

- *Encryption.* Encrypted information can only be decrypted, and therefore read, by those possessing the appropriate cryptographic key. While encryption can provide strong access control, it is accompanied by the need for strong key management. Encryption will be utilized where appropriate and required.

- *Port Protection Devices.* Fitted to a communications port of a host computer, a port protection device (PPD) authorizes access to the port itself, often based on a separate authentication (such as a dial-back modem) independent of the computer's own access control functions.

- *Secure Gateways/Firewalls.* Secure gateways block or filter access between two networks (e.g. Intranet, Internet, State partners, contractors, vendors, and other state agencies). Secure gateways allow internal users to connect to external networks while protecting internal systems from compromise. Additional information and requirements regarding gateways and firewalls are contained in the "Network" Chapter of this Handbook and on the State's Information Security web site.
- *Host-Based Authentication.* Host-based authentication grants access based upon the identity of the host originating the request, instead of the identity of the user making the request. The State IT Organization shall use network applications utilizing host-based authentication where appropriate and required.
- *System Log-On Banner.* A security log on banner shall be incorporated on all networked systems. This is displayed to users as part of the log on dialogue, followed by a pause requiring manual intervention to continue. The State Log-on banner displayed each time a user logs on to the State Log-on Banner is a reminder that any use of the State information technology resources is made with the understanding that such use is generally not secure, is not private, and is not anonymous.

WELCOME TO THE DEPARTMENT of ADMINISTRATION

This is a State of Rhode Island system operated and maintained by the Department Of Administration, Division of Information Technology. We encourage you, as a Department employee, researcher, contractor, or member of the public, to use this system. You should not expect privacy while using this system and your activity may be monitored to protect the system from unauthorized use. Authorized employees have the right to examine active and stored email and files within all systems. By using this system you expressly consent to such monitoring and to reporting your unauthorized use to the proper authorities. Unauthorized use of this system and/or unauthorized access may be prosecuted to the full extent of the law.

1.3.4. *Audit Trails* - Audit trails maintain a record of system activity by system or application processes and by user activity. In conjunction with appropriate tools and procedures, audit trails provide a means to help accomplish several security-related objectives, including individual accountability, reconstruction of events, intrusion detection, and problem identification.

1.3.4.1. The State IT Organization audit trails will be used for the following:

- Individual Accountability. The audit trail supports accountability by providing a trace of user actions. While users cannot be prevented from using resources to which they have legitimate access authorization, audit trail analysis can be used to examine their actions.
- Reconstruction of Events. The Department will use audit trails to support after-the fact investigations of how, when, and why normal operations ceased.
- Intrusion Detection/Prevention. The State IT Organization will design and implement their audit trails to record appropriate information to assist in intrusion detection. Intrusions can be detected in real time, by examining audit trails as they are created or after the fact, by examining audit records in a batch process.
- Problem Identification. The State IT Organization will use audit trails as online tools to help identify problems other than intrusions as they occur. This is often referred to as real-time auditing or monitoring.
- The CISO must be notified of all investigative audits of IT resources.

1.3.4.2. **Contents of Audit Trail Records:** An audit trail must include sufficient information to establish what event occurred and who (or what) caused them. The scope and contents of the audit trail will balance security needs with performance needs, privacy, and costs. At a minimum the event record must specify:

- Type of event
- When the event occurred (time and day)
- User ID associated with the event
- Program or command used to initiate the event

1.3.4.3. **Audit Trail Security:** The State IT Organization will protect the audit trail from unauthorized access. The following precautions will be taken:

- Control online audit logs. Access to online audit logs will be strictly controlled.

- Separation of duties. The State IT Organizations will ensure separation of duties between security personnel who administer the access control function and those who administer the audit trail.

- Protect confidentiality. The State offices and facilities will ensure the confidentiality of audit trail information.

1.3.4.4. Audit Trail Reviews. Audit trails will be maintained, at a minimum, for six months. The following must be considered when reviewing audit trails:

- Recognize normal activity. Reviewers must know what to look for to be effective in identifying unusual activity. They need to understand what normal activity looks like.

- Utilize a search capability. Audit trail review can be easier if the audit trail function can be queried by user ID, device ID, application name, date and time, or some other set of parameters to run reports of selected information.

- Follow-up reviews. The appropriate system administrator will review the audit trails following a known system or application software problem, a known violation of existing requirements by a user, or some unexplained system or user problem.

- Develop review guidelines. Application owners, data owners, system administrators, and the CISO will determine how much review of audit trail records is necessary, based on the importance of identifying unauthorized activities.

1.3.4.5. Automated tools. Traditionally, audit trails are analyzed in a batch mode at regular intervals (e.g., daily). Audit analysis tools, such as those based on audit reduction, attack signature, and variance techniques, can be utilized in real-time or near real-time fashion. the State IT Organizations should use the many types of tools that have been developed to help reduce the amount of information contained in audit trails, as well as to distill useful information from the raw data.

1.3.4.6. All the State information systems must have the ability to audit password activity, specifically when and who last changed a password, and when and who last changed account privileges.

1.3.4.7. Annually, individual accounts must be audited to ensure compliance with the minimum standards outlined in this policy.

1.3.5. The State IT systems that cannot meet these minimum standards must be modified to remedy any deficiencies. Until such time as deficient systems are brought up to these security standards, system owners, as part of their DOIT mandated security plans and risk assessments, must accept in writing any risk to the State infrastructure.

1.4. RESPONSIBILITIES

1.4.1. **The State CIO:** Ensures that the provisions of this chapter are implemented at all agencies within the State.

1.4.2. **Agency Directors:** Ensure that adequate technical security controls are implemented on all systems for which they hold responsibility.

1.4.3. **The Agency Manager:**

1.4.3.1. Certifies the systems under their control. The technical controls must be in place and functioning as intended, prior to certification of the system.

1.4.3.2. Ensures that during the development and acquisition phase of developing local systems that security requirements and specifications are incorporated into any purchase of automated information systems.

1.4.4. **System administrators**:

1.4.4.1. Ensures that the technical controls are functioning as expected and report any significant discrepancies noted to the CISO.

1.4.4.2. Monitors the system by reviewing system logs and utilizing various automated tools such as virus scanners, check-summing, password crackers, integrity verification programs, intrusion detectors, and system performance monitoring.

1.4.4.3. Evaluates account and password management controls yearly to ensure that the State password policy is being technically implemented.

1.4.4.4. Ensures that the CISO is notified of all investigative audits of IT systems.

1.4.5. **CISO/ACISO**:

1.4.5.1. Assists the State CIO in performing sensitivity assessments and in determining security requirements and specifications for technical controls in any new systems to be purchased and operated at the facility.

1.4.5.2. Audits the technical controls. This can be accomplished by conducting regular audits of the system. The CISO must work with the system manager and the State CIO in developing effective measures to audit the various systems in a facility.

1.4.5.3. Develops procedures and policy concerning authorizing and documenting access privileges for users based on a legitimate and demonstrated need to have system access.

1.4.6. **Individual users:** Select strong passwords in accordance with this policy.

2. SOFTWARE AND DATA SECURITY

2.1.PURPOSE

2.1.1. This chapter provides security guidance on software selection, development, testing, implementation and maintenance of State of Rhode Island software.

2.1.2. Security controls for operating system and application software are detailed below and are applicable to all software (the State developed and Commercial Off-The-Shelf (COTS)) used in the State IT resources.

2.2.BACKGROUND

2.2.1. The State currently buys COTS software. Security controls must be met in these circumstances to ensure that mission critical and all other sensitive data is established, maintained, transported and utilized in a secure manner.

2.3.POLICY

2.3.1. General Software Security Elements are:

2.3.1.1. Controlling what software is used on a system

- All COTS application software purchases must be certified and accredited prior to use.
- Application software used on the State IT resources must be obtained through authorized procurement channels.
- Each system installation of the State developed or off-the-shelf software must be reviewed and approved by the review board prior to installation. This also includes software acquired by any other means (e.g., public domain software, bulletin board services, personally owned software, Internet obtainable freeware). All application software authorized to run on the State IT resource must be identified in the system's security plan.

2.3.1.2. Ensuring that software has not been modified without proper authorization

- Willful and intentional modification of the State software for illegal or disruptive purposes or for personal gain is a crime. There must not be any modifications of these programs except by an authorized agent of the CIO.
- Safeguards must be in place to detect and minimize inadvertent or malicious modification or destruction, or attempts to do so, of the State's IT application software, operating system software, and critical data files.
- The safeguards should achieve the integrity objectives and be documented in the system's security plan. The level of protection must be commensurate with the sensitivity of the information processed.
- Approved software, regardless of source, must be scanned for viruses prior to initial use.
- Anti-Virus and malicious code (software) must be employed on every the State IT resource to protect the integrity of the software and data.

2.3.1.3. Ensuring that software is properly licensed, as required

- Use of copyrighted software will comply with copyright laws and license agreements.
- The State licensed software may not be installed on other systems without management approval (e.g. anti-virus software).

2.3.2. **Operating System Software Controls**: The operating system software employed to process data by multiple users, including local area networks, must control user access to resources and capabilities that are required and authorized. The operating system software should also have the capability to identify, journal, report, and assign accountability for the functions performed or attempted by a user and to deny user access to capabilities or resources that have not been authorized. At a minimum, the operating system must:

2.3.2.1. Control all transfers between memory and on-line storage devices between a central computer and remote devices and between on-line storage devices.

2.3.2.2. Control all operations associated with allocating system resources (e.g. memory, peripheral devices, etc.), memory protection, system interrupts and changes between the privileged and non-privileged states.

2.3.2.3. Identify a valid system user and direct the user to authorized options or applications. Use of such a feature (log-on dialogue) limits user access and protects system programs and data files from unauthorized access.

2.3.2.4. Provide the capability to limit the types of operations (e.g., read, write, and delete) that can be performed by individual users on given data or program files.

2.3.2.5. Control system access through an approved form of user authentication.

2.3.2.6. Provide the capability to record actual or attempted access to the system and other activity.

2.3.2.7. Provide the capability to terminate a process automatically and log-off a user when an access session remains inactive for some specified length of time.

2.3.2.8. Provide the capability upon a break of connection or a log-off to terminate an access session.

2.3.2.9. Control programs or utilities which may be used to maintain and/or modify the operating system, access control systems, sensitive databases and other software modules which could affect or compromise the integrity of the general purpose software or sensitive applications.

2.3.2.10. Prevent a user program from executing privileged instructions.

2.3.2.11. Isolate the programs and data areas of one user from those of other users and the operating system software.

2.3.2.12. Assure error detection when accessing memory as well as parity and hardware register checking.

2.3.2.13. Cause a screen warning message to be displayed at logon to identify to the user that access is restricted to authorized users for legitimate purposes only and that their activities are subject to monitoring.

2.3.2.14. Be maintained by the minimum number of authorized persons. This is accomplished by limiting the number of employees with administrative privileges.

2.3.2.15. Be copied after each modification with the copy to be immediately stored as a backup for emergency use.

2.3.3. **Application Software Controls:** An application that processes sensitive data, or requires protections because of the risk and magnitude of loss or harm that could result from improper operation, manipulation or disclosure must be provided protection appropriate to its sensitivity. The following will be considered as the minimum controls to be applied to sensitive applications, with additional controls or safeguards to be imposed if appropriate:

2.3.3.1. The State approved security requirements and specifications will be defined prior to acquiring or starting development of applications, or prior to making a substantial change to the existing application.

