1. Purpose

Establish policy for the effective management of Enterprise risk via a security planning program to ensure the confidentiality, integrity, and availability of information systems and data.

2. Applicability

This policy is applicable to all State of Rhode Island Executive Branch Departments\(^1\) (including agencies, boards and commissions), and their employees (including permanent, non-permanent, full-time, and part-time) and interns, consultants, contractors, vendors, contracted individuals, and any entity having access to state information systems and data, whether operated or maintained by the state or on behalf of the state. For this policy, the term "agency" is used to refer to any department, agency, division, or unit of the Executive branch of the State of Rhode Island.

3. Definitions

**Information Security Architecture**
An overall security architecture design that addresses information security necessities and potential risks, including an architectural description, allocation of security controls and functionality, security-related information for external interfaces, protection mechanisms associated with each interface, type of data being processed, stored, transmitted, or exchanged across interfaces, user roles and access privileges, restoration priorities, and any other information required for ensuring adequate security of information systems and data.

**Personally Identifiable Information (PII)**
Data that, either alone or in combination with other data, can be used to identify an individual. Data in electronic or hard copy paper format is considered PII when an individual's first name, or first initial and last name, in combination with one or more of the following:
- Social security number.
- Driver's license number, RI identification card number, or tribal identification number.

---

\(^1\) State of Rhode Island Executive Branch Departments does not include the University of Rhode Island, the State Colleges, the General Treasurer, the Attorney General, or the Secretary of State.
• Account, credit, or debit card number, in combination with any required security code, access code, password, or personal identification number that would permit access to an individual's financial account.
• Medical or health insurance information.
• Email address with any required security code, access code, or password that would permit access to an individual's personal, medical, insurance, or financial account.

System Security Plan (SSP)
A plan that details security-based controls and mitigating factors to ensure the safety and security of information systems and data.

4. Procedures for Compliance

Security controls in this policy will be implemented in accordance with the security categorization of the information system. The security categorization is based on the Information Assurance Level (IAL) requirements of the information system.

Low Risk Systems (IAL1)
Information systems that only contain data that is public by law or directly available to the public via mechanisms such as the internet. In addition, desktops, laptops, and supporting systems used by agencies are Low Risk unless they store, process, transfer, or communicate private or sensitive data.

Moderate Risk Systems (IAL2)
Information systems that store, process, transfer, or communicate private or sensitive data or have a direct dependency on a Moderate system. At a minimum, any information system that stores, processes, transfers, or communicates PII or other sensitive data types is classified as a Moderate system.

4.1. [IAL1, IAL2] Security Planning Policy and Procedures (PL-1). The agency will develop, document, disseminate, review, and annually update a security planning policy and procedures.

4.2. [IAL1, IAL2] System Security Plan (PL-2). The agency will (i) develop a SSP for the information system, (ii) distribute copies of the SSP and communicate subsequent changes to the plan to the State Chief Information Security Officer (CISO), Agency Information Managers (AIM), Agency Technical Support Managers (TSM), and all personnel designated by the agency to have access to the SSP, (iii) annually review the SSP and update it, as required, to address changes to the information system, operational environment, or issues identified during plan implementation or security control assessments, and (iv) protect the SSP from unauthorized disclosure and modification. The SSP developed by the agency for the information system will:
Division of Information Technology

- Reflect the information security architecture and is consistent with the Enterprise architecture.
- Explicitly define the authorization boundary for the information system.
- Describe the operational context of the information system in terms of mission and business processes.
- Provide the security category and impact level of the information system, including supporting rationale.
- Describe the operational environment for the information system.
- Describe relationships with or connections to other information systems.
- Provide an overview of the security requirements for the information system.
- Describe the security controls in place for meeting security requirements.
- Be reviewed and approved by the authorizing official prior to plan implementation.

4.2.1. [IAL2] Plan/Coordinate with Other Agency Entities (PL-2.3). The agency will plan and coordinate security-related activities affecting the information system with EOC Enterprise Teams (i.e. Security, Server Admin, Network, Unix, Storage), Agency Information Manager (AIM), Agency Technical Support Manager (TSM), and other individuals, as designated by the agency, prior to performing activities to reduce the impact to the Enterprise and other agencies.

4.3. [IAL1, IAL2] Rules of Behavior (PL-4). The agency will (i) establish, and make readily available to individuals requiring access to the information system, the rules that describe their responsibilities and expected behavior regarding information and information system usage, (ii) receive a signed acknowledgement from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system, (iii) annually review and update, as required, the rules of behavior, (iv) require individuals who have signed a previous version of the rules of behavior to read and re-sign the acknowledgement form when the rules of behavior are updated. Prior to granting access, the agency will require all agency users who require access to state network resources to sign the “Network Access Rights and Obligations User Agreement Acknowledgement” form found within ETSS Technology Acceptable Use Policy 00-02.

4.3.1. [IAL2] Social Media and Network Restrictions (PL-4.1). The agency will include, within rules of behavior, explicit restrictions on the use of social media and networking sites and the posting of agency information on publicly accessible websites in accordance with ETSS Social Networking Policy 10-09.

4.4. [IAL1, IAL2] Information Security Architecture (PL-8). The agency will develop an information security architecture for the information system that (i) describes the overall philosophy, requirements, and approach for protecting the confidentiality, integrity, and availability of agency information systems and data, (ii) describes how the information security architecture is integrated and supports the Enterprise architecture, and (iii) describes information security assumptions and dependencies regarding external services.
The agency will annually review and update the information security architecture to reflect updates in the Enterprise architecture and ensures that planned information security architecture changes are reflected in the security plan.

5. Approval /Review Signature

Brian Tardiff
Digitally signed by Brian Tardiff
Date: 2020.09.14 12:09:19
-04'00'

Chief Information Security Officer