Policy: 6550-P4
Section: 6000 – Management Support

Procedure - Asset Management

Purpose

The purpose of this procedure is to determine the protective controls associated with each ESD information asset and to provide a foundation for all employees (and contractors, third parties, etc. who deal with information assets) to the security and handling of such assets.

Information Classification

Data classification, in the context of information security, is the classification of data based on its level of sensitivity and the impact to the district should that data be disclosed, altered, or destroyed without authorization. The classification of data helps determine what baseline security controls are appropriate for safeguarding that data. All district data should be classified into one of three sensitivity levels, or classifications:

Confidential

Data should be classified as confidential when the unauthorized disclosure, alteration, or destruction of that data could cause a significant level of risk to the district or its affiliates. Examples of confidential data include data protected by state or federal privacy regulations and data protected by confidentiality agreements. The highest level of security controls should be applied to confidential data.

Example: Student data, Cardholder data

Sensitive

Data should be classified as sensitive when the unauthorized disclosure, alteration, or destruction of that data could result in a moderate level of risk to the district or its affiliates. By default, all district data that is not explicitly classified as confidential or public data should be treated as sensitive data. A reasonable level of security controls should be applied to sensitive data.

Example: Salaries

Data classified as sensitive may be disclosable as public record under RCW 42.56. However, the sensitivity level of the data can warrant the assigned data classification and associated safeguard security controls.

Public

Data should be classified as public when the unauthorized disclosure, alteration, or destruction of that data would result in little or no risk to the district and its affiliates. Examples of public data include information intended for broad use within the district community at large or for public use. While little or no controls are required to protect the confidentiality of public data, some level of control is required to prevent unauthorized modification or destruction of public data.

Example: Board minutes

Information Labeling and Handling
It is important that an appropriate set of rules are defined for information labeling and handling in accordance with the classification scheme adopted by ESD. These procedures must cover information assets in physical and electronic formats. For each classification, handling procedures should be defined to cover the following types of information processing activity;

- Copying
- Storage
- Transmission by post, fax, and electronic mail
- Destruction

The Information Security Officer sets the rules as part of the operating practices for labeling and handling.

Handling and Protection Rules
Each asset classification shall have handling and protection rules. These rules must cover any media the assets may reside in at any time.

Unless it has specifically been designated as “Public”, or “Sensitive”, all ESD information assets shall be assumed to be confidential and shall be protected from disclosure to unauthorized third parties.

Handling and protection rules must include all parts of an asset’s life-cycle, from creation/installation through use and finally to destruction/disposal. Sensitive information or systems must be appropriately disposed of when no longer needed.

The Information Security Officer sets the rules as part of the guidelines, manuals, and operating practices for labeling and handling.

Information Retention
Information shall not be retained any longer than as defined in RCW 40.14 and the agency requires it to be retained. This reduces the window of time that data can potentially be available for misuse. Controls should be implemented to delete data that exceeds required retention time.

Ownership of Assets
All information assets must be assigned a Data Owner. Ownership shall be assigned when the assets are created.

Acceptable Use of Assets
Board Policy 2022: Electronic Resources and Internet Safety is the ESD’s acceptable use policy for use of information systems. All employees acknowledge the policy before network and email credentials are issued.

Return of Assets
All employees and external party users will return any ESD and information assets upon termination of their employment, contract or agreement. This obligation will be extended to relevant agreements with staff, contractors and others. In coordination with the data owner, the Information Security Officer sets the operating practices for return of assets.

Removable Media
IT sets the operating practices for removable media, including transfer and disposal. The operating practices shall account for the information asset classification scheme. Removable media should only be allowed if there is a justified business reason.

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.