Enterprise Technology Strategy and Services Policy 10-25
Risk Assessment Policy
Last Revision: 9/11/2020

1. Purpose

Establish policy that effectively manages inherent risk, vulnerabilities, threats, and countermeasures based on the criticality of the information system and data to ensure its confidentiality, integrity, and availability, and achieve an acceptable level of enterprise risk.

2. Applicability

This policy is applicable to all State of Rhode Island Executive Branch Departments (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

Privacy Impact Assessment (PIA)
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.

Risk Assessment
A determination of risk, including likelihood and impact estimates, from potential threats and vulnerabilities that result in a compromise in the confidentiality, integrity, and availability of information systems and data they process, store, and transmit.

Security Categorization
A level of risk (category) that is assigned to information systems and data based on risk assessments and the potential of specific events to impact individuals, systems operations, and State assets should the confidentiality, integrity, and availability of information systems and data be compromised.

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.
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] Risk Assessment Policy and Procedures (RA-1). The agency will develop, document, disseminate, review, and annually update a risk assessment policy and procedures.

4.2. [IAL1, IAL2] Security Categorization (RA-2). The agency will (i) categorize the information system and data in accordance with federal and state laws, regulations, policies, and standards, (ii) document security categorization results within the information system security plan, and (iii) ensure the security categorization is reviewed and approved by the agency authorizing official.

4.3. [IAL1, IAL2] Risk Assessment (RA-3). The agency will (i) perform a risk assessment, including the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification or destruction of the information system and the information it processes, stores, or transmits, (ii) document risk assessment results within the information system security plan, (iii) disseminate the system security plan to appropriate agency personnel, and (iv) review and update risk assessment results annually or whenever there is a significant change to the information system or its operational environment. Risk assessments will be performed in accordance with ETSS Information Technology Security and Risk Program Management (PM-1).

4.4. [IAL1, IAL2] Vulnerability Scanning (RA-5). The agency will (i) scan for vulnerabilities in information systems and hosted applications in accordance with their assigned security categorization, but no less than monthly, and when new vulnerabilities potentially affecting the system or application are identified and reported, (ii) employ
vulnerability scanning tools that facilitate interoperability among tools and automate parts of the vulnerability management process (e.g. use standards for enumerating platforms, software flaws, and improper configurations, format checklists and test procedures, and measure vulnerability impact), (iii) analyze vulnerability scan reports and results from security controls assessments, (iv) remediate vulnerabilities within appropriate time frames in accordance with risk assessments, and (v) share vulnerability scan and security control assessment results with appropriate personnel to help mitigate similar vulnerabilities in other information systems.

4.4.1. [IAL2] Update Tool Capability (RA-5.1). The agency will employ vulnerability scanning tools that provide the capability to readily update the information system to be scanned.

4.4.2. [IAL2] Update by Frequency, Prior to New Scan, When Identified (RA-5.2). The agency will update the information system vulnerabilities scanned quarterly, prior and when new vulnerabilities are identified and reported.

4.4.3. [IAL2] Privileged Access (RA-5.5). The information system will implement privileged access authorization for authenticated vulnerability scans and if it contains confidential or other sensitive data.

5. Approval / Review Signature:

Brian Tardiff

Digitally signed by Brian Tardiff
Date: 2020.09.14 12:18:40 -04'00'

Chief Information Security Officer