ODE Information Security and Privacy Program Overview

Security through Education

The Oregon Department of Education (ODE) is a Family Educational Rights and Privacy Act (FERPA) compliant organization. We are required by law to collect and store student educational records and have done so for more than a decade. There has not been a single breach or exposure of personally identifiable information (PII) stored in ODE systems. ODE is responsible for securing its information systems and protecting the privacy of data collected, used, shared and stored by the Department.

This information is an asset that, like other important business assets, is essential to ODE's business and consequently needs to be diligently protected. Information security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and meet the legal and regulatory obligations of the department. In accordance with the Oregon Department of Administrative Services' (DAS) implementation of Oregon Revised Statute 182.122 Information Systems Security and in compliance with the DAS Information Security Policy 107-004-052, ODE employs a Chief Information Security Officer (CISO) and maintains a complete Information Security and Privacy Program.

The ODE Information Security and Privacy Program addresses information security and privacy by focusing on three distinct elements: people, processes, and technology. Each year this comprehensive Program is updated to include initiatives focused on these three elements.

People

The risk of human error and misuse of information and equipment is an ever present risk in all organizations. To address this element, the ODE Program focuses on a range of training and education opportunities including

- annual mandatory information security and privacy fundamentals training;
- monthly security and privacy newsletters and "just in time" security bulletins published by the CISO; and
- targeted information security training for specific groups within the agency and our partner organizations (e.g., Information Security and Privacy Training for District Security Administrators, Special Education Collections Coordinators).

In accordance with the Program, ODE employees must complete the annual mandatory training or access to ODE systems and networks will be terminated. Employees must also sign and obey Department and State Acceptable Use Policies and other related Information and Security Privacy policies.

Processes

Processes are the repeatable steps necessary to accomplish an organization's business objectives. The development, documentation, and implementation of effective processes are a key step in managing an effective information security and privacy program. The following examples demonstrate areas in which this element of the Program focuses:

- ODE monitors changes in state and federal regulations and updates ODE procedures to meet new requirements (e.g., recent changes to FERPA regulations).
- FERPA was recently reauthorized to include additional clarity around (and support for) the construction and use of Statewide Longitudinal Data Systems (SLDS). A Summary from ODE, with links to additional resources, is available at https://district.ode.state.or.us/wma/groups/itmanagers/2011-12/ferpa-summary.pdf.
- ODE maintains and enforces a series of policies related to information security, including:
    - 581-101 Handling Confidential Information
    - 581-108 Public Records Requests

  - 581-110 Building Security
  - 581-116 Personally Identifiable Student Information Acceptable Use Policy
  - 581-302 Purchase and Use of Department Hardware and Software
  - 581-308 Accessing Secure Rooms Containing Test Development Materials
  - 581-309 Information Asset Classification
  - 581-310 Information Security Policy
  - 581-515 State School Fund Database Access
- ODE does not mandate collection of Social Security Numbers for K-12 students. ODE is compliant with the Oregon Consumer Identity Theft Protection Act of 2007.
  - http://www.leg.state.or.us/07reg/measures/sb0500.dir/sb0583.en.html
  - http://www.cbs.state.or.us/dfcs/identity_theft/fact_sheet.pdf
- ODE conducts security audits against systems to make sure access and rights continue to be appropriate and meet the standard of minimum access necessary to complete work.
- ODE maintains Business Continuity and Disaster Recovery Plans.
- ODE executes data sharing agreements with partner state agencies. For example, ODE is in the initial stage of negotiating a data sharing agreement for Project ALDER. To date, no data have been shared between state agencies as part of this project.
- ODE conducts security reviews of any procurements and contracts involving data, hardware, information services, etc.

Technology

Technology is the third element of the ODE Information Security and Privacy Program. The technology element focuses on technologies that support the protection of the confidentiality, integrity and availability of the data and systems we are responsible for securing. Technology protections extend across the entire infrastructure of the ODE environment and are included at all levels including, but not limited to, database security, application security, network security, security of the hardware infrastructure (servers, desktops, laptops, etc.) and secure handling of information in all electronic formats.

In August 2010, the ODE data center was moved from the third floor of the Public Service Building in Salem to the Open Source Laboratory on the Oregon State University (OSU OSL) campus. Details are contained at these links:

- http://osuosl.org/services/hosting
- http://nces.ed.gov/whatsnew/conferences/MIS/2011/presentations/I_D_handout.pdf
- http://nces.ed.gov/whatsnew/conferences/MIS/2011/presentations/I_D.pdf

ODE has a co-location arrangement with OSU OSL. This means that staff at OSU OSL have no access to ODE systems or data. OSU OSL staff are responsible for maintaining the facility and related services (e.g., access, power, cooling) only. They do not maintain ODE equipment or hardware.

An exhaustive discussion of the details of ODE's security infrastructure would be inappropriate for a published document for security reasons. However, all appropriate means to protect the data we collect and handle are in place including, but not limited to:

- Encryption of data in transit and at rest
- Review and testing of application code for security issues
- Firewalls
- Access management for systems used by ODE employees and/or partner agencies
- Web blocking and monitoring implementation
- Patch management of all servers and end user workstations
- Backup and offsite secure storage
- Asset management

Education Information Security Council (EISC)

In addition to maintaining a comprehensive Information Security and Privacy Program for the department, in the fall of 2011, the ODE CISO initiated a collaborative effort with the school districts and education service districts (ESDs) to launch a statewide Education Information Security Council. Visit the Education Information Security Council page to read the group's charter, review meeting minutes, and see work products.