2.3.3.2. Design reviews will be conducted at periodic intervals during the developmental process to assure that the proposed design will satisfy the functional and security requirements specified.

2.3.3.3. New or substantially modified sensitive applications must be thoroughly tested prior to implementation to verify that the user functions and the required administrative, technical, and physical safeguards are present and are operationally adequate. This is to be accomplished as part of the certification and accreditation process.

2.3.3.4. Sensitive data or files will not be used to test applications software until software integrity has been reasonably assured by testing with non-sensitive data or files.

2.3.3.5. Sensitive application software will not be placed in a production status until the system tests have been successfully completed and the application has been properly certified and accredited. Prototypes that process production data must be certified and accredited before they are deployed or implemented.

2.3.3.6. Current backup copies of critical application software, documentation, data bases and other resources required for its operation, will be maintained and be readily available for use in the event of an emergency.

2.3.3.7. Sensitive applications will be re-certified every three years or following major changes.

2.3.3.8. Sensitive software documentation must be provided the same degree of protection as that provided for the software.

2.3.4. **Software Security Implementation Procedures**. Software designed to provide information security is limited by the effectiveness of the procedures implemented to support it. Procedural issues, which relate to the use of the system software and which should be addressed, are as follows:

2.3.4.1. A minimum length of eight characters is required for passwords. The minimum length will be software controlled.

2.3.4.2. Default User Accounts. Operating systems are sometimes installed with a standard set of default user accounts and associated standard security passwords. The access route shall be protected by either disabling the standard user account or by changing the passwords.

2.3.4.3. All security problem fix software, patches, command scripts, and the like provided by vendors, official computer emergency response teams (CERTs), and other trusted third parties must be promptly installed and documented.

2.3.5. **Processing Environments:** The State automated information systems use several processing environments that meet the specific and varied needs of users. Following are descriptions of processing environments and the unique information security aspects related to them:

2.3.5.1. Production environment is the environment for the processing of official data utilized in support of office and facility missions and management. Information security procedures for production environments must specifically address controls for:

- Viewing, modifying, downloading or deleting production system data and programs
- Generation and disposition of outputs
- Tracking production program version changes (maintenance of a software update history log is required under configuration

management discussed in Chapter 4 of the State Operational Controls Handbook)

- Access to the computer and its peripheral devices

2.3.5.2. Development and Verification is the environment for the development, testing, and verification of program code for the maintenance, modification or enhancement of existing applications, or the development of new applications. Information security procedures for this environment must specifically address controls for:

- Viewing, modifying, or deleting test data
- Creating, viewing, modifying, or deleting development programs
- Generation and disposition of outputs
- Transfer of application programs and data files from the development and verification environment to the production environment
- The computer system and its peripheral and telecommunication devices

2.3.5.3. Demonstration and/or Training enables use of system or application software functions in an on-line mode (using production or development computer resources) without affecting the production or development environments. The demonstration and/or training environment must simulate on a demonstration or training disk, the production environment and use non-sensitive data to test, train, or demonstrate the system. Information security procedures for this environment must specifically address:

- Protecting production and development system programs and data files
- Accessing the "Demonstration" account by the general public (other than the State staff)
- Limiting user access to only those capabilities necessary to utilize the demonstration programs
- Limiting access to the computer and its peripheral and communications devices
- Generic access codes may be used to enter the "Demonstration" environment and is the only exception to the mandated requirement for individual password codes

2.4. *RESPONSIBILITIES*

2.4.1. **State Software Developers**:

2.4.1.1. Ensure that security controls are incorporated in the design, development, and testing of contractor-developed software.

2.4.1.2. Ensure that the State developed application software and patches are certified prior to release to the State.

2.4.2. **State CIO, Technical Services, or designee**:

2.4.2.1. Accredit all the State software and patches prior to release to the State

2.4.2.2. Ensure that all the State IT Organizations are in compliance with the policy outlined in this chapter.

2.4.3. **Office Heads, and Facility Directors:** Ensure that adequate application security controls on locally purchased application software are implemented at their sites.

2.4.4. **Agency Manager**:

2.4.4.1. Ensures that the operating system and application software security controls on all software used throughout the State meet the agency requirements.

2.4.4.2. Ensures that any COTS applications purchased by offices and regional facilities meet the State security controls.

2.4.5. **System administrators**:

2.4.5.1. Maintain the software utilized on their systems.

2.4.5.2. Ensure that the operating system and application software controls are operating as intended on the systems under their responsibility.

2.4.5.3. Install all problem fix software, patches, command strips on appropriate systems in a timely manner.

2.4.6. **CISO/ACISO**:

2.4.6.1. Ensure that locally procured software has been approved by the review board and certified and accredited by the office head or facility director.

2.4.6.2. Audit to ensure that software (application and operating system) controls are in place and functioning as designed.

3. NETWORK AND COMMUNICATION SECURITY

3.1.PURPOSE

3.1.1. This chapter provides guidance and policy related to network and communication security for the State sites. Independent Internet gateways, electronic mail, facsimile (fax) transmissions, local areas networks (LANs), and wide area networks (WANs) need security controls established to ensure the confidentiality, integrity, and availability of the data being transmitted.

3.1.2. The policy contained in this chapter covers all the State IT resources maintained in-house or in the interest of the State. These policies are mandatory on all organizational units, employees, contractors, and others having access to and/or using the IT resources of the State.

3.1.3. This policy applies to all the State automated information systems processing sensitive data currently in existence and any new automated technology acquired after the effective date of this policy document.

3.2. BACKGROUND

3.2.1. Network security is not any different from single host security in terms of confidentiality, integrity, and availability of resources. The real difference in providing basic security services occurs because of the increased complexity of the networked environment. Providing confidentiality of information, for example, is difficult enough when the entire system resides in a single room. Consider the implications of allowing access to information from multiple locations both inside and outside of the State. Security for a single host is generally the responsibility of a single individual. In a networked environment, the security of individual systems is the responsibility of numerous individuals. Intruders to networks continually count on finding a single weak link in the network chain that will then allow them access to the rest of the network. Network security measures must account for this, as well as other complexities, in an attempt to maintain the security of the network data and resources.

3.3. POLICY

3.3.1. **General Network Policy**

The State IT safeguards must ensure the privacy of sensitive information during storage, processing, and transmission.

3.3.1.1. The State users will be granted access to the State networks based upon duty requirements and the need to access resources.

3.3.1.2. The State IT Organizations will implement the necessary mechanisms and procedures to protect information processed on networks, to include:

- Maintaining a record of authorized users of a network and their network privileges and reviewing this record on a regular basis to ensure that access to the network is limited to only those individuals with a justified need.
- Ensuring that all networks are certified and accredited. (See Management Controls Handbook for details)
- Ensuring that computer systems are configured to terminate a user process if that user-network connectivity is interrupted before a proper log out.
- Ensuring that the network and systems automatically terminate sessions after periods of inactivity.
- Establishing individual accounts for each user on the network. "Generic accounts" that allow users access to network resources anonymously, are prohibited.
- Establishing formal reporting procedures for unexpected events and activity.

3.3.2. **External Connections**. An external connection is any connection (not just an Internet connection) from an outside network (a source other than the State) that is electronically linked to a system or network that is owned or operated by or in behalf of the State.

3.3.2.1. External connections must incorporate adequate controls to safeguard the State IT resources.

3.3.2.2. At a minimum, all external connections must incorporate a firewall. Network firewalls are devices used to protect a trusted computer network from an untrusted one.

3.3.2.3. The State policy has established the following as the minimum specifications for a firewall:

3.3.2.3.1. Configuration and Installation:

- Activate the minimum set of operating system services to support firewall operation. Activate no other operating system services.
- Configure the firewall computer's operating system with all current patches and updates to known exploits.
- Support high availability configurations and load balancing through integrated capabilities or by integration of third party products.
- Configure the firewall so that it cannot be identifiable as such to other network(s), or, at most, appears to be just another router.
- Disguise or hide internal Domain Name Systems (DNS) to prevent direct external requests.
- Ignore service requests like "echo" or "chargen" that could be used in a denial of service attack.
- Prevent network connections from bypassing the firewall.
- Be installed in locations that are physically secure from tampering.

3.3.2.3.2. Access Management:

- Restrict use of a particular application only to customers authorized to access the application.
- Implement a "deny all services except those specifically permitted" design policy.
- Implement two-factor authentication for administrative log-in to permit secure remote log-in by the authorized system administrator.
- Support integration of external authentication databases, such as RADIUS or LDAP.
- Employ techniques such as content filtering to permit or deny services to specific external hosts, such as web sites that the State staffs are restricted from accessing.

- Incorporate and operate a systematic method of intrusion detection/prevention. Data from intrusion detection/prevension must be stored such that it can serve as evidence in forensic investigations.

3.3.2.3.3. Auditing and Filtering

- Log access to and through the firewall.
- Capture log-in attempts by authorized and unauthorized users.
- Employ a flexible, user-friendly IP-filtering language that is easy to program and can filter on a wide variety of attributes, including source and destination IP addresses, protocol types, port numbers, and inbound and outbound interfaces.
- Screen data coming through the firewall.
- Concentrate, filter, and log dial-in and VPN access.
- Generate an audit trail of calls passing through the firewall for review of security anomalies at future times.
- Support third-party products for log analysis and data reduction. **Notification**

3.3.2.4. Provide notification of threats, including unsolicited distribution of executable files, and notification of efforts by accepted users to gain access to systems or applications that they do not have permission to enter.

3.3.2.5. Generate alarms, predicated on the occurrence of a specific event or combination of events, on a timely basis (e.g., within 60 seconds) after the event occurs.

3.3.3. **Future Security Enhancements**

3.3.3.1. Accommodate new services and needs to allow for changes in the State and the State security policy.

3.3.3.2. Contain advanced authentication measures, or the hooks for installing advanced authentication measures, if strong authentication for inbound access is required.

3.3.3.3. External connections must be accredited prior to use.

3.3.3.4. External connections will be periodically independently reviewed by an organization other than that which sponsors the use and administration of the external connection. These reviews will be conducted when there is significant change to the protected asset, or at least every other year after initial accreditation. These reviews will ensure that external connections remain in compliance with the minimum security standards outlined in this policy, and will ensure that risk assessments, security plans, and contingency plans remain current.

3.3.3.5. Where user access originates from outside the internal the State protected network, all users must be identified and authenticated at the gateway prior to being granted access to internal resources.

3.3.3.6. Where sensitive data is to be accessed from or through untrusted networks, the entire session must be encrypted.

3.3.4. **Internet/Public Access**

3.3.4.1. There are several methods available for connecting to the Internet system. They include, but are not limited to purchasing a commercial service, establishing an independent gateway or connecting through the State Internet Gateways.

3.3.4.2. The Division of IT (DOIT) Internet Gateway has been established as a common resource for all the State IT Organizations to use. The DOIT Internet Gateway is provided to support information sharing, research, and education in and among the State IT Organizations, research and instructional institutions, and other government agencies and commercial services. Use of the DOIT Internet Gateway is mandatory.

3.3.4.3. Those sites with their own connection to the Internet or to other networks external to the State (i.e., universities, vendors, other state government agencies) must meet all of the security requirements established by the DOIT

3.3.4.4. The State must approve external connections prior to operation.

3.3.4.5. The State employees are expected to conduct themselves professionally in the workplace and must not use the Internet for activities that are inappropriate or offensive to co-workers or the public. Such activities include playing electronic games, or accessing sexually explicit materials or materials that ridicule others on the basis of race, creed, religion, color, sex, disability, national origin or sexual orientation.

