High Desert
Education Service District

Code: **EHB-AR**
Adopted: 12/12/2023

CYBERSECURITY

Throughout its lifecycle, an information system that stores, processes or transmits ESD data shall be protected in a manner that is considered reasonable and appropriate, as defined in documentation approved and maintained by the Technology Services Department, given the level of sensitivity, value, and criticality that the ESD data has to the ESD.

Individuals who are authorized to access ESD data shall adhere to the appropriate Roles and Responsibilities, as defined in this administrative regulation.

Roles and Responsibilities
"Designated Information Security Officer (ISO)" means an employee designated by the superintendent to oversee the information security program. The ISO will be a senior-level employee in the ESD. The responsibilities of the ISO include the following:

1. Developing and implementing an ESD-wide information security program;

2. Documenting and disseminating information security policies and procedures;

3. Coordinating the development and implementation of required information security training and awareness program for staff and administrators;

4. Coordinating a response to actual or suspected breaches in the confidentiality, integrity or availability of ESD data and following statutory requirements;

5. Implementing Multi-Factor Authentication (MFA) for logins, and;

6. Implementing an information security audit program.

"Data owner" means a management-level employee of the ESD who oversees the lifecycle of one or more sets of ESD data. Responsibilities of a data owner include the following:

1. Assigning an appropriate classification to ESD data;

2. Determining the appropriate criteria for obtaining access to ESD data;

3. Ensuring that data custodians implement reasonable and appropriate security controls to protect the confidentiality, integrity and availability of ESD data;

4. Understanding and approving how ESD data is stored, processed, and transmitted by the ESD and by third-party agents of the ESD; and

5. Understanding how ESD data is governed by ESD policies, state and federal regulations, contracts and other legal binding agreements.

"Data custodian" means an employee of the ESD 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:

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

2. Implementing appropriate physical and technical safeguards to protect the confidentiality, Integrity and availability of ESD data;

3. Documenting and disseminating administrative and operational procedures to ensure consistent storage, processing and transmission of ESD data;

4. Provisioning and deprovisioning access to ESD data as authorized by the data owner;

5. Understanding and reporting on security risks and how they impact the confidentiality, integrity, and availability of ESD data;

6. Backing up data daily; and

7 Forcing email and domain passwords to expire at least annually.

"User," for the purpose of information security, means any employee, contractor, or third-party agent of the ESD who is authorized to access ESD Information Systems and/or ESD data. A user is responsible for the following:

1. Adhering to policies, guidelines, and procedures pertaining to the protection of ESD data;

2. Reporting actual or suspected vulnerabilities in the confidentiality, integrity, or availability of ESD data to a manager or the Technology Services Department; and

3. Reporting actual or suspected breaches in the confidentiality, integrity, or availability of ESD data to the Technology Services Department.

Classification of Information

Data classification, in the context of information security, is the classification of data based on its level of sensitivity and the impact to the ESD 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 ESD data should be classified into one of three sensitivity levels or classifications: confidential, sensitive and public. In some cases, data could fall into multiple categories, e.g., salary information.

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 ESD 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. Examples: student data, evaluation, and disciplinary records.[1]

[1] These examples are for information security purposes and may not be consistent with record request and disclosure requirements.

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 ESD or its affiliates. By default, all ESD 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 private data. Examples: salary information and staff personal contact information.

Data classified as sensitive may be disclosable as public record under Oregon Revised Statute (ORS) Chapter 192. However, the sensitivity level of the data can warrant the assigned data classification and associated safeguard security controls.

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 ESD and its affiliates. Examples of public data include information intended for broad use within the ESD 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. Examples: board minutes and policies.

Online Services and Applications

ESD employees are encouraged to research online services or applications to support the pursuit of ESD objectives. However, ESD employees are prohibited from installing or using applications, programs or other software, or online systems/websites that store, collect or share confidential or sensitive data, until the Information Security Officer (ISO) approves the vendor and software or service. Before approving the use or purchase of any such software or online service, the ISO, or designee, shall verify that it meets the requirements of all applicable laws, regulations and board policies, and that it appropriately protects ESD data. This prior approval is required whether or not the software or online service is obtained or used without charge.

Implementation

The Technology Services Department is directed to develop operating policies, standards, baselines, guidelines, and procedures for the implementation of this administrative regulations to include, but not limited to, addressing data encryption, logical access control, physical access control, vulnerability management, risk management and security logging and monitoring.

Violations of Policy and Misuse of Information

Violations of this administrative regulation include, but are not limited to: accessing information to which the individual has no legitimate right; enabling unauthorized individuals to access information; disclosing information in a way that violates applicable policy, procedure or other relevant regulations or laws; inappropriately modifying or destroying information; inadequately protecting information; or ignoring the explicit requirements of data owners for the proper management, use and protection of information resources.

Violations may result in disciplinary action in accordance with ESD policies, procedures and/or applicable laws. Sanctions may include one or more of the following:

1. Suspension or termination of access;
2. Disciplinary action up to and including dismissal; and
3. Civil or criminal penalties.

Employees are to report suspected violations of this administrative regulation to the Information Security Officer or to the appropriate data owner. Reports of violations are considered sensitive information until otherwise designated.