1. Purpose

Establish policy for the effective implementation of security controls to safeguard State of Rhode Island IT system resources, infrastructure, 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

**Authorizing Official**
A senior level official at the agency with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency and enterprise operations, assets, and personnel.

**Continuous Monitoring**
The monitoring of various aspects of network and information system activity that maintains ongoing awareness of information security, vulnerabilities, and threats to support both Enterprise and agency risk management decisions. The strategy for implementing a continuous monitoring program should identify the security controls to be monitored, monitoring frequency, type of assessment, correlation and analysis, response activities, and responsibilities of personnel with continuous monitoring roles.

**Corrective Action Plan (CAP)**
A list of planned actions and an implementation timetable for correcting deficiencies identified during the security assessment and for mitigating or eliminating known vulnerabilities.

---

\(^1\) 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.
Interconnection Security Agreement (ISA)
An agreement that describes the interface characteristics, security requirements, and nature of information communicated via dedicated connections between information systems.

Penetration Testing
An authorized attempt to gain access to information system resources using techniques that are similar to those used by adversaries in order to identify security weaknesses and exploitable vulnerabilities.

Plan of Action and Milestones (POAM)
A document that identifies tasks needing to be accomplished to correct weaknesses or deficiencies noted during an assessment of security controls to reduce or eliminate known vulnerabilities in the information system. A POAM details resources required to accomplish specific elements of the plan, identifies milestones essential in meeting the tasks, and formalizes scheduled completion dates for the milestones. Additionally, a POAM allows the agency to track vulnerabilities identified by security controls assessments, security impact analysis’, continuous monitoring activities, self-assessments, internal inspections, and external audits.

Security Assessment
An assessment of security controls of the information system and its operational environment to determine if the controls have been implemented correctly, are operating as intended, and producing desired outcomes according to established security requirements.

Security Authorization
The authorization decision made to commence information system operations and accept all risk to agency assets and operations based on the implementation of agreed-upon security controls. Security authorizations decisions are usually made by the system owner (e.g. senior-level Agency executives or management).
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 Assessment and Authorization Policy and Procedures (CA-1).**
The agency will develop, document, disseminate, review, and annually update a security assessment and authorization policy and procedures.

4.2. **[IAL1, IAL2] Security Assessments (CA-2).** The agency will develop a security assessment plan that describes the scope of the assessment including security controls to be assessed, assessment environment, assessment procedures used to determine the effectiveness of security controls, and assessment team, including roles and responsibilities. The agency will perform security control assessments, in accordance with the security assessment plan, initially (prior to the information system being placed into the production environment), on an annual basis thereafter, and after a critical information system upgrade to determine if security controls are implemented correctly, operating as intended, and producing the desired outcome to meet security requirement. The agency will document security assessment results in a report and provide the report to the agency’s authorizing official.

4.2.1. **[IAL2] Independent Assessors (CA-2.1).** The agency will employ assessors or assessment teams that have an appropriate level of independence to perform security control assessments. The authorizing official will determine the level of independence required based on the ultimate risk to agency operations, assets, and personnel.

4.3. **[IAL1, IAL2] System Interconnections (CA-3).** The agency will authorize dedicated connections from the information system to other information systems via Interconnection Security Agreements (ISA), or other similar agreement, and annually review and update dedicated connections and their associated connection agreements.
The agency will document connection interface characteristics, security requirements, and nature of the information being communicated for each interconnection. System interconnections should be terminated when the agency business case no longer requires the system interconnection, the authority to operate an interconnected system is withdrawn, or ISA (or other similar agreement) expires. Upon terminating a system interconnection, relevant security controls should be re-assessed and appropriate security documentation should be updated (e.g. Risk Assessments, Contingency Plans, System Security Plans, Incident Response Plans).

4.3.1. [IAL2] Restrictions on External System Connections (CA-3.5). The agency will employ a deny-all/allow-by-exception policy when allowing the information system to connect to external information systems.

4.4. [IAL1, IAL2] Plan of Action and Milestones (CA-5). The agency will develop a Plan of Action and Milestones (POAM) for the information system to document planned remedial actions and update the POAM on a quarterly basis, as required, based on findings from security controls assessments, security impact analyzes, and continuous monitoring activities.

4.5. [IAL1, IAL2] Security Authorization (CA-6). The agency will (i) assign an authorizing official (e.g. senior-level executive or manager) for the information system, (ii) ensure authorization is granted by the authorizing official for information system processing prior to commencing operations, and (iii) update the security authorization every three (3) years or whenever there is a significant change to the information system.

4.6. [IAL1, IAL2] Continuous Monitoring (CA-7). The agency will develop, implement and maintain a continuous monitoring program that establishes the metrics and frequency of monitoring activities, correlates and analyzes information generated by assessment and monitoring activities, defines response actions for addressing analysis results, and reports the security status of information systems to appropriate personnel.

4.6.1. [IAL2] Independent Assessment (CA-7.1). The agency will employ assessors or assessment teams that have an appropriate level of independence to monitor information system security controls. The authorizing official will determine the level of independence required based on the ultimate risk to agency operations, assets, and personnel.

4.7. [IAL2] Penetration Testing (CA-8). The agency will perform periodic penetration testing on information systems and system components. The agency should contact ETSS to perform penetration testing of information systems and system components on the state network.

4.8. [IAL1, IAL2] Internal System Connections (CA-9). The agency will authorize internal connections of information system components (or class of components) to the information system and document the internal connection interface characteristics,
security requirements, and nature of the information being communicated for each interconnection.

5. Approval / Review Signature:

Brian Tardiff

Digitally signed by Brian Tardiff
Date: 2020.09.14 12:15:11 -04'00'

Chief Information Security Officer