3.3.4.6. Employees must ensure that all sites accessed have no cost attached. For example, a prompt to enter a special password or to register prior to entering the database may indicate that it is fee-based.

3.3.4.7. Government-issued credit cards must not be used for personal access to the Internet, or to purchase items from the Internet for personal use.

3.3.4.8. Employees must not use dial-out modems to connect to commercial Internet service providers, such as America Online. If exceptions are required, approval must be obtained from senior management.

3.3.4.9. Employees using the State resources to access the Internet are subject to monitoring. Incidents of inappropriate access will be reported to supervisors and the CISO for disciplinary action.

3.3.4.10. All software and files downloaded from non-the State sources via the Internet (or any other public network) must be screened with virus detection software. The screening must take place prior to being run or examined via another program such as a word processing package.

3.3.4.11. All public access systems will be located outside the internal the State network.

3.3.4.12. Systems that are exposed to the Internet, such as the State public access systems, will not be permitted direct access to the internal the State network.

3.3.5. **Modem communications**

3.3.5.1. Data communication connections via modems are to be limited and tightly controlled as they pose a serious risk that can circumvent security controls intended to protect the State networks from external, "untrusted" networks.

3.3.5.2. Employees are prohibited from connecting dial-up modems to the State workstations that are simultaneously connected to the State network or another internal communication network.

3.3.5.3. Remote users (telecommuters and employees on travel) dialing into the State systems must be routed through a modem pool that includes an approved extended user authentication security system.

3.3.5.4. Reliable and confidential hardware and software authentication systems are to be incorporated into the State approved communication servers. Positive authentication is to be established prior to granting access to network resources.

3.3.5.5. Event logging functions are to be provided to enable a review of suspicious activities.

3.3.5.6. Controls are required for remote access to the State systems. A log will be maintained and reviewed quarterly of individuals granted remote access to ensure that accountability is maintained.

3.3.6. **Electronic Mail** (email)

3.3.6.1. Only authorized email software may be used.

3.3.6.2. The State employees who utilize email systems will do so with the understanding that they have no expectation of personal privacy relating to that use.

3.3.6.3. When appropriately authorized by management, electronic mail messages flowing through the State systems may be monitored for internal policy compliance, suspected criminal activity, and other systems management reasons.

3.3.6.4. The State users are prohibited from sending or forwarding any messages via the State's information systems that a reasonable person would consider to be defamatory, harassing, or explicitly sexual. Employees are also prohibited from sending or forwarding messages or images via the State systems that would be likely to offend on the basis of race, gender, national origin, sexual orientation, religion, political beliefs, or disability.

3.3.6.5. When employees receive unwanted and unsolicited e-mail (also known as SPAM), they must refrain from responding directly to the sender. Instead, forward the message to the email administrator who will take steps to prevent further transmission.

3.3.6.6. The State projects and commercial products for secure electronic mail (email) systems are undergoing rapid development and will be available in the near future. Until such products are implemented, users must not send sensitive information via email.

3.3.6.7. The State system administrators establish and maintain a systematic process for the retention and destruction of electronic mail messages and accompanying logs.

3.3.6.8. Users must regularly move important information from electronic mail message files to word processing documents, databases, and other files. Electronic mail systems are not intended for the archival storage of important information. Stored electronic mail messages are periodically expunged by system administrators, mistakenly erased by users, and otherwise lost when system problems occur.

3.3.7. Telecommuting Security

3.3.7.1. The security of the State property at an alternative work site (i.e., home, hotel, etc.) is just as important as it is at the State IT Organization. At alternative work sites, reasonable precautions must be taken to protect the State hardware, software, and information from theft, damage, and misuse.

3.3.7.2. Users must not discard sensitive information at home, in hotel wastebaskets or other publicly accessible trash containers. Instead, sensitive information must be retained until it can be shredded, or destroyed by other approved methods.

3.3.7.3. Telecommuters must ensure that the systems they utilize remotely maintain the current anti-virus software.

3.3.7.4. Remote users should not maintain sensitive data on their systems unless adequately secured via encryption or authenticated access control mechanisms. This is especially important if the system is also used to connect to the Internet.

3.3.7.5. Telecommuters must use the password facility in their screen saver.

3.3.7.6. Only authorized telecommuters will be given access to the State's networks. Managers must take steps to ensure that telecommuting employees do not compromise the integrity of the State systems.

3.3.7.7. Telecommuters must be authenticated prior to access to the State's network. Where possible, user access should be limited to specific systems specified during the log-in process.

3.3.7.8. Sensitive data should not be transmitted unless appropriately secured via encryption.

3.3.7.9. Employees are responsible for the integrity and confidentiality of the data on remote systems. Access controls must be in place to protect the State systems and electronic information located at remote sites (i.e., home, telecommuting work locations, hotels and convention centers).

3.3.8. Facsimile (fax) transmission

3.3.8.1. Sensitive information will only be transmitted via a secure facsimile system (e.g., encrypted or via a protected network). Commercial-off-the-shelf (COTS) software and hardware are available to provide the necessary safeguards and should be employed as appropriate.

3.3.8.2. Each office and facility should develop policies and procedures to protect privacy while transmitting information via facsimile. The policy and procedures must:

- Limit use to urgent situations
- Ensure appropriate location of facsimile machines

- Assign accountability for managing each facsimile machine
- Define appropriate safeguards to ensure transmissions are sent to the appropriate individual
- Define procedures for cases of misdirected transmissions and receipts
- Routine disclosure of information should be made through regular mail or courier
- Auto-faxing, which allows automatic facsimile transmission of reports, should be set up carefully to ensure that they are necessary and that correct facsimile numbers are contained in the system
- A cover letter should accompany each transmission and include:
    - Date/time transmission
    - Sending facility's name, address, telephone and facsimile numbers
    - Authorized receiver's name
    - Number of pages transmitted
    - Confidentiality notice, including instructions on re-disclosure and destruction

3.3.8.3. A procedure must be developed to cover instances when a site is notified that a fax was received by other than the intended recipient. The internal logging system of the facsimile machine should be checked to obtain the number to which the transmission was sent in error. If the number was incorrect a facsimile should be sent to that number explaining that the information was misdirected and ask for the documents to be returned by mail to the sending facility.

3.3.8.4. A procedure must be developed regarding the receipt of facsimile documents containing sensitive information. The procedure should address the following areas:

- Accountability for monitoring the facsimile machine. A fax machine must be located in a secure, controlled area.
- Ensuring the removal of documents promptly
- Checking for completeness and legibility of received information

- Notifying senders of transmission problems
- Following the instructions on the cover page
- Arranging for secure delivery of the documents

3.3.9. PBX (Telephone) Security

3.3.9.1. Keep PBX attendant console rooms, telephone wiring closets, telephone equipment rooms, and Local Exchange Company (LEC) demarcation rooms locked and secured. These rooms shall meet the same physical security requirements as outlined in the State's Operations Handbook, Chapter 5 "Physical/Environmental Security."

3.3.9.2. Request positive identification from all service equipment vendors and technicians.

3.3.9.3. Ensure that any remote maintenance line phone number is unpublished, preferably not in the same numbers groups, and not recorded on jacks, wall field, distribution frame, etc.

3.3.9.4. Secure any reports, documentation, or other information files that may reveal the trunk access codes or passwords.

3.3.9.5. Change all default passwords immediately after installation.

3.3.9.6. Choose passwords that meet the requirements as outlined in Chapter 1 "Technical Security" of this Handbook.

3.3.9.7. Deactivate unused codes and features.

3.3.9.8. Allow only three attempts to enter a valid access code.

3.3.9.9. Have the PBX wait four or five rings before answering the remote access line.

3.3.9.10. Restrict calling privileges to individual employees

3.3.9.11. Block area codes where business is not done, especially 900, 700, and 976.

3.3.9.12. Use the maximum authorization and Remote Access barrier code length.

3.3.9.13. Use security devices on all ports.

3.3.9.14. Ensure that all unused ports are disconnected from the system.

3.3.10. **Voice Mail**

3.3.10.1. Don't allow outgoing calls from a mailbox.

3.3.10.2. Block access to long distance trunks or local lines.

3.3.10.3. Toll restrict lines between the voice mail system and PBX.

3.3.10.4. Delete all unused voice mailboxes.

3.4.RESPONSIBILITIES

3.4.1. **The State CIO** Ensures that all IT systems in the State Government are in compliance with the technical policy outlined in this chapter.

3.4.2. **Department Directors**:

3.4.2.1. Ensure that the security technical controls are established on all the systems at their departments.

3.4.2.2. Accredit all systems implementing external connections initiated from the site to non-the Department sources.

3.4.2.3. Prior to implementation, ensure that the review board has approved all external connections initiating from the site that connects the State's network with an external non-State network.

3.4.3. **Agency Managers**:

3.4.3.1. Ensures that the security technical controls outlined in this chapter are implemented on the State IT resources.

3.4.3.2. Ensures that all systems implementing external connections from the site to non-the State sources are secure and certified.

3.4.3.3. Ensures that all external connections from the State's network to non-the State networks meet the State security criteria and receive final approved of the review board prior to accreditation by the CIO.

3.4.3.4. Ensures that all systems implementing external connections from the site to non-the State sources are accredited prior to operation.

3.4.3.5. Ensures that all external connections are re-certified and accredited every other year after initial accreditation.

3.4.3.6. Ensures that all dial-up modems are justified and approved prior to use.

3.4.4. **CISO/ACISO**:

3.4.4.1. Maintains a record of authorized users of a network and their network privileges. This may be delegated to the review board if appropriate.

3.4.4.2. Reviews this record on a regular basis to ensure that access to the network is limited to only those individuals with a justified need.

3.4.4.3. Work with the system administrators and the CIO to ensure that all systems are certified and accredited.

3.4.4.4. Conducts audits to ensure that technical controls are implemented and performing as required.

4. APPENDIX A

4.1. ACRONYMS

ACL	Access Control List
ACISO	Alternate Chief Information Security Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
COTS	Commercial Off-The- Shelf
DOD	Department of Defense
DNS	Domain Name Systems
EMAIL	Electronic Mail
FAX	Facsimile
IP	Internet Protocol
IRS	Internal Revenue Service
ISO	Information Security Officer
IT	Information Technology
LAN	Local Area Network
LEC	Local Exchange Company
PBX	Private Branch Exchange
PIN	Personal Identification Number
PPD	Port Protection Device
SAM	Security Account Manager
SSA	Social Security Administration
WAN	Wide Area Network

5. APPENDIX B

5.1. GLOSSARY

Access Control Security control designed to permit authorized access to an IT system or application.

Accreditation A formal declaration by the Agency Manager that the IT is approved to operate in a particular security mode using a prescribed set of safeguards. Accreditation is the official management authorization for operation of IT and is based on the certification process, as well as other management considerations. The accreditation statement affixes security responsibility with the Agency Manager and shows that due care has been taken for security.

Authentication Verification of the identity of a user, user device, or other entity, or the integrity of data stored, transmitted, or otherwise exposed to unauthorized modification in an IT.

Audit Trail A record showing who has accessed a computer system and what operations he or she has performed during a given period of time. Audit trails are useful both for maintaining security and for recovering lost transactions.

Automated Information System(s) (AIS) An assembly of computer hardware, software and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information.

Availability of Data The state when data are in the place needed by the user, at the time the user needs them, and in the form needed by the user.

Backup A copy of data and/or applications contained in the IT stored on magnetic media outside of the IT to be used in the event IT data are lost.

