

# Administrative Policies

Policy Name: Information Security Policy  
 Number: IRM 7 (2)  
 Issuing Section: IT Services  
 Revision Date: 12/03/08  
  
 Issue Date: 02/12/09  
  
 Selected References:  
 Type: Amended  
 Policy Council Approval:  
 Staff Review:  
 Executive Team Review:  
 Policy & Procedure Administrator: Leslie Cummings  
 Information Security Program Manager  
 Contact Information: (503) 947-1622  
  
 Approval: Laurie A. Warner, Director

Policy:	The agency shall have in place procedures to make certain that information assets are protected to ensure confidentiality, integrity, and availability. The procedures describe agency methods for protecting information assets physically from unauthorized use or modification and from accidental or intentional damage or destruction and are used by authorized personnel for approved business purposes. The procedures cover the life span of information assets from creation through useful life and proper disposal.
Application:	This policy applies to all Oregon Employment Department information users including employees, contractors, vendors, consultants, volunteer workers, business partners and other authorized individuals accessing OED information resources.
Links:	<a href="#">DAS Policy for Acceptable Use of State Electronic Resources, 03-21</a> <a href="#">OED Confidentiality Manual</a> <a href="#">OED Commitment to Confidentiality Form 101</a> <a href="#">OED Policy, Collection and Disclosure of customer Information ADM 12 (1)</a>
Procedure Location:	<a href="#">General Security Practices</a> <a href="#">Employee Security</a> <a href="#">Mobile Communications/Computing Devices</a> Information Asset Classification: (link) Information Security Program: (link) <a href="#">Transporting Information Assets</a> <a href="#">Incident Response</a> Web Server, Network Access, Extranet: (link) Application Service Provider, Authentication Credentials: (link)
Responsibilities:	<a href="#">Information Security Responsibilities</a>

# Administrative Procedures

Procedure Name: General Security Practices  
 Accompanying Policy: Information Security Policy, IRM 7 (2)  
 Issuing Section: IT Services  
 Revision Date: 12/03/08  
  
 Issue Date: 02/12/09  
  
 Policy & Procedure Administrator: Leslie Cummings  
 Information Security Program Manager  
 Contact Information: (503) 947-1622  
  
 Approval: Leslie Cummings  
 Information Security Program Manager  
 Date: 02/12/2009

**Summary:** The purpose of this procedure is to provide information regarding OED's general security practices. It describes the following general security practices and includes procedural requirements for each topic:

1. Physical and Environmental Security
2. Access Control, Integrity, and Data Security
3. Network Security
4. Personal Use
5. Compliance, Reporting and Enforcement, and
6. Disaster Recovery Management

**Detail:** **1. Physical and Environmental Security**

Physical security practices prevent unauthorized physical access, damage, and interruption to OED information, systems, and other property. Physical security practices for each facility must be sufficient to protect the types of information and property housed in that facility. OED management and staff shall take the appropriate physical security measures to provide:

1. Management control of physical access by agency staff and others to information assets (including personal computer systems, computer terminals, and mobile devices) by agency staff and others.
2. Prevention, detection, and suppression of fires.
3. Prevention, detection, and minimization of water damage.
4. Protection, detection, and minimization of loss or disruption of operational capabilities due to electrical power fluctuations or failure.
5. Protection and minimization of loss from theft or damage.

**Procedural Requirements:**

**Secure Locations.** Host computers, servers and other essential computer devices such as routers and switches shall be stored in locations that protect them from

unauthorized physical access. Access control devices such as locks or key cards shall be used to secure these locations. Designated agency staff shall provide escort when non-authorized persons such as repair personnel require access.

**Location Selection.** Physical locations for all computer related equipment shall be selected to protect against equipment and information loss by theft, flood, fire, and other disasters.

**LAN Connection Points.** All unused LAN connection points (RJ45 jacks) shall be disabled by disconnecting them from hubs or switches.

**Review of New Connections to Outside Sources.** Proposed access to or from a network external to the agency must be reviewed and approved by the Security Administrator prior to establishment of the connection.

**Platform-specific Security.** Platform-specific security must be established, implemented and periodically reviewed and revised as necessary to address vulnerabilities of that platform. This shall be accomplished by the Technical Support Center for workstations and laptops, by the appropriate Data Administrator for data, and by the appropriate System Administrator for host computers and servers.

**Laptop, Notebook, and Portable Computer Devices.** Portable computing devices (mobile phones, palm pilots, diskettes, CDs, DVDs, flash drives, and other such devices) must not be left unattended at any time unless the device has been secured. Where possible when traveling, users shall keep OED portable computers and other portable devices with the carry-on hand luggage. All mobile computing devices shall be encrypted as specified in the Mobile Communications/Computing Device Policy.

