Procedure - Organization of Information Security

Purpose
The purpose of this procedure is to assign responsibility for information security to all relevant job roles. It will also adopt security guidelines for when employees access, process and store information while working remotely.

Roles and Responsibilities
ESD defines the following roles:

Designated Information Security Officer (ISO)
The superintendent will designate the IT director as the information security officer.

The Information Security Officer is a senior-level employee of the ESD who oversees the information security program. Responsibilities of the Information Security Officer include the following:

- Developing and implementing an agency-wide information security program.
- Documenting and posting information security policies and procedures.
- Coordinating the development and implementation of an agency-wide information security training and awareness program.
- Coordinating a response to actual or suspected breaches in the confidentiality, integrity, or availability of agency data.

Data Owner
A data owner is a management-level employee of the ESD who oversees the lifecycle of one or more sets of agency data. Responsibilities of a data owner include the following:

- Assigning an appropriate classification to agency data.
- Determining the appropriate criteria for obtaining access to agency data.
- Ensuring that data custodians implement reasonable and appropriate security controls to protect the confidentiality, integrity, and availability of agency data.
- Understanding and approving how agency data is stored, processed, and transmitted by the agency and by third-party agents of the agency.
- Understanding how agency data is governed by ESD policies, state and federal regulations, contracts, and other legal binding agreements.

Data Custodian
A data custodian is an employee who has administrative and/or operational responsibility over ESD data. In many cases, there will be multiple data custodians. A data custodian is responsible for the following:

- Understanding and reporting on how agency data is stored, processed, and transmitted by the agency and by third-party agents of the ESD.

- Implementing appropriate physical and technical safeguards to protect the confidentiality, integrity, and availability of agency data.
- Documenting and disseminating administrative and operational procedures to ensure consistent storage, processing, and transmission of agency data.
- Provisioning and deprovisioning access to agency data as authorized by the data owner.
- Understanding and reporting on security risks and how they impact the confidentiality, integrity, and availability of agency data.

User

For the purpose of information security, a user is any employee, contractor, or third-party agent of the agency who is authorized to access agency information systems and/or agency data. A user is responsible for the following:

- Adhering to policies, guidelines, and procedures pertaining to the protection of agency data.
- Reporting actual or suspected vulnerabilities in the confidentiality, integrity, or availability of agency data to a manager or Information Technology.
- Reporting actual or suspected breaches in the confidentiality, integrity, availability, privacy of agency data to Information Technology.

Separation of Duties

Care will be taken that no single person can perpetrate fraud in areas of single responsibility without being detected. The initiation of an event should be separated from its authorization.

- It is important to segregate activities that require collusion in order to defraud, e.g. developing software and administering production systems.
- If there is a danger of collusion, then controls need to be devised so that two or more people need to be involved, thereby lowering the possibility of conspiracy.
- As a general rule, application developers and IT support personnel will not have access to the underlying operating system or to databases as administrators. Likewise, systems administrators will not have access to applications or databases, nor will database administrators have access to the application or operating system as an administrator. This will prevent one person from subverting critical applications or processes.

Telecommuting and Remote Access

Remote connections to the ESD network may be made by mobile devices at public places under the following provisions.

- Public places are defined as any place outside an ESD facility and include, but are not limited to hotels, hot spots at food or drink establishments, airports or train stations, employee's or other people's homes, government or partner facilities.
- Users must protect the ESD's information assets against the possible threats associated with telecommuting. These threats include theft of the remote computing devices and unauthorized access to ESD's computing facilities.
- This procedure applies equally to the connection to the ESD network and connections to ESD information assets within the network.

- IT will develop, implement, and review operating practices for mobile devices connecting to the ESD network. IT will set the approved methods for system remote access.

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.