Certification The comprehensive evaluation of the technical and non-technical security features of an IT and other safeguards, made in support of the accreditation process that establishes the extent to which a particular design and implementation meet a specified set of security requirements.

Ciphertext

Form of cryptography in which the *plaintext* is made unintelligible to anyone, who intercepts it by a transformation of the information itself, based on some key.

Confidentiality

The concept of holding sensitive data in confidence limited to an appropriate set of individuals or organizations.

Configuration Management

The process of keeping track of changes to the system, if needed, approving them.

Contingency Plan

A plan for emergency response, backup operations, and post-disaster recovery maintained by an activity as a part of its security program that will ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation.

COTS Software

Commercial Off The Shelf Software – software acquired by government contract through a commercial vendor. This software is a standard product, not developed by a vendor for a particular government project.

Data Integrity

The state that exists when automated data is the same as that in source documents, or has been correctly computed from source data, and has not been exposed to alteration or destruction.

Degaussing Media

Method to magnetically erase data from magnetic tape.

Default

A value or setting that a device or program automatically selects if you do not specify a substitute.

Dial-up

The service whereby a computer terminal can use the telephone to initiate and effect communication with a computer.

Encryption The process of making information indecipherable to protect it from unauthorized viewing or use, especially during transmission or storage. Encryption is based on an algorithm and at least one key. Even if the algorithm is known, the information cannot be decrypted without the key(s).

Facsimile A document that has been sent, or is about to be sent, via a fax machine.

Firewall A system or combination of systems that enforces a boundary between two or more networks.

Friendly Termination The removal of an employee from the organization when there is no reason to believe that the termination is other than mutually acceptable.

Gateway A bridge between two networks.

Hardware Refers to objects that you can actually touch, like disks, disk drives, display screens, keyboards, printers, boards, and chips.

Identification The process that enables recognition of a user described to an IT.

Internet A global network connecting millions of computers. As of 1999, the Internet has more than 200 million users worldwide, and that number is growing rapidly.

Intranet A network based on TCP/IP protocols (an internet) belonging to an organization, usually a corporation, accessible only by the organization's members, employees, or others with authorization. An intranet's Web sites look and act just like any other Web sites, but the firewall surrounding an intranet fends off unauthorized access.

Intrusion Detection Pertaining to techniques, which attempt to detect intrusion into a computer or network by observation of actions, security logs, or audit data. Detection of break-ins or attempts either manually or via software expert systems that operate on logs or other information available on the network.

CISO/ACISO The persons responsible to the CIO for ensuring that security is provided for and implemented throughout the life cycle of an IT from the beginning of the concept development plan through its design, development, operation, maintenance, and secure disposal.

Issue-specific Policy Policies developed to focus on areas of current relevance and concern to an office or facility. Both new technologies and the appearance of new threats often require the creation of issue-specific policies (e.g., e-mail, Internet usage).

IT Security Measures and controls that protect an IT against denial of and unauthorized (accidental or intentional) disclosure, modification, or destruction of IT and data. IT security includes consideration of all hardware and/or software functions.

IT Security Policy The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.

IT Systems An assembly of computer hardware, software and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information.

LDAP Short for Lightweight Directory Access Protocol, a set of protocols for accessing information directories. LDAP is based on the standards contained within the X.500 standard, but is significantly simpler. And unlike X.500, LDAP supports TCP/IP, which is necessary for any type of Internet access.

Least Privilege The process of granting users only those accesses they need to perform their official duties.

Local Area Network A short-haul data communications systems that connects IT devices in a building or group of buildings within a few square miles, including (but not limited to) workstations, front-end processors, controllers, switches, and gateways.

Management Controls Security methods that focus on the management of the computer security system and the management of risk for a system.

Modem An electronic device that allows a microcomputer or a computer terminal to be connected to another computer via a telephone line.

Network Two or more systems connected by a communications medium; a network is composed of a communications medium and all components attached to that medium whose responsibility is the transference of information.

Operating System The most important program that runs on a computer. Every general-purpose computer must have an operating system to run other programs. Operating systems perform basic tasks, such as recognizing input from the keyboard, sending output to the display screen, keeping track of files and directories on the disk, and controlling peripheral devices such as disk drives and printers.

Operation Controls Security methods that focus on mechanisms that primarily are implemented and executed by people (as opposed to systems).

Overwriting media Method for clearing data from magnetic media. Overwriting uses a program to write (1s, Os, or a combination) onto the media. Overwriting should not be confused with merely deleting the pointer to a file (which typically happens when a “delete” command is used).

Password Protected/private character string used to authenticate an identity or to authorize access to data.

Parity

The quality of being either odd or even. The fact that all numbers have parity is commonly used in data communication to ensure the validity of data. This is called parity checking.

PBX

Short for private branch exchange, a private telephone network used within an enterprise. Users of the PBX share a certain number of outside lines for making telephone calls external to the PBX.

Peripheral Device

Any external device attached to a computer. Examples of peripherals include printers, disk drives, display monitors, keyboards, and mice.

Port

An interface on a computer to which you can connect a device.

Port Protection Device

A device that authorizes access to the port itself, often based on a separate authentication independent of the computer's own access control functions.

RADIUS

Short for Remote Authentication Dial-In User Service, an authentication and accounting system used by many Internet Service Providers (ISPs). When you dial in to the ISP you must enter your username and password. This information is passed to a RADIUS server, which checks that the information is correct, and then authorizes access to the ISP system.

Real Time

Occurring immediately. Real time can refer to events simulated by a computer at the same speed that they would occur in real life.

Remote Access

The hookup of a remote computing device via communication lines such as ordinary phone lines or wide area networks to access network applications and information

Risk
The probability that a particular threat will exploit a particular vulnerability of the system.

Risk Analysis
The process of identifying security risks, determining their magnitude, and identifying areas needing safeguards. Risk analysis is a part of risk management.

Risk Management
Process of identifying, controlling, and eliminating or reducing risks that may affect IT resources.

Router
An interconnection device that is similar to a bridge but serves packets or frames containing certain protocols. Routers link LANs at the network layer.

Rules of Behavior
Rules established and implemented concerning use of, security in, and acceptable level of risk for the system. Rules will clearly delineate responsibilities and expected behavior of all individuals with access to the system. Rules should cover such matters as work at home, dial-in access, connection to the Internet, use of copyrighted works, unofficial use of Federal Government equipment, the assignment and limitation of system privileges, and individual accountability.

Security Incident
An adverse event in a computer system or the threat of such an event occurring.

Security Plan
Document that details the security controls established and planned for a particular system.

Security Specifications
A detailed description of the safeguards required to protect a system.

Sensitive Data
Any information, the loss, misuse, modification of, or unauthorized access to, could affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, U.S. Code, but has not been specifically authorized under criteria established by an Executive order or an act of Congress to be kept classified in the interest of national defense or foreign policy.

Separation of Duties
A process that divides roles and responsibilities so that a single individual cannot subvert a critical process.

Server
The control computer on a local area network that controls software access to workstations, printers, and other parts of the network.

Smart Card
A credit-card-sized device with embedded microelectronics circuitry for storing information about an individual. This is not a key or token, as used in the remote access authentication process.

Software
Computer instructions or data. Anything that can be stored electronically is software.

Software Copyright
The right of the copyright owner to prohibit copying and/or issue permission for a customer to employ a particular computer program.

SPAM Process designed to crash a program by overrunning a fixed-site buffer with excessively large input data. Also, to cause a person or newsgroup to be flooded with irrelevant or inappropriate messages.

System Set of processes, communications, storage, and related resources that are under the same direct management control, have the same function or Mission objective, have essentially the same operating characteristics and security needs, and reside in the same general operating environment.

System Availability The state that exists when required automated information can be performed within an acceptable time period even under adverse circumstances.

System Integrity The quality that a system has when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

System Administrator The individual responsible for defining the system's operating parameters, authorized functions, and security requirements. This individual is usually the person who maintains the system on a day-to-day basis.

System Owner The individual who is ultimately responsible for the function and security of the system.

TCP/IP Transmission Control Protocol/Internet Protocol. The Internet Protocol is based on this suite of protocols.

Technical Controls Security methods consisting of hardware and software controls used to provide automated protection to the system or applications. Technical controls operate within the technical system and applications.

Technical Security Policy Specific protection conditions and/or protection philosophy that express the boundaries and responsibilities of the IT product in supporting the information protection policy control objectives and countering expected threats.

Telecommunications Any transmission, emission, or reception of signals, writing, images, sound or other data by cable, telephone lines, radio, visual or any electromagnetic system.

Threat Any circumstance or event with the potential to cause harm to a system in the form of destruction, disclosure, modification of data, and/or denial thereof.

Trojan Horse Any program designed to do things that the user of the program did not intend to do, or that disguise its harmful intent. A program that installs itself while the user is making an authorized entry; and, then is used to break-in and exploits the system.

Unfriendly Termination The removal of an employee under involuntary or adverse conditions. This may include termination for cause, RIF, involuntary transfer, resignation for "personality conflicts," and situations with pending grievances.

User Any person who is granted access privileges to a given IT.

User Interface The part of an application that the user works with. User interfaces can be text-driven, such as DOS, or graphical, such as Windows.

Virus A self-propagating Trojan horse (a program that surreptitiously exploits the security/integrity of a program), composed of a mission component, a trigger component, and a self-propagating component.

Vulnerability A weakness in automated system security procedures, technical controls, environmental controls, administrative controls, internal controls, etc., that could be used as an entry point to gain unauthorized access to information or disrupt critical processing.

Wide Area Network A physical or logical network that provides capabilities for a number of independent devices to communicate with each other over a common transmission-interconnected topology in geographic areas larger than those served by local area networks.

6. APPENDIX C

6.1. REFERENCES

doIT RIght	POLICY#	STATUS	ISSUED	LAST REVISED	PAGE
	10-08	Accepted		09/03/2008	1 of 12
State of Rhode Island **Department of Administration** **Division of Information Technology**		TITLE	***Policy on Forensic Investigation and Authorization***		
		DRAFTED BY		Dmitry Kuchynski	

1.0 Purpose:

The purpose of this document is to establish policy and procedure for requesting an investigation involving the use of computers and/or any other devices capable of storing electronic data.

A process should be established for dealing with incidents that require non-criminal forensic investigation. This policy is not meant to supersede any standards of best practice for criminal forensic investigations.

2.0 Applicability

This policy is applicable to all persons who may request computer forensic services from the RI Division of Information Technology (DOIT) or perform computer forensic services on behalf of DOIT.

3.0 Objectives:

Establish the appropriate requirements for requesting an examination involving the use of computers and/or any other devices capable of storing electronic data.

4.0 Investigation Authorization Requests and Approvals:

4.1 The following State officials are authorized to approve/direct an investigation which involves the use/misuse of computers and any other related devices capable of storing electronic data

4.1.1 State Chief Information Officer (CIO) or designee;

4.1.2 Agency HR representative;

4.1.3 Agency Director's representative;

4.1.4 State Chief Information Security Officer (CISO) or designee.

4.2 An investigation request can be submitted by e-mail, letter, and/or fax using the "Authorization for Computer Forensic Services" form.

4.3 Agency Information Manager (AIM) or Technical Support Manager (TSM) shall make his/her investigation request through his/her respective

HR representative.