**Network Connections.** Employment Department network connections to external networks may be established only by Information Technology Services Network Support staff. Such connections may only be established after technical review by the staff managing the office's wide area and local area network connections (Department of Administrative Services or Department of Human Services, and OED Information Technology Services, Network Support). The office manager shall make the review request by contacting the OED Network Support Unit. Furthermore, such connections may be established only with signed contracts between OED and the owners of the external network. These contracts must go through the normal agency contract clearance process.

## **2. Access Control, Integrity, and Data Security**

Information which has been inappropriately modified or destroyed (by employees or others) can adversely impact public policy or the rights of citizens. Consequently, the accuracy and completeness of information systems and the data maintained within those systems are a management concern. OED shall establish controls to ensure that data entered into and stored in its automated files and data bases are complete and accurate, as well as ensure the accuracy of disseminated information. Depending upon the nature of the information being protected and the threats to which it is subjected, additional measures may be required to ensure data integrity and security. Security measures to prevent unauthorized access include methods ranging from password protection to encryption.

**Procedural Requirements:**

**Access Control.** Access rights to computer services and information shall be authorized on the basis of strict "need to know" and the requirements of "least privilege".

**Identification and Authentication.** Authorized users shall be assigned unique user identifications for access to OED network and information systems. User identifications must be used only by the assigned user. Authorized users are responsible for activities taken using their assigned user identification and password. OED assigned user identifications shall not be used as personal user identifications outside of OED network systems (e.g., non-OED websites, Internet, Yahoo, AOL, etc.). User accounts shall not be shared.

- Group/Job Identification. In circumstances where there is a clear business need, an exception may be granted for assignment of unique identification for a group of users or a specific job. Approval for exception shall be obtained from the Information Security Office, documented, and reviewed annually. Additional controls may be required to maintain accountability.

**Password Policy.** Passwords are an important aspect of computer security used in combination with unique user identifications. They are the front line of protection for OED information systems. A poorly chosen password may result in the compromise of the OED's entire corporate network. As such, all OED employees (including contractors and vendors with access to OED systems) are responsible for taking the appropriate steps outlined in [password details](#) to select and secure their passwords.

**Use of Automatic Logons.** Authorized users shall not facilitate any logon procedure using keyboard macro programming or scripting.

**User Accounts.** New user accounts, changes to existing accounts, and account deletions shall be requested by management service personnel or authorized staff. The Network User Request Form (NURF) on EDWEB shall be used to make these requests. The user must have signed the Commitment to Confidentiality before the account is requested.

**Who Is Authorized to Have Accounts.** All OED staff are authorized for access to accounts for systems and applications required to perform their assigned duties. Business partners may be authorized to access systems and data based on applicable law and under established contractual agreements with OED. Authorized contractors and business partners needing accounts shall be granted access after signing the Commitment to Confidentiality, Appropriate Use, and OED Information Security forms. Contractor and business partner accounts shall be established with an expiration date and the access granted shall be the minimum access needed to perform work for OED. If the work is completed prior to the account expiration, the responsible manager must submit a Network User Change Request (NURF) to have the account deleted (or inactivated when the contractor is expected to return at a later date).

**Proxy Access.** The use of proxy access is allowed for email and calendaring systems when appropriately authorized.

**Generic Accounts.** Generic accounts are allowed only:

- For desktop and network log in to provide a minimal access login for certain PCs in field offices. This may be done when the access is

necessary to provide direct service to the public at a field office, front counter machine, and other approved exceptions (such as when the time needed for a worker to log in is not acceptable to the office manager due to PC sharing or quick rotation of front counter workers.)

- On networked PCs provided for public use (public display, resource room) for the purpose of printing to a nearby printer.

### **Software Control.**

**Acquisition, Development, and Maintenance.** OED must provide for the integrity and security of its information assets throughout their full life cycle beginning at acquisition and ending with appropriate disposal. Security is an integral component of all OED information technology activities. When implemented appropriately, security is a business enabler.

**Virus Protection.** All agency workstations shall be equipped with up-to-date virus protection software with established methods for keeping the software up-to-date. However, because virus scanning software is limited to the detection of identified viruses, and since new and more sophisticated viruses are being developed constantly, care must still be taken when accessing incoming email and files received from across the network or on floppy disks. Employees shall contact the Technical Support Center if they see evidence that a virus has been transferred to OED systems.

**Downloading Software.** Only approved software shall be used on OED computers. Employees shall not download or install software without prior approval and assistance from the Technical Support Center, including freeware or shareware. Questions regarding what constitutes approved software shall be referred to the Technical Support Center.

