Procedure - Information Security

Purpose
The purpose of this procedure is to set the management direction for information security by creating a structure, setting philosophy for consideration, and establishing initial rules for implementing procedures and/or guidelines, manuals, and/or operating practices in the areas defined by Board Policy 6550.

Philosophy of Protection
ESD's protection philosophy is comprised of four pillars:

1. Security is everyone's responsibility. Maintaining an effective and efficient security posture for ESD requires a proactive stance on security issues from everyone. Security is not "somebody else's problem;" ESD employees and contractors have the responsibility to adhere to the information security policies and procedures of the ESD and to take issue with those who are not doing the same.
2. Security permeates the ESD agency. Security is not just focused on physical and technical "border control." Rather, ESD seeks to ensure reasonable and appropriate levels of security awareness and protection throughout the organization and infrastructure. There is no place where security is not a consideration.
3. Security is a business enabler. A strong security foundation, proactively enabled and maintained, becomes an effective market differentiator for our company. Security has a direct impact on our viability within the marketplace and should be treated as a valued commodity.
4. Defense is achieved through depth. Defense in depth is achieved when information and information assets are protected against attacks through the balanced application of security services such as: availability, integrity, authentication, confidentiality, and non-repudiation. The application of these services should be based on the "protect, detect, delay and react" paradigm. This means that in addition to incorporating protection mechanisms, ESD must expect attacks and include intrusion detection tools and operating practices that allow a timely response to and recovery from these attacks. An important principle of the defense in depth tenet is that achieving it requires a balanced focus on three primary organizational elements: people, technology and operations.

The pillars of ESD's philosophy of protection are mutually supportive; ignoring any one pillar in favor of another undermines the overall security posture of the organization.

Information Security Risk Management
Information security requirements will be determined through a methodical assessment of risks. The ESD will then balance the costs employed with implementing information security controls and mechanisms against the potential harm that could result from a security failure of the ESD system.

When conducting risk assessments, the following must be considered:

- Harm to the business as a result of a security failure, considering potential consequences of a loss of confidentiality, integrity and/or availability of information or other assets
- The likelihood of a failure occurring in light of existing threats and vulnerabilities, and the security controls and mechanisms implemented in the ESD system environment

Following a comprehensive risk assessment, the appropriate actions and priorities for managing information security risks in the ESD system environment can be determined.

Selecting Appropriate Security Controls and Mechanisms

Once information security requirements are identified, ESD will evaluate and select appropriate security controls and mechanisms to be deployed to ensure risks are mitigated to an appropriate level as determined by Cabinet.

Appropriate security controls and mechanisms will be evaluated and selected based on the costs associated with implementing them in relation to the risks being mitigated and the potential losses that could result if a security breach occurs. The potential loss of customer trust and confidence (ESD reputation) will be factored in when selecting appropriate security controls and mechanisms.

Information Security Procedure Reviews

Reviews of information security procedures, risks, and the implemented controls and mechanisms will be conducted annually to:

- Address changes to business requirements and priorities
- Consider new threats and vulnerabilities that might exist
- Confirm that security controls and mechanisms remain effective and efficient

Timeline for Implementation of Procedure

Given the required changes to ESD processes to fully implement this procedure, new technology systems will be subject to this procedure immediately while existing processes or systems will be reviewed as required by the procedure's periodic review. If an operating practice is needed from IT as part of the procedure, IT will develop and have implemented that process before running proposed technology system through it. Procedure to be fully implemented by September 1, 2024.