5.0 Forensic Investigation Process

5.1 The scope of the forensic investigation will be determined by the State Computer Examiner assigned to the case.

5.2 Physical chain of custody will be maintained at all times utilizing the "DOIT Chain of Custody Document".

5.3 Updates and notifications on the forensic case will be provided to the requestor based on the progress as determined by the State Computer Examiner.

5.4 Any copies of the forensic reports must be produced by DOIT and accompanied by the "DOIT Removable Media Transmittal Sheet"

6.0 State Computer Examiner Compliant Activities:

6.1 Examination of media should be conducted in a forensically sound examination environment;

6.2 Properly prepared media should be used when making forensic copies to insure no commingling of data from different cases. Properly prepared media is that which has been completely overwritten and is in compliance with the DOIT Policy "Media Handling and Security" Policy #05-01.

6.3 State Computer Examiner should always sterilize the media used for evidence acquisition and image storage with the Department of Defense compliant disk wiping utility.

6.4 Verify successful acquisition by comparing known values of the original and the copy or by doing a sector-by-sector comparison of the original to the copy.

7.0 Exceptions to Policy:

7.1 Exceptions to this policy may be granted solely by the CISO or the CISO's designee.

7.2 The examination may be performed by an approved outside entity at the discretion of the CISO or the CISO's designee.

7.3 Examinations deemed criminal will be turned over to the appropriate law enforcement agency.

8.0 Implementation Responsibility

Only State Computer Examiners can perform computer examinations in the State of Rhode Island and its agencies unless an exception has been provided.

State Computer Examiners will follow all aspects of DOIT policies in computer forensics.

9.0 Compliance Responsibility

The DOIT and the State Agencies shall be responsible for implementing and enforcing this policy within their supported areas.

10.0 Definitions

Computer Forensics - The scientific examination and analysis of data held on, or retrieved from, computer storage media in such a way that the integrity of the information can be used as evidence in a court of law.

Computer Forensic Investigations (CFI) – A scientific investigation involving acquiring, preserving, retrieving, and presenting data that has been processed electronically and stored on computer media.

Media – media including but not limited to hard drives, removable media (flash drives, floppy discs, CDs, DVDs, etc.), media from PDA and Blackberry devices.

Forensically-sterile media – media properly wiped with the Department of Defense compliant utility at least 4 times (three overwrite passes and a full verification pass) and verified by the examiner.

Forensically sound examination environment - is one which is completely under the control of the examiner: no actions are taken without the examiner permitting them to happen; and when the examiner permits or causes an action he/she can predict with reasonable certainty what the outcome of the action will be.

State Computer Examiner – an investigator with specialized training in the area of computer forensics responsible for the recovery, analysis, and subsequent presentation of electronic evidence and authorized by the State CIO.

Forensic software – properly licensed copy of the software used by the computer examiner.

11.0 References

05-01 DOIT Policy Media Handling and Security.
US DOJ Forensic Examination of Digital Evidence: A Guide to Law Enforcement (April 2004).
US-Cert First Responders Guide to Computer Forensics (October 2005)

12.0 Attachments

Authorization for Computer Forensic Services Form
DOIT Chain of Custody Document
DOIT Removable Media Transmittal Sheet

13.0 Approvals:

Chief Information Security Officer — 9-3-08
Date

Chief Information Officer — 9/4/08
Date

Director of Administration — 9/5/08
Date

Authorization for Computer Forensic Services

General Information (required)

□ Agency Official has been contacted: ______________________________

Name of the Agency Official contacted

□ This request has been evaluated / reported to the member of the legal department or State Police ______________________________

Name and Title of Responsible person(s)

Name and Title of Person Requesting Forensics: *(results will be reported to this individual)*

Address:

Contact Phone#:

Notes:

Details on the case (required)

1. Why do you need this service?

□ To administer appropriate use audits
□ To assist in the investigation/prosecution of an employee
□ To assist in the investigation/prosecution of a customer
□ To gain access to an employee's encrypted or password protected data
□ To identify source of hacker/terrorist
□ To recover deleted data files
□ To recover reformatted drive data
□ Other ______________________________

2. What kind of data are you seeking?

□ Employee Work Documents
□ Entire Drive recovery

□ Harassment documentation
□ Employee internet/email abuse
□ Internal malicious data
□ External malicious data
□ Pornographic graphic files
□ Illegal activity
□ Other ______________________

3. If data may be taken to court, will case be:
□ Civil
□ Criminal
□ Employment termination
□ Other ____

Note: any criminal investigation needs to be forwarded to the RI State Police or FBI and will not be handled by DOIT

4. What kind of computer needs to be examined?
□ Desktop computer
□ Digital Camera
□ Floppy Disk
□ Laptop computer
□ Memory card
□ Workstation
□ Zip disc
Other

5. How many computers need this service?
□ 1
□ 2
□ 3-5
□ more then 5

6. What is the Operating System?
□ Windows 95/98/ME
□ Windows 2000
□ Windows NT
□ Windows XP
□ Windows 2003
□ Other ____

7. Priority of the Case:
□ Low
□ Medium
□ High

Member of the agency management: ______________________________ Date: _______

Member of the DOIT Security Management: ________________________ Date:_______

DOIT Chain of Custody Document

Submitting Activity

Before submitting any computer components, you must print and fill out by hand the Chain of Custody Form. The purpose of the document is to prove that the integrity of the evidence was maintained through seizure to the production to court if necessary.

□ Agency Official has been contacted: ______________________________

Name of the Agency Official contacted

□ Name and title of person from whom received (owner, other ____________________)

____

Name and Title of Responsible person(s)

Name and Title of Person Requesting Forensics: *(results will be reported to this individual)*

Address:	Contact Phone#:
Location from Where Obtained:	
Description of Item to Be Tested:	Date Obtained:
Name and Title of Person Collecting Evidence: *(if different from above)*	Time Obtained:

For Internal Use Only

Article Received from: *(name, title, federal express package, etc)*

Description of Articles

Chain of Custody

Date & Time	Released By	Received By	Purpose of Change in Custody
	Signature	Signature	
	Name, Title	Name, Title	
	Signature	Signature	
	Name, Title	Name, Title	

Turn form over for additional Chain of Custody blanks

Chain of Custody

Date & Time	Released By	Received By	Purpose of Change in Custody
	Signature	Signature	
	Name, Title	Name, Title	
	Signature	Signature	
	Name, Title	Name, Title	
	Signature	Signature	
	Name, Title	Name, Title	
	Signature	Signature	
	Name, Title	Name, Title	
	Signature	Signature	
	Name, Title	Name, Title	
	Signature	Signature	
	Name, Title	Name, Title	
	Signature	Signature	
	Name, Title	Name, Title	

	Signature	Signature	
	Name, Title	Name, Title	
	Signature	Signature	
	Name, Title	Name, Title	
	Signature	Signature	
	Name, Title	Name, Title	

Final Disposal Action

□ Released to: ______________________________

□ Destroyed: ______________ ______________________________

Date Signature, Name, Title

Witness to Destruction of Article(s)

The article(s) listed above was(were) destroyed by the evidence custodian, in my presence, on the date indicated above.

______________________________ ______________________________

Name, Title Signature

DOIT ENTERPRISE SECURITY

DOIT Removable Media Transmittal Sheet

Date:

Case:

Number of media items (for ex. CDs):

Description of Contents:

Transmitted by:

Name: ______________________________

Signature: ______________________________

Received by:

Name: ______________________________

Signature: ______________________________

NOTE Please request any required duplicates of removable media from DoIT Security. **Do Not** make duplicates of the media.

State of Rhode Island Department of Administration Division of Information Technology	**V.1.0** **Effective 07/31/2014**
Audit and Accountability	**Policy 10-13**

1. Background

Organizations require a means of examining the actions of users with legitimate access authorization to IT system resources, assessing individual accountability, reconstructing events, detecting system intrusions, and identifying problems that do not trigger alerts. Various State and Federal laws, regulations, executive orders, and mandates require that organizations establish and maintain an effective audit function, especially with regard to sensitive information systems and confidential data. The ability to assess system actions and assign accountability to specific users is critical to maintain overall information system security.

2. Purpose

To provide the Agency with policy, standards, and guidelines for establishing and effectively managing an Information Systems Audit and Accountability program at the Agency.

3. Scope

This policy covers all State Executive Branch Departments[1] (including agencies, boards and commissions), and its and their employees, whether permanent, non-permanent, full or part-time, and interns as well as all individuals including, but not limited to, employees, whether permanent, non-permanent, full or part-time, interns, and all consultants, contractors, vendors, contracted individuals, and any entity with access to State data or computers and systems operated by the State or maintained on behalf of the State.

4. Authority

Executive Order 04-06 established the Division of Information Technology ("DoIT") within the Department of Administration to improve the efficiency, effectiveness, and security of IT management and operations within the Executive Branch of the State of Rhode Island. The DoIT Chief Information Officer ("CIO") is authorized, directed, and responsible for the oversight, coordination, and development of all IT resources within the Executive Branch. DoIT will define, maintain, and enforce State-wide IT related policies, standards, and procedures for the effective use and security of these resources.

5. Definitions

[1] State Executive Branch Departments does not include the University of Rhode Island, the State colleges, State Treasurer, the Attorney General and State Secretary of State.

Auditable Event
An observable occurrence identified for its significance and relevance to the security of the information system and environment in which it operates (e.g., user logins/logoffs, system administrator activities).
Audit Reduction
A process that manipulates, organizes, and reduces audit record data to provide useful and more meaningful information within audit reports for analysts during reviews.
Non-Repudiation
Ensuring that a user or process cannot falsely deny having performed a particular action.
Processing Failures
Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded.
Waiver
A dispensation from policy due to extenuating circumstances.

6. Policy

6.1. **Auditable Events.**

6.1.1. Auditable events to be recorded by information systems will be identified.

6.1.2. The list of auditable events will be reviewed annually.

6.2. **Audit Records.**

6.2.1. Information systems will generate audit records of identified auditable events that contain sufficient data to establish:

- The type of event that occurred.
- The time and place the event occurred.
- The source and outcome of the event.
- The identity of the user(s) and significant information system components associated with the event.

6.2.2. Audit records will not be modified or deleted.

6.3. **Storage Capacity.** Sufficient storage capacity will be allocated within information systems audit record repository to ensure that all auditable events are logged.

6.4. **Processing Failures.**

6.4.1. Information systems will automatically alert designated personnel when there is an audit processing failure.

6.4.2. The Agency will develop procedures for handling audit processing failures that are appropriate for the information system.

6.5. **Reviews.**

6.5.1. Audit records will be periodically reviewed for indications of inappropriate or suspicious activity in accordance with all applicable Federal and State laws, regulations, Executive Orders, compliance mandates, and any other requirements.

6.5.2. Any findings resulting from the audit review will be promptly reported to appropriate personnel.

6.6. **Audit Reduction and Report Generation.**

6.6.1. Information systems will have an audit reduction and report generation capability that supports on-demand, ad hoc, customizable, and after-the-fact analysis of security incidents.

6.6.2. Audit records will not be altered during the audit reduction and report generation process.

6.7. **Time Stamps.** Information systems will use synchronized internal system clocks to generate audit record time stamps.

6.8. **Securing Audit Information.**

6.8.1. Audit information, including audit tools, records, settings, and reports, will be secured and protected from unauthorized access, modification, and deletion.

6.8.2. Audit records that contain federal tax information and other sensitive or confidential data will be encrypted at all times.

6.9. **Non-Repudiation.** Information systems will have adequate controls in place to assure, with a high level of confidence, the non-repudiation of actions performed on the system.

