1. Purpose
Establish policy that ensures information system users are aware of current threats to information security and are adequately trained to perform their assigned roles and responsibilities in a manner that maintains system security. An on-going security awareness and training program that exposes employees and system users to current information security threats, creating strong passwords and maintaining password security, common elements of an email phishing scam, and how to properly handle sensitive data is critical to maintaining 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. Procedures for Compliance

<table>
<thead>
<tr>
<th>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.</th>
</tr>
</thead>
</table>
| **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. |

\(^1\) 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.
3.1. \textit{[IAL1, IAL2]} Security Awareness and Training Policy and Procedures (AT-1). The agency will develop, document, disseminate, review, and annually update a security awareness and training policy and procedures.

3.2. \textit{[IAL1, IAL2]} Security Awareness Training (AT-2). The agency will provide basic security awareness training to information system users as part of initial training for new users, when required due to information system changes, and annually thereafter.

3.2.1. \textit{[IAL2]} Insider Threat (AT-2.2). The agency will include security awareness training regarding the recognition of potential indicators of insider threats (e.g. repeated attempts to access systems not relevant to job duties, unexplained access to financial resources, workplace violence or harassment).

3.3. \textit{[IAL1, IAL2]} Role-Based Security Training (AT-3). The agency will provide personnel assigned security roles and responsibilities critical to maintaining the security, management, operational, and technical integrity of information systems with role-based training tailored to their assigned duties prior to authorizing access to the information system to perform assigned duties, when required due to information system changes, and annually thereafter. Privileged users, third-party providers, and stakeholders should be trained, as appropriate, to understand their roles and responsibilities in regard to securing information systems and data in accordance with DoIT and agency policies, procedures, agreements, and guidelines.

3.4. \textit{[IAL1, IAL2]} Security Training Records (AT-4). The agency will document security awareness and training activities of all information system users and retain the training records for as long as they’re employed by the state or required by law.

4. Approval / Review Signature:

\begin{center}
Brian Tardiff \hspace{1cm} Digitally signed by Brian Tardiff
Date: 2020.09.14 12:21:09
-04'00'
\end{center}

Chief Information Security Officer