Education Data System Security Management Standard

Why is an Education Data System Security Management Standard needed?

- The Educational Data System (EDS) is a public web portal that provides access to multiple State Educational Agency applications and data collections. EDS is a secure portal that provides appropriate access to systems, tools, and data based on a user's roles within their organization.
- The security of EDS is directly tied to the creation of user accounts and the roles assigned to those user accounts within organizations.
- EDS employs a distributed security model where each organizational entity within EDS is empowered through their security administrator to create user accounts, assign, and manage roles, and provide access to the data and systems for that specific organization.
- EDS contains sensitive and confidential data and users must be aware of their responsibilities in preventing unauthorized disclosure and abuse of data.
- This standard is established to ensure organizational entities are aware of their responsibilities in managing and maintaining security of the EDS portal and its applications.

Who does the standard apply to?

- Office of Superintendent of Public Instruction (OSPI) employees and contractors.
- All organizations or individuals having or requesting access to EDS.

What systems does this standard apply to?

- The Washington Educational Data System (EDS).

What are the District Data Security Manager's responsibilities?

- Assigning the District Data Security Manager (DDSM) role, the EDS Technical Support fulfils this role for OSPI and makes the initial DDSM assignment for an organization.
- All LEA organizations and ESD organizations are required to officially identify to OSPI at least one individual within that district assigned to be the DDSM for that organization. The organization Superintendent will provide this identification by signing and sending

the 'Appointment and/or Removal of DDSM Form to OSPI Customer Support approving the appointment of this individual to the role of DDSM.

What are the DDSM duties?

- The DDSM is responsible for the management of all EDS accounts, role assignment, security, and directory information for their organization and any affiliated public schools (child organizations).
    - The creation and management of EDS user accounts including username changes and password resets.
    - The appropriate assignment of roles.
    - Inactivate user roles when no longer appropriate.
    - Updating common and legal name of the district and all schools.
    - Adding and updating the official superintendent.
    - Adding and updating the official principal.
    - Adding and updating the official phone number(s), address(s), website, and email address of all schools within the organization.
    - Any employee or persons affiliated with an LEA wishing to access any non-public application available through the OSPI EDS portal will seek approval and access from the DDSM for that organization.
- Any DDSM requiring assistance or direction in the execution of their duties as Data Security Manager should contact OSPI Customer Support.
- It is necessary that the DDSM only provide access when requests are approved by the appropriate organizational level and the appropriate business need exists for access to confidential and/or sensitive data.
- The DDSM is responsible for ensuring all users with roles providing access to their organization are aware of and have provided consent to follow any district, state, or federal laws or policies governing acceptable use of data contained within EDS and applications within EDS. Persons wishing to report unacceptable use of data pertaining to the DDSM's organization should report violations directly to the District Data Security Manager of said organization.
- The DDSM is responsible for annually auditing the users who have access within their school district and child organizations to ensure only active employees have access.

What is the role of OSPI EDS Technical Support (formerly Customer Support)?

- Serve as the District Data Security Manager (DDSM) for:
    - OSPI and all other State or Federal agencies.

    - Other non-standard Educational Organizations with mutual agreement between OSPI and those organizations, such as but not limited to: Private Schools, non-school district/non-public school individuals, and non-profit organizations, etc.
    - Vendors or partners not directly associated with an LEA.
    - Higher Education including Washington State Universities, Community Colleges, Technical Colleges, or any other educational institution not directly associated with an LEA.
    - Any other individual or entity not directly associated with a Washington Public School Organization that needs access to EDS.
- Grant access to confidential or sensitive data only when requested by a supervisor or some other organizational leadership role and when appropriate business need exists for the access requested.

How do we manage Security, Proprietary Information, and Acceptable Use?

1. The following are examples of security and proprietary information:

- Usernames and passwords are considered confidential data and must be protected and may not be shared. Authorized users are responsible for the security of their passwords and accounts. Sharing passwords is strictly prohibited. EDS enforces password changes every 120 days.
- DDSM's are not permitted to change passwords over the phone without a documented method to authenticate the caller. Organizations are required to have a policy or standard in place that describes the process used to authenticate a caller to an account for password changes.

2. Unacceptable Use

The following are examples of prohibited activities and are considered security violations:

- sharing an EDS account (more than one person accessing one account);
- intentionally revealing your EDS account password to others or allowing use of your EDS account by others;
- accessing data of which the user is not an intended recipient; and
- circumventing user authentication or security of any system, or account.
- This is not intended to be a comprehensive list. Each organization should define within their acceptable use standards a comprehensive definition of acceptable use.
- DDSMs will never ask for a password over the phone.

3. What are the steps if a violation is reported to the DDSM?

- Organizations with a DDSM should have a standard in place that describes the process that will be used when a violation is reported to the DDSM.
- At a minimum, organization standards should make clear who is responsible for investigating and resolving reported violations and process associated with removing either temporary or permanent system access as a result of reported violations.

At the request of the DDSM, OSPI EDS Technical Support Team may discontinue a user's EDS access during an investigation or in response to a security breach.