6.10. **Retention.** Information systems will retain audit records in accordance with all applicable Federal and State laws, regulations, Executive Orders, mandates, and compliance requirements.

6.11. **Policy Issuance.** This policy becomes effective upon approval and shall supersede all previously issued policies. This policy may be amended or revoked.

6.12. **Policy Reviews.** This policy will be reviewed annually and updated as required.

6.13. **Noncompliance.** Any entity or person who violates this policy may be subject to disciplinary action up to and including termination.

6.14. **Waivers.** The Agency may request a waiver from this policy by formally submitting justification for the waiver and demonstrating that compensating controls are in place to mitigate the risk. If approved, the Agency Director must accept in writing all risk to IT system resources and data associated with the waiver. Waivers require approval from and are granted solely by the DoIT Chief Information Officer. Waivers expire one year from date of issue, or upon the ending for the reason for the waiver, whichever occurs sooner, whereupon they must be renewed.

7. *Roles and Responsibilities*

Chief Information Security Office

- Periodically review and update this policy, as required.
- Periodically perform audit and accountability security assessments of Agency information systems to ensure compliance with this policy.
- Identify and document auditable events required by every Agency information system.

Agency

- Comply with provisions documented in this policy.

- Develop procedures for handing audit processing failures appropriate for the information system.
- Identify and document auditable events specific to the information system and not identified by the Chief Information Security Office but that are required by Federal or State laws, regulations, Executive Orders, compliance mandates, or other requirements.
- Periodically review audit records.

8. Revision History

Version	Date	Reason for Revision
V.1.0	07/21/2014	Initial

This policy is scheduled for review on or before 07/31/2015.

9. Approvals

Chief Information Officer, DoIT — Date 11/25/2014

Chief Information Security Officer, DoIT — Date 11/24/2014

Director, Department of Administration — Date 12-3-14

State of Rhode Island
Department of Administration
Division of Information Technology

Audit and Accountability

V.1.0
Effective 07/31/2014
Standard 10-13

1. Background

Organizations require a means of examining the actions of users with legitimate access authorization to IT system resources, assessing individual accountability, reconstructing events, detecting system intrusions, and identifying problems that do not trigger alerts. Various State and Federal laws, regulations, executive orders, and mandates require that organizations establish and maintain an effective audit function, especially with regard to sensitive information systems and confidential data. The ability to assess system actions and assign accountability to specific users is critical to maintain overall information system security.

2. Purpose

To determine user accountability and maintain system security by ensuring there is adequate tracking of all logical access and system configuration changes to State of Rhode Island information resources.

3. Scope

This policy covers all State Executive Branch Departments[1] (including agencies, boards and commissions), and its and their employees, whether permanent, non-permanent, full or part-time, and interns as well as all individuals including, but not limited to, employees, whether permanent, non-permanent, full or part-time, interns, and all consultants, contractors, vendors, contracted individuals, and any entity with access to State data or computers and systems operated by the State or maintained on behalf of the State.

4. Authority

Executive Order 04-06 established the Division of Information Technology (DoIT) within the Department of Administration to improve the efficiency, effectiveness, and security of IT management and operations within the Executive branch of the State of Rhode Island. The DoIT Chief Information Officer (CIO) is authorized, directed, and responsible for the oversight, coordination, and development of all IT resources within the Executive branch. DoIT will define, maintain, and enforce State-wide IT related policies, standards, and procedures for the effective use and security of these resources.

5. Definitions

Auditable Event
An observable occurrence identified for its significance and relevance to the security of the information system and environment in which it operates (e.g. user logins/logoffs, system administrator activities).

[1] State Executive Branch Departments does not include the University of Rhode Island, the State colleges, State Treasurer, the Attorney General and State Secretary of State.

Audit Reduction
A process that manipulates, organizes, and reduces audit record data to provide useful and more meaningful information within audit reports for analysts during reviews.
Non-Repudiation
Ensuring that a user or process cannot falsely deny having performed a particular action.

6. Standards

6.1. **Auditable Events.** Auditable events should be relevant to the security of information systems and the environments in which they operate. A balance must be struck between business needs, compliance requirements, and information system performance capabilities.

6.1.1. At a minimum, information system audit logs will capture the following auditable events:

- Successful and failed authentication attempts.
- Logons and logoffs.
- Activities of privileged users (e.g. system and network administrators).
- Changes (i.e. creation/modification/deletion) to user accounts, access permissions, and system/application configurations.
- Modifications to security functions (e.g. disabling logging, password criteria).
- System/Application startups, shutdowns, restarts, reboots, and errors.
- Network configuration changes (e.g. routers, firewalls, switches, proxies, servers).

6.1.2. In addition to those listed above, Agencies that process FTI will log the following events:

- Any changes with the potential to compromise the integrity of audit policy configurations and audit trail generation services.
- Command line changes, batch file changes, and system queries.

6.1.3. Auditable events will be logged for the following information system components:

- Desktops and laptops (end-users).
- Network devices (e.g. routers, switches, firewalls, intrusion detection).
- Servers (e.g. file, print, web, terminal).

6.1.4. Any event not specifically specified here, but that is required by federal or State law, regulation, or other mandate, must be logged in accordance with the federal or State law, regulation, or other mandate. Agency management is responsible for identifying these events and ensuring they're properly logged.

6.1.5. Monitoring devices will be employed strategically to collect pre-determined essential information and to record specific types of transactions of interest to the Agency. In case there is an indication of an increased risk to State of Rhode Island assets, operations and/or environment, the level of monitoring activity will be increased.

6.2. **Audit Records.** Adequate controls should be in place to assure, with a high level of confidence, the non-repudiation of actions performed on the system. Audit records should provide sufficient information to enable the creation of the chronological order of activities leading to an auditable event. Meeting this requirement may differ depending on a number of variables, such as the audit logging capability of the information system, business processing requirements, security, costs, and compliance requirements. At a minimum, however, all audit records will contain the following information:

- Event type and description.

- Time stamp (date and time) indicating when the event occurred.
- Event source, destination, and outcome.
- Identity of user generating the event.
- Any other information that is deemed critical to reconstructing the chronological order of activities leading to the event (e.g. software/hardware, process, filename).

6.3. **Audit Storage Capacity.** Information system audit record repositories will have sufficient storage capacity to ensure that all auditable events are logged. Determining audit storage capacity depends on various factors, such as business processing and compliance requirements, the types of events being logged, costs, user base, the sensitivity of the information system/data, etc. System owners are responsible for allocating sufficient disk space for proper audit log retention.

6.4. **Audit Processing Failures.** In the event of an audit processing failure, information systems could, for example, shutdown, stop generating audit records, or overwrite the oldest records. System and data owners are responsible for developing procedures for handling audit processing failures that are appropriate for their information systems and data.

6.4.1. Information systems will automatically send an alert to designated personnel when:

- Auditable events are not being logged.
- The generation of audit reports has stopped.
- Audit records are being overwritten.
- Audit storage capacity utilization is at 75%, 90%, and 100%.

6.4.2. Alerts will be distributed via a mechanism(s) that ensures designated personnel receive them, both on and off hours (e.g. email, text message).

6.4.3. When audit storage capacity is reached and no other storage media is available, the oldest audit records will be overwritten to ensure the most current audit records are saved. Information systems will immediately alert designated personnel whenever this occurs.

6.5. **Reviews.** Audit logs should be analyzed for to assess indications of inappropriate and unusual activity and to provide assurance that the logging function is performing properly. In order to be able to identify unusual activity, reviewers must first understand and recognize normal activity. Reviews should correlate logs between different systems to obtain a more granular view of the interactions between Agency information systems and network devices.

6.5.1. Audit logs will be periodically reviewed for indications of inappropriate or suspicious activity in accordance with all applicable Federal and State laws, regulations, Executive Orders, compliance mandates, and any other requirements. The timeframe between reviews depends on the sensitivity of the system, data, applicable compliance requirements, and a number of other factors specific to the Agency or unique business process. The Agency is responsible for determining this timeframe. In the absence of any applicable and/or documented requirements, audit logs will be reviewed:

- At least quarterly for critical or sensitive information systems.
- At least semiannually (every 6 months) for non-sensitive or non-critical information systems.
- System and application alerts and errors will be reviewed as close to real-time as possible. Alerts and errors for sensitive information systems take precedent over non-sensitive systems.

6.5.2. Any actual/suspected incident or suspicious activity resulting from the review or continuous monitoring activities will be handled in accordance with DoIT's Incident Handling and Response Policy for more information. Follow-up reviews may be necessary depending on the type of security incident.

6.5.3. Reviews will be formally documented to ensure there is a record of the review being performed.

6.6. **Audit Reduction and Report Generation.** Audit logs should be reduced to save storage space and provide useful information within the audit report and for the review process.

6.6.1. Information systems will have the capability of generating audit reports based on selectable criteria (i.e. ad hoc) for near real-time or after-the-fact analysis.

6.6.2. Reviews will be easier if automated tools and information system audit reduction and report generation capabilities are used that support on-demand, ad hoc, customizable, and after-the-fact analysis of security incidents. Automated audit analysis tools improve the effectiveness of audit log reviews and increase the likelihood that they are performed on a timely and periodic basis. Automated tools should be used whenever possible to:

- Detect intrusions based attack signatures, variance techniques, audit reduction methodologies, etc.
- Generate audit reports by distilling relevant information from raw data contained within audit logs.

6.7. **Time Stamps.** Information systems will use synchronized internal system clocks to generate audit record time stamps. If possible, information systems should use a centralized timeserver for network time protocol (NTP) time synchronization.

6.8. **Securing Audit Information.** Audit information, including audit tools, records, settings, and reports, will be protected from unauthorized access, modification, and deletion.

6.8.1. Separation of duties will be enforced such that personnel who administer the access control function are not the same as those who administer or have access to the audit log data.

6.8.2. Audit logs that contain federal tax information and other sensitive or confidential data will be encrypted at all times.

6.8.3. Audit logs will be read-only and not be modified or deleted by anyone at any time prior to the end of the retention period.

6.8.4. The audit log repository and backup log archives will be accessible only to authorized personnel and be protected from breaches of confidentiality and integrity.

6.9. **Retention.** Audit logs will be retained in accordance with all applicable Federal and State laws, regulations, Executive Orders, mandates, and compliance requirements. If the absence of documented retention requirements, audit logs will be retained for a minimum of six (6) months.

6.10. **Standards Reviews.** These standards will be reviewed annually and updated as required.

6.11. **Noncompliance.** Any employee who willfully violates these standards shall be subject to disciplinary action up to and including termination of employment.

6.12. **Waivers.** The Agency may request a waiver from these standards by formally submitting justification for the waiver and demonstrating that compensating controls are in place to mitigate the risk. If approved, the Agency Director must accept in writing all risk to IT system resources and data associated with the waiver. Waivers require approval from and are granted solely by the DoIT Chief Information Officer. Waivers expire one year from date of issue, whereupon they must be renewed.

7. Roles and Responsibilities

Enterprise Information Security Office

- Periodically review and update these standards, as required.
- Periodically perform audit and accountability security assessments of Agency information systems to ensure compliance with these standards.
- Identify and document auditable events required by every Agency information system.

Agency

- Comply with provisions documented in these standards.
- Develop procedures for handing audit processing failures appropriate for the information system.
- Identify and document auditable events specific to the information system and not identified by the Enterprise Information Security Office but that are required by Federal or State laws, regulations, Executive Orders, compliance mandates, or other requirements.
- Periodically review audit records.

