



DEPARTMENT OF ADMINISTRATION

Enterprise Policy

DOIT-10-18-2014

DIVISION OF INFORMATION TECHNOLOGY

Security Planning Policy

Date of Last Revision 07/31/2014

Bijay Kumar

(401) 574-9220

bijay.kumar@doit.ri.gov

1. Background

- a. 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. Scope

- a. This policy covers all State Executive Branch Departments¹ (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. Policy

- a. 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. Authority

- a. 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. Policy Insurance

- a. This policy becomes effective upon approval and shall supersede all previously issued policies. This policy may be revoked or amended.

6. Enforcement

- a. Any person or entity found to have violated this policy may be subject to disciplinary action up to and including termination.

7. Definitions

- a. **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.
- b. **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. Policy

- a. **System Security Plan:** All State of Rhode Island Business Systems must develop a security plan for the information assets that:
 - (i.) Is consistent with the organization's enterprise architecture.
 - (ii.) Explicitly defines the authorization boundary for the system.
 - (iii.) Describes the operational context of the information asset in terms of missions and business processes.
 - (iv.) Provides the security category and impact level of the information asset including supporting rationale.
 - (v.) Describes the operational environment for the information asset.
 - (vi.) Describes relationships with or connections to other information systems.
 - (vii.) Provides an overview of the security requirements for the system.
 - (viii.) Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions.
 - (ix.) Is reviewed and approved by the authorizing official or designated representative prior to plan implementation.
- b. **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.
- c. **Privacy Impact Assessment:** All State of Rhode Island Business Systems must conduct a privacy impact assessment of the information assets associated with their systems.
- d. **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. Roles and Responsibilities

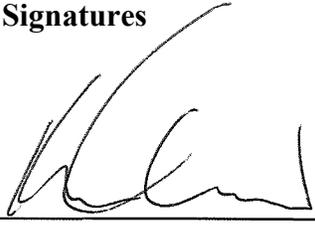
- a. *Chief Information Security Office*

- (i.) Periodically review this policy and update as required.
- (ii.) Perform periodic audits to ensure compliance with this policy.
- (iii.) Review requests for external connections to the internal network.

b. Agencies

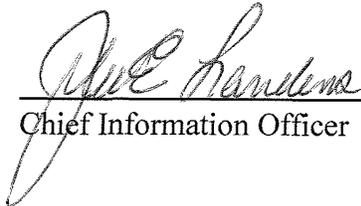
- (i.) Comply with provisions documented in this policy.
- (ii.) Obtain approval from DoIT prior to connecting to the external network.
- (iii.) Periodically review external connections to the internal network.

10. Signatures



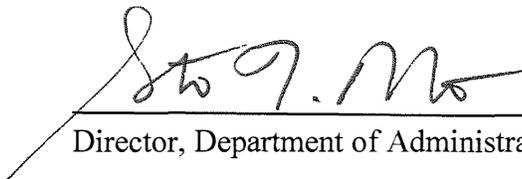
Chief Information Security Officer

11/24/2014
Date



Chief Information Officer

11/25/2014
Date



Director, Department of Administration

12-3-14
Date