In addition to collaboration with the EISC, the Oregon Department of Education continues to collaborate with all organizations with which we work to meet state and federal requirements around data collection and data sharing. The Department's commitment to information security and privacy is prevalent throughout our people, processes and technology.

State Privacy Laws and Rules

Oregon Consumer Identity Theft Protection Act (2007), ORS 646A.600-628

The Oregon Consumer Identity Theft Protection Act, enacted by the 2007 legislature, means consumers will have more tools to protect themselves against identity theft, and Oregon businesses and government will have clear direction and expectations to ensure the safety of the personal identifying information they maintain. Personal information includes a consumer's name in combination with a Social Security number, Oregon drivers license number or Oregon identification card, financial, credit or debit card number along with a security or access code or password that would allow someone access to a consumer's financial account.

Oregon Revised Statute: http://www.leg.state.or.us/ors/646a.html

State Administrative Agencies Information Systems Security, ORS 182.122

The Oregon Department of Administrative Services has responsibility for and authority over information systems security in the executive department, including taking all measures reasonably necessary to protect the availability, integrity or confidentiality of information systems or the information stored in information systems. The Oregon Department of Administrative Services shall, after consultation and collaborative development with agencies, establish a state information systems security plan and associated standards, policies and procedures.

Agencies are responsible for the security of computers, hardware, software, storage media, networks, operational procedures and processes used in the collection, processing, storage, sharing or distribution of information outside the state's shared computing and network infrastructure following information security standards, policies and procedures established by the Oregon Department of Administrative Services and developed collaboratively with agencies. Agencies may establish plans, standards and measures that are more stringent than the standards established by the department to address specific agency needs if those plans, standards and measures do not contradict or contravene the state information systems security plan. Independent agency security plans shall be developed within the framework of the state information systems security plan.

Oregon Revised Statute: http://www.leg.state.or.us/ors/182.html

Department of Administrative Services (DAS), Enterprise Security Office (ESO)

The goal of information security is to protect the confidentiality, integrity, and availability of information assets. ORS 182.122 (House Bill 3145, 2005 Legislative Session) designates DAS as the "single point of accountability" for information security at the state.

In support of this mandate, the Enterprise Security Office (ESO) is instituting a security strategy wherein DAS works collaboratively with state agencies to ensure the state's security posture is at an acceptable level. Information security management enables information to be shared while ensuring protection of that information and its associated technology assets.

Enterprise Security Office: http://www.oregon.gov/DAS/EISPD/ESO/
ESO Information Security Plan: http://oregon.gov/DAS/EISPD/ESO/Pub/InfoSecurityPlan_2009_FinalApproved_092809.pdf
ESO Information Security Standards: http://oregon.gov/DAS/EISPD/ESO/Pub/InfoSecurityStandards_2009_12_Final.pdf

Oregon Department of Education, Information Security and Privacy Program

The Oregon Department of Education's Information Security and Privacy Program is responsible for ensuring ODE complies with standards and regulations related to information security and privacy, and for educating employees about best practices, acceptable use policies and threats to information security. The Program provides annual information security training to all personnel.

As a component of this Program, the CISO publishes the monthly *InfoSec Insider* newsletter and periodic *Security and Privacy Bulletins*. The monthly newsletter is intended to increase employee awareness. The newsletter will inform staff about different kinds of information security threats and hazards and provide tips to better protect the sensitive data with which we work. For immediate threats, staff will receive *Security and Privacy Bulletins*. The bulletins will provide timely information related to specific potential issues.

Governing Statewide Statutes and Rules

Number	Title	Effective Date
ORS 646A.600 – 626	Oregon Revised Statute – Oregon Consumer Identity Theft Protection Act	2007
ORS 182.122	Oregon Revised Statute – Information systems security in executive department; rules	2005
ORS 291.038	Oregon Revised Statute – State agency planning, acquisition, installation and use of information and telecommunications technology; integrated videoconferencing; online access service; Stakeholders Advisory Committee; rules	2003
ORS 184.305	Oregon Revised Statute – Purpose and authority of the Oregon Department of Administrative Services to provide centralized services, provide rules and oversight of policy compliance by agencies, etc.	1993
ORS 291.037	Oregon Revised Statute – Legislative findings on information resources identifying that information is a strategic asset of the state and allowing for centralized establishment of rules and standards for information management.	1991
OAR 125-800-0005	Oregon Administrative Rule, Division 800, State Information Security – Purpose, Application, and Authority	12/28/2006
OAR 125-800-0010	Oregon Administrative Rule, Division 800, State Information Security – Definitions	12/28/2006
OAR 125-800-0020	Oregon Administrative Rule, Division 800, State Information Security – State Information Security	12/28/2006
DAS 107-004-110	DAS Statewide Policy – Acceptable Use of State Information Assets	1/01/2010
DAS 107-004-053	DAS Statewide Policy – Employee Security	7/30/2007

Oregon Department of Education Internal Policies

Number	Title	Effective Date
581-101	Handling Confidential Information	2006
581-110	Building Security	2006
581-111	Internal Audit Charter	2007
581-112	Audit Committee Charter	2007
581-116	Personally Identifiable Student Information Acceptable Use	2009
581-203	Telecommuting	2008
581-306	Remote Access	2007

581-308	Accessing Secure Rooms Containing Test Development Materials	2009
581-309	Information Asset Classification	2010
581-310	Information Security Policy	2010
--	Business Continuity Plan	2009

Questions

Questions about the Information Security and Privacy Program at the Oregon Department of Education should be directed to ode.infosec@state.or.us.