8. Revision History

Version	Date	Reason for Revision
V.1.0	07/21/2014	Initial

These standards are scheduled for review on or before 07/31/2015.

9. Approvals

Chief Information Officer, DoIT

7/31/14
Date

Chief Information Security Officer, DoIT

7/30/14
Date

State of Rhode Island
Department of Administration
Division of Information Technology

V.1.0

Effective 07/31/2014

Configuration Management

Policy 10-14

1. Background

Information systems consist of hardware and software that are networked and configured in a complex manner and are typically in a constant state of flux throughout their lifecycle in response to changes in business processes, new or updated hardware and software, vulnerability patching, security threats, etc. This state of flux requires that changes, often intricate and extensive, to information system configuration setting be made. Managing the implementation of system changes is critical to maintaining system security and reducing overall organizational risk.

2. Purpose

To establish a Configuration Management Policy for effectively managing risk associated with changes to and that have an impact on system configurations, baseline configuration settings, and overall information system security.

3. Scope

This policy covers all State Executive Branch Departments[1] (including agencies, boards and commissions), and its and their employees, whether permanent, non-permanent, full or part-time, and interns as well as all individuals including, but not limited to, employees, whether permanent, non-permanent, full or part-time, interns, and all consultants, contractors, vendors, contracted individuals, and any entity with access to State data or computers and systems operated by the State or maintained on behalf of the State

4. Authority

Executive Order 04-06 established the Division of Information Technology ("DoIT") within the Department of Administration to improve the efficiency, effectiveness, and security of IT management and operations within the Executive Branch of the State of Rhode Island. The DoIT Chief Information Officer ("CIO") is authorized, directed, and responsible for the oversight, coordination, and development of all IT resources within the Executive Branch. DoIT will define, maintain, and enforce State-wide IT related policies, standards, and procedures for the effective use and security of these resources.

5. Definitions

Baseline Configuration

[1] State Executive Branch Departments does not include the University of Rhode Island, the State colleges, State Treasurer, the Attorney General and State Secretary of State.

An agreed upon set of technical, functional, and physical specifications that reflects the current information system architecture, serves as the basis for future changes, and is the foundation of Configuration Management. A baseline configuration includes, for example, standard software installed on workstations, laptops, servers, network components, and mobile devices, operating system and application versions and patch sets, and configuration settings.

Configuration Management
The process of establishing, maintaining, and managing changes to system hardware, software, documentation, and functional and physical characteristics of the operational environment throughout the information system lifecycle.

Configuration Management Plan
Defines system level processes and procedures for how configuration management will be implemented to support system development lifecycle activities.

Configuration Settings
Parameters within information system hardware, software, or firmware components that may be changed and, as a consequence, have an effect on the security posture or functionality of the system.

Inventory
A detailed, itemized list, report, or record of things associated with the system.

Security Impact Analysis
An analysis of a proposed change to determine its potential impact on system security. The analysis may include such tasks as reviewing security plans, conducting risk assessments, and performing tests within a test environment.

Waiver
A dispensation from policy due to extenuating circumstances.

6. *Policy*

6.1. **Configuration Change Control.**

6.1.1. Configuration settings will be established, documented, monitored, and controlled.

6.1.2. The types of changes to be placed under configuration control will be identified.

6.1.3. Proposed changes to information systems will be reviewed by appropriate personnel. A security impact analysis will be performed to determine its potential impact on system security.

6.1.4. Configuration change decisions will be documented, retained, and available for audit.

6.1.5. Configuration change control activities will be coordinated by an oversight committee.

6.1.6. Physical and logical access restrictions associated with configuration changes to information systems will be defined, documented, approved, and enforced according to the principles of separations of duties and least privilege.

6.2. **Configuration Management Plan.** A configuration management plan for the information system will be developed, documented, periodically reviewed, and protected from unauthorized disclosure and modification. This plan will define the roles, responsibilities, and configuration management processes and procedures necessary for identifying and managing configuration items throughout the system development lifecycle.

6.3. **Baseline Configuration.** A current baseline configuration for each information system will be developed, documented, maintained, and periodically reviewed.

6.4. **Inventory.** An inventory that accurately reflects the current information system and all of its components will be developed, documented, periodically reviewed, and updated as required.

6.5. **Software.**

6.5.1. Software will be authorized and approved prior to being installed on information systems.

6.5.2. Software and associated documentation will be used according to and tracked for compliance with contracts, licensing agreements, and copyright laws.

6.6. **Policy Issuance.** This policy becomes effective upon approval and shall supersede all previously issued policies. This policy may be revoked or amended.

6.7. **Policy Reviews.** This policy will be reviewed annually and updated as required.

6.8. **Noncompliance.** Any person or entity that violates this policy may be subject to disciplinary action up to and including termination.

6.9. **Waivers.** The Agency may request a waiver from this policy by formally submitting justification for the waiver and demonstrating that compensating controls are in place to mitigate the risk. If approved, the Agency Director must accept in writing all risk to IT system resources and data associated with the waiver. Waivers require approval from and are granted solely by the DoIT Chief Information Officer. Waivers expire one year from date of issue, or upon the ending for the reason of the waiver, whichever occurs sooner, whereupon they must be renewed.

7. Roles and Responsibilities

Chief Information Security Office

- Periodically review and update this policy, as required.
- Periodically assess Agency information systems to ensure compliance with this policy.
- Assist in performing the security impact analysis. Review the security impact analysis.

Agency

- Comply with provisions documented in this policy.
- Develop and update, as required, a configuration management plan for each information system.
- Develop and update, as required, a baseline configuration for each information system.
- Document and update, as required, an inventory of each information system.
- Perform a security impact analysis.

8. Revision History

Version	Date	Reason for Revision
V.1.0	07/21/2014	Initial

This policy is scheduled for review on or before 07/31/2015.

9. Approvals

Chief Information Officer, DoIT

11/25/2014
Date

Chief Information Security Officer, DoIT

11/24/2014
Date

Director, Department of Administration

12-3-14
Date

State of Rhode Island Department of Administration Division of Information Technology	V.1.0 Effective 07/31/2014
Network and Communications Security	Policy 10-15

1. Background

Network security is critical to maintaining business data. However, many organizational networks are a patchwork of local area networks that run various technological platforms and require different solutions. As a result, maintaining an adequate information security posture is difficult. Because no single solution is able to provide absolute security against all types of threats, many organizations utilize the concept of defense in-depth to mitigate these limitations inherent within all security technologies. This strategy implements layers of security technologies to increase the odds that a security breach in one layer is caught within another layer and, thereby, reduce organizational risk.

2. Purpose

To establish policy for implementing effective system and communications security over IT system resources and to ensure the confidentiality, integrity, and availability of transmitted data.

3. Scope

This policy covers all State Executive Branch Departments[1] (including agencies, boards and commissions), and its and their employees, whether permanent, non-permanent, full or part-time, and interns as well as all individuals including, but not limited to, employees, whether permanent, non-permanent, full or part-time, interns, and all consultants, contractors, vendors, contracted individuals, and any entity with access to State data or computers and systems operated by the State or maintained on behalf of the State.

4. Authority

Executive Order 04-06 established the Division of Information Technology (DoIT) within the Department of Administration to improve the efficiency, effectiveness, and security of IT management and operations within the Executive Branch of the State of Rhode Island. The DoIT Chief Information Officer ("CIO") is authorized, directed, and responsible for the oversight, coordination, and development of all IT resources within the Executive branch. DoIT will define, maintain, and enforce State-wide IT related policies, standards, and procedures for the effective use and security of these resources.

5. Definitions

Collaborative Computing
A multifaceted group-oriented, and distributed environment with many users and shared resources and devices that enables multiple parties to collaborate on textual and graphical documents. Examples

[1] State Executive Branch Departments does not include the University of Rhode Island, the State colleges, State Treasurer, the Attorney General and State Secretary of State.

include audio and visual conferencing capabilities and their networked devices, such as cameras, microphones, and white boards.

Communication Session
The entirety of a data transmission from start to end.

Cryptography
Securing information in such a manner that ensures its confidentiality and integrity (e.g. encryption).

Domain Name Service (DNS)
A hierarchal distributed naming system that provides domain name and address resolution, essentially translating a domain name to its numerical TCP/IP address, and is critical to the functionality of any IT system resource connected to the internet or within a private network.

Internet Telephony
Hardware and/or software that allow a broad range of services traditionally performed over telephone lines (e.g., transmitting voice, video, and data) to be performed over the internet.

Mobile Code
Software downloaded from remote systems and executed locally on servers and workstations, often without the user's explicit authorization, knowledge, or awareness. Mobile code is also referred to as executable or active content. Examples include Java Applets, ActiveX, Flash, JScript, VBScript, VBA, macros, content embedded within emails and web pages, etc.

Public Key Infrastructure (PKI)
Enables data to be transferred privately and securely over a public network (e.g., internet) through the use of public and private key certificates obtained from trusted authorities.

Partitioning
The process of separating and dividing roles, responsibilities, and functions.

Perimeter Security
Devices or systems that exist at the edge of infrastructure and are considered a firt line of defense from external attack.

Wireless
Also known as "wifi", is an implementation of local area network over radio frequency.

Waiver
A dispensation from policy due to extenuating circumstances.

6. Policy

6.1. Partitioning.

6.1.1. Information system management functionality will be partitioned and separate from non-privileged user functionality.

6.1.2. Information system security functions will be isolated from non-security functions.

6.1.3. Publically accessible information system resources will be physically and logically separate from the internal network. The internal network will be secured and protected from untrusted external networks at all times.

6.2. **Shared Resources.**

6.2.1. Information systems will prevent the unauthorized or unintentional transfer of information via shared system resources.

6.2.2. Collaborative computing devices will be disabled and/or physically disconnected from the network until ready for use.

6.2.3. Information systems will prevent collaborative computing devices from being remotely activated without prior authorization.

6.2.4. Information systems will provide an explicit indication to local users that collaborative computing devices are active and in use.

6.3. **Perimeter Security.**

6.3.1. Information systems will connect to external networks only via managed perimeter security devices.

6.3.2. Communications at information system perimeters and critical internal boundaries will be monitored and controlled.

6.3.3. Information systems will protect against and limit the effects of denial of service attacks.

6.4. **Data Security.**

6.4.1. Data will be appropriately secured at all times, including when at rest, while processing, and during transmission, to ensure its confidentiality and integrity.

6.4.2. Cryptography controls will be implemented where appropriate and as required in accordance with applicable federal and State laws, Executive Orders, policies, regulations, compliance requirements, and standards.

6.4.3. Procedures will be developed for obtaining, issuing, and managing cryptographic keys and public key certificates.

6.5. **Communications Sessions.**

6.5.1. Network connections associated with communications sessions will automatically terminate at the end of the session or after a period of inactivity.

6.5.2. Information systems will protect the authenticity of communications sessions.

6.6. **Domain Name Service (DNS).**

6.6.1. DNS will provide the security status of child subspaces. If the child supports secure resolution services, DNS will enable the verification of the chain of trust among parent and child domains.

6.6.2. DNS will be fault tolerant and have an internal/external role structure for processing name and address resolution requests.

6.7. **Mobile Code.**

6.7.1. Acceptable and unacceptable mobile code will be defined.

6.7.2. Mobile code access and usage restrictions will be established.

6.7.3. The use of mobile code within information system resources will be authorized, monitored, and controlled.

6.8. **Internet Telephony.** Internet telephony access will be authorized, monitored, and controlled, and usage restrictions will be established.

