Procedure - Human Resource Security

Purpose
The purpose of this procedure is to establish controls on the hiring, training, and termination of all personnel (e.g. employees, contractors) to enforce compliance with the information security policy, procedures, and any other guidelines, manuals, and operating practices to protect the ESD's information assets.

Personnel Screening Policy
ESD conducts background checks of all employees in accordance with Policy 5005 upon hiring.

Confidential Information Handling
ESD expects that information disclosed to ESD employees will be treated with the appropriate level of confidentiality. Except as required by law or expected for job performance, information concerning the ESD's confidential information is not to be discussed with others and e-mails containing information on the ESD's business to anyone outside of the ESD or otherwise transmitting ESD-confidential information outside of the ESD, whether over the Internet or otherwise.

Information Security Education and Training
All employees will be appropriately trained in the ESD's information security operating practices and kept up to date on any additions or changes to the operating practices. Training is mandatory prior to receiving access to information or services.

Human Resources is responsible for initial training and education on the organization's security policies during the employee orientation process. Employees should have recurring annual refresher training on current threats, as well as material changes to operating practices.

Reporting Security Incidents
ESD will educate employees on and establish formal reporting and feedback procedures and incidence response procedures for all security incidents. In this way, ESD will react to all security incidents immediately and provide all employees with the information necessary to assist the ESD in doing so immediately.

All suspected policy violations, system intrusions, virus infestations and other conditions that might jeopardize ESD information or ESD information systems shall be immediately reported to the Information Security Officer.

If an employee learns that ESD confidential information has been lost, disclosed to unauthorized parties, or is suspected of being lost or disclosed to unauthorized parties, the employee shall immediately notify the Data Owner of the information or the Information Security Officer.

The Information Security Officer will inform employees how to report possible incidents by providing information to the Human Resources Director to be included in the initial training material.

Incidents will be reviewed for the purposes of learning how they can be avoided in the future.

Reporting Security Weaknesses
ESD requires all users to immediately report suspected security weaknesses in, or threats to, systems or services to management or service providers. These weaknesses should only be reported if actually discovered by the user.

Only users authorized by the Information Security Officer may test systems for suspected security weaknesses. Any unauthorized testing by users shall be considered misuse of the system and be subject to disciplinary measures.

Disciplinary Process
ESD will follow Policy 5281 for appropriate disciplinary actions for violating security policy or causing a security breach.

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.