**Copyrights and Licensing of Software.** Software shall be fully licensed and obtained only from a reputable source. Obtaining system software, applications, and automated data files from user's groups, bulletin boards, the Internet, or other information services shall be done only in accordance with department policy by authorized staff. OED adheres to all copyright laws and commercial software licensing agreements. Copyrighted software shall not be illegally duplicated or used on any OED computer system. The Technical Support Center shall periodically perform an inventory of all software on each computer system and audit against the organization's license agreement records to ensure that no illegal copies of commercial software are installed on any equipment.

**Disposal of Computer Software and Data.** Disk drives or other storage media on all computers to be reassigned or discarded shall be reviewed and all OED data and copyrighted software shall be removed. If the storage media cannot be accessed because the computer system is inoperable, the storage media shall be removed and destroyed separately.

**Cryptography** - Encryption, or equally effective measures, is required for all OED information stored on portable electronic storage media (including but not limited to CDs and thumb drives) and on portable computing devices (including but not limited to laptop and notebook computers). This policy does not apply to mainframe and server tapes. Alternatives to encryption shall be reviewed on a case-by-case basis and approved in writing by the Information Security Program Manager.

**Confidentiality of Data.** Use of the OED network and authorized access provides all staff access to information that is confidential. All OED employees and other authorized users must read, sign and comply with the OED Commitment to Confidentiality.

**System Usage.** All OED employees and other authorized users are responsible for actions they perform on computer systems or that are performed using their User ID and password. All OED Employees and other authorized users shall read, sign and comply with the Acceptable Use Policy and OED Information Security Policy. Prohibited uses include:

- Attempts to gain unauthorized access to systems, applications, or data.
- Assisting others in attempts to gain unauthorized access to systems, applications, or data.
- Knowingly destroying or modifying data without permission.
- Intentional or negligent exposure of OED systems to malicious software (viruses or worms) or infected files
- Using OED computer resources for personal gain.
- Leaving a workstation or other computer system unattended and unsecured.

**State and Federal Access, Privacy, and Confidentiality Laws.** All information, regardless of the medium in which it is maintained or communicated, is subject to applicable State and federal law governing access, the protection of privacy and prohibitions against unauthorized disclosure.

**Employment Changes.** Managers must report changes in employment status or job duties of staff or business partners to the designated Information Security Administrator. Personnel reports regarding employee status changes must be regularly provided to the Information Security Administrator.

**Vendor/Contractor Agreements.** All contracts and vendor agreements shall contain a requirement that any OED information obtained as a result of such an agreement shall be the property of OED and shall not be used, released or disclosed, without written authorization.

**Auditing.** Where the system will support it, and where the performance of the system can be maintained at an acceptable level, the following audit trail events shall be recorded:

- User logons, both successful and failed
- Unsuccessful attempts to access objects (resources) or perform functions that are denied by lack of privileges or rights
- Changes to a user's security privileges/profiles
- Changes to the system security configuration
- Modification of system-supplied software
- Activities of a specified User ID

**System and File Backup.** Data and software essential to the continuation of mission critical functions shall be backed up nightly. End user files stored on servers shall be backed up nightly. All central computer systems files shall be backed up (full backup) on a regular schedule. Backup tapes or other media shall be stored off-site.

### 3. NETWORK SECURITY

Network security is essential to protect OED information from unauthorized access. OED's network security begins with a user authentication process that requires strong, regularly changed passwords. In addition, the network firewall controls access to agency information and access to external sites. There are several OED policies in place that govern internet and email usage. As a standard practice, OED reserves the right to monitor use of agency technology resources.

#### Procedural Requirements:

**Internet Acceptable Use Policy.** Department of Administrative Services (DAS) Policy 03-21 "Acceptable Use of State Electronic Resources" provides general State of Oregon policy on acceptable use of state electronic information systems. All OED employees shall read, sign and comply with this policy. The policy can be accessed on the OED internal web site: EDWEB.

**Personal email usage.** Incidental personal use of email is authorized provided it does not interfere with work or reflect unfavorably on OED. Racist, sexist, threatening, harassing or other inappropriate, discriminatory or derogatory language is strictly prohibited. Email shall not be used for any private commercial purposes or for any personal monetary interests or gain. Users' email is subject to state open records laws, and may be subject to future requests for public disclosure.

**Privacy Policy.** OED reserves the right to monitor and/or log all network and user activity with or without notice, including email and all web site communications. Therefore, users have no reasonable expectation of privacy in the use of OED information technology resources.

**Internet Firewall.** A firewall shall be placed between OED's network and the internet to protect internal network resources from being accessed except by trusted external sources, and to prevent internal users from accessