TABLE OF CONTENTS

1. MIS INFORMATION TECHNOLOGIES (IT) SECURITY POLICY 2
   - 1.1. PURPOSE 2
   - 1.2. BACKGROUND 2
   - 1.3. POLICY 2
   - 1.4. RESPONSIBILITIES 2
2. IT SECURITY PROGRAM MANAGEMENT 4
   - 2.1. PURPOSE 4
   - 2.2. POLICY 4
   - 2.3. RESPONSIBILITIES 5
3. SECURITY PLANS 9
   - 3.1. PURPOSE 9
   - 3.2. POLICY 10
   - 3.3. RESPONSIBILITIES 12
4. RISK MANAGEMENT 14
   - 4.1. PURPOSE 14
   - 4.2. BACKGROUND 14
   - 4.3. POLICY 14
   - 4.4. RESPONSIBILITIES 15
5. CONTINGENCY PLANS 17
   - 5.1. PURPOSE 17
   - 5.2. BACKGROUND 17
   - 5.3. POLICY 17
   - 5.4. PROCEDURES 18
   - 5.5. RESPONSIBILITIES 23
6. CERTIFICATION 26
   - 6.1. PURPOSE 26
   - 6.2. BACKGROUND 26
   - 6.3. POLICY 26
   - 6.4. PROCEDURES 29
   - 6.5. RESPONSIBILITIES 32
7. ACCREDITATION 34
   - 7.1. PURPOSE 34
   - 7.2. BACKGROUND 34
   - 7.3. POLICY 34
   - 7.4. PROCEDURES 36
   - 7.5. RESPONSIBILITIES 37
8. APPENDIX A 39
   - 8.1. ACRONYMS 39
9. APPENDIX B 40
   - 9.1. GLOSSARY 40
10. APPENDIX C 49
   - 10.1. REFERENCES 49

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. **Directors** 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. **State CSO** 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. **Department, Unit and Office Heads, and Regional Facility Directors** 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. **Department Director;** ensures that all offices have business resumption and contingency plans for all IT resources.

5.5.2. **Department IT Manager**:

- 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 Contingency Plan Project Coordinator 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 Contingency Plan Project Leader:

- 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. **Contingency Plan Project Coordinator**:

- 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. **Certification Team** 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. **System Administrators** 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. **CISO/ACISO** 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. **CISO:** ensures that all systems within the Department have been accredited.

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

- 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. **Department IT Manager** 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. **System Administrators** 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. **CISO:**

- 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