6.9. **Wireless Access.** Wireless access will be authorized, monitored, and controlled, and usage restrictions will be established.

6.10. **Policy Issuance.** This policy becomes effective upon approval and shall supersede all previously issued policies. This policy may be amended or revoked.

6.11. **Policy Reviews.** This policy will be reviewed annually and updated as required.

6.12. **Noncompliance.** Any person or entity that violates this policy may be subject to disciplinary action up to and including termination.

6.13. **Waivers.** The Agency may request a waiver from this policy by formally submitting justification for the waiver and demonstrating that compensating controls are in place to mitigate the risk. If approved, the Agency Director must accept in writing all risk to IT system resources and data associated with the waiver. Waivers require approval from and are granted solely by the DoIT Chief Information Officer. Waivers expire one year from date of issue, or upon the ending for the reason for the waiver, whichever occurs first, whereupon they must be renewed.

7. *Roles and Responsibilities*

Chief Information Security Office

- Periodically review this policy and update as required.
- Perform periodic audits to ensure compliance with this policy.
- Review requests for external connections to the internal network.

Agencies

- Comply with provisions documented in this policy.
- Obtain approval from DoIT prior to connecting to the external network.
- Periodically review external connections to the internal network.

8. *Revision History*

Version	Date	Reason for Revision
V.1.0	07/21/2014	Initial

This policy is scheduled for review on or before 07/31/2015.

9. Approvals

11/25/2014

Chief Information Officer, DoIT

Date

11/24/2014

Chief Information Security Officer, DoIT

Date

12-3-14

Director, Department of Administration

Date

State of Rhode Island Department of Administration Division of Information Technology	V.1.0 Effective 07/31/2014
Physical and Environmental Security	Policy 10-16

1. Background

Physical and environmental security controls protect information system facilities from physical and environmental threats. Physical access to facilities and supporting infrastructure, such as communications, power, and cabling, must be secured to prevent their compromise.

2. Purpose

To establish a Physical and Environmental Security Policy that effectively protects information systems and information system components from physical and environmental hazards.

3. Scope

This policy covers all State Executive Branch Departments[1] (including agencies, boards and commissions), and its and their employees, whether permanent, non-permanent, full or part-time, and interns as well as all individuals including, but not limited to, employees, whether permanent, non-permanent, full or part-time, interns, and all consultants, contractors, vendors, contracted individuals, and any entity with access to State data or computers and systems operated by the State or maintained on behalf of the State.

4. Authority

Executive Order 04-06 established the Division of Information Technology (DoIT) within the Department of Administration to improve the efficiency, effectiveness, and security of IT management and operations within the Executive Branch of the State of Rhode Island. The DoIT Chief Information Officer ("CIO") is authorized, directed, and responsible for the oversight, coordination, and development of all IT resources within the Executive Branch. DoIT will define, maintain, and enforce State-wide IT related policies, standards, and procedures for the effective use and security of these resources.

5. Definitions

Emergency Controls

Systems or system components that provide for continued control, or that can be activated to provide enhanced control, in the event of an emergency.

Environmental Controls

Systems or system components that ensure a stable operating environment with respect to the environment, such as temperature, humidity, water levels, etc.

[1] State Executive Branch Departments does not include the University of Rhode Island, the State colleges, State Treasurer, the Attorney General and State Secretary of State.

Physical Access
The process by which a person may corporeally be present in a given area or location.

Waiver
A dispensation from policy due to extenuating circumstances.

6. Policy

6.1. **Physical Access Authorizations.**

6.1.1. An access control list of personnel authorized to physically access the information system facility will be developed, approved, maintained current, updated to reflect individuals no longer requiring access, and periodically reviewed.

6.1.2. Authorization credentials will be issued for physical access to information system facilities. Different credentials may be required for different information system facilities and persons/entities may be required to sign certain documents before entrance.

6.2. **Physical Access Controls.**

6.2.1. Physical access authorizations will be controlled and verified at information system facility entrances prior to granting access.

6.2.2. Physical access logs for all personnel, including visitors, accessing information system facilities will be maintained and periodically reviewed.

6.2.3. Physical access to information system facilities will be monitored to detect and respond to physical security incidents. Visitors will be escorted and their activities will be monitored while within controlled areas of information system facilities.

6.2.4. Publically accessible areas within information system facilities will be designated, controlled, and secured.

6.2.5. Devices that control physical access to information system facilities will be secured and periodically inventoried.

6.2.6. Cipher lock combination codes will be changed annually, whenever there is an actual or suspected incidence of a compromised code, or personnel knowing the combination are transferred or terminated. Keys and/or card keys will be changed whenever reported as being lost or personnel having keys and/or card keys are transferred or terminated.

6.2.7. Physical access to distribution lines, transmission lines, output devices, and other power equipment and cabling critical to the functionality of information systems will be secured, restricted to authorized users/individuals, and protected from damage.

6.2.8. Information system components entering and leaving information system facilities will be authorized, monitored, documented, and controlled.

6.2.9. Physical access to alternate work sites will be secured, periodically assessed, and provide a means to communicate with information security personnel in the event of an incident.

6.2.10. Information system components will be positioned within facilities to minimize the opportunity for unauthorized access and the potential damage from physical and environmental hazards.

6.3. **Emergency Controls.**

6.3.1. An emergency shutoff switch that cuts power to information systems and/or individual system components in emergency situations will be installed, be easily accessible to personnel, and be protected from unauthorized or inadvertent activation.

6.3.2. An uninterruptible power supply will be installed in order to facilitate an orderly information system shutdown or to transition to an alternate power source in the event the primary source of power is lost.

6.3.3. Emergency lighting that is automatically activated in the event of a power outage or disruption will be installed.

6.4. **Environmental Controls.**

6.4.1. Fire suppression and detection systems and devices that are maintained and periodically tested will be installed at information system facilities.

6.4.2. Temperature and humidity levels at information system facilities will be monitored and maintained at appropriate levels.

6.4.3. Information systems will be protected against water damage.

6.5. **Policy Issuance.** This policy becomes effective upon approval and shall supersede all previously issued policies. This policy may be amended or revoked.

6.6. **Policy Reviews.** This policy will be reviewed annually and updated as required.

6.7. **Noncompliance.** Any person or entity that violates this policy shall be subject to disciplinary action up to and including termination..

6.8. **Waivers.** The Agency may request a waiver from this policy by formally submitting justification for the waiver and demonstrating that compensating controls are in place to mitigate the risk. If approved, the Agency Director must accept in writing all risk to IT system resources and data associated with the waiver. Waivers require approval from and are granted solely by the DoIT Chief Information Officer. Waivers expire one year from date of issue, or upon the ending for the reason for the waiver, whichever occurs first, whereupon they must be renewed.

7. *Roles and Responsibilities*

Chief Information Security Office

- Periodically review and update this policy, as required.
- Periodically assess physical and environmental security at Agency information system facilities to ensure compliance with this policy.

Agency

- Comply with provisions documented in this policy.
- Maintain a list of personnel authorized to access information system facilities.
- Issue credentials for physical access to information systems.
- Log all access to information system facilities.
- Ensure physical and environmental controls are in place to secure information system facilities.

8. *Revision History*

Version	Date	Reason for Revision
V.1.0	07/21/2014	Initial

Policy is scheduled for review on or before 07/31/2015.

9. Approvals

John E Landers

Chief Information Officer, DoIT

11/25/2014

Date

Chief Information Security Officer, DoIT

11/24/2014

Date

Director, Department of Administration

12-3-14

Date

	State of Rhode Island Department of Administration Division of Information Technology	*Ver 1* *Effective* *07/31/2014*
	Security Planning Policy	*Policy* *10-18*

1.0 Purpose

This policy establishes the Enterprise Security Planning Policy, for managing risks from inadequate security planning through the establishment of an effective security planning program. The security planning program helps implement security best practices with regard to enterprise security planning, preparation, and strategy.

2.0 Scope

This policy covers all State Executive Branch Departments[1] (including agencies, boards and commissions), and its and their employees, whether permanent, non-permanent, full or part-time, and interns as well as all individuals including, but not limited to, employees, whether permanent, non-permanent, full or part-time, interns, and all consultants, contractors, vendors, contracted individuals, and any entity with access to State data or computers and systems operated by the State or maintained on behalf of the State.

3.0 Policy

Agencies shall develop, test, review, and maintain coordinated plans for the security of information systems. Such coordinated plans are privileged and/or confidential under Rhode Island Law. As such, these coordinated plans will not be publicly disclosed.

4.0 Authority

Executive Order 04-06 established the Division of Information Technology ("DoIT") within the Department of Administration to improve the efficiency, effectiveness, and security of IT management and operations within the Executive Branch of the State of Rhode Island. The DoIT Chief Information Officer ("CIO") is authorized, directed, and responsible for the oversight, coordination, and development of all IT resources within the Executive Branch. DoIT will define, maintain, and enforce State-wide IT related policies, standards, and procedures for the effective use and security of these resources.

5.0 Policy Issuance

This policy becomes effective upon approval and shall supersede all previously issued policies. This policy may be revoked or amended.

6.0 Enforcement

[1] State Executive Branch Departments does not include the University of Rhode Island, the State colleges, State Treasurer, the Attorney General and State Secretary of State.

Any person or entity found to have violated this policy may be subject to disciplinary action up to and including termination.

7.0 Definitions

Systems Security Plan

A plan that details security-based controls and mitigating factors to ensure the safety and security of data that is part of an information system.

Privacy Impact Assessment

A privacy impact assessment is a tool for identifying and assessing privacy risks throughout the development life cycle of a program or system. It states what personally identifiable information is collected, and explains how that information is maintained, protected, and shared.

8.0 Policy

8.1 System Security Plan: All State of Rhode Island Business Systems must develop a security plan for the information assets that:

8.1.1 Is consistent with the organization's enterprise architecture.

8.1.2 Explicitly defines the authorization boundary for the system.

8.1.3 Describes the operational context of the information asset in terms of missions and business processes.

8.1.4 Provides the security category and impact level of the information asset including supporting rationale.

8.1.5 Describes the operational environment for the information asset.

8.1.6 Describes relationships with or connections to other information systems.

8.1.7 Provides an overview of the security requirements for the system.

8.1.8 Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions.

8.1.9 Is reviewed and approved by the authorizing official or designated representative prior to plan implementation.

8.2 Rules of Behavior: All State of Rhode Island Business Systems must establish and make readily available to all information asset users, the rules that describe their responsibilities and expected behavior with regard to information and information asset usage. In addition, they must receive signed acknowledgment from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information asset.

8.3 Privacy Impact Assessment: All State of Rhode Island Business Systems must conduct a privacy impact assessment of the information assets associated with their systems.

8.4 Security-Related Activity Planning: All State of Rhode Island Business Systems must plan and coordinate security-related activities affecting company information assets before conducting such activities in order to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation), organizational assets, and individuals.

9.0 Roles and Responsibilities

Chief Information Security Office

- Periodically review this policy and update as required.
- Perform periodic audits to ensure compliance with this policy.
- Review requests for external connections to the internal network.

Agencies

- Comply with provisions documented in this policy.
- Obtain approval from DoIT prior to connecting to the external network.
- Periodically review external connections to the internal network.

10.0 Revision History

Version	Date	Reason for Revision
V.1.0	07/21/2014	Initial

This policy is scheduled for review on or before 07/31/2015.

11.0 Approvals

Chief Information Security Officer

11/24/2014
Date

Chief Information Officer

11/25/2014
Date

Director, Department of Administration

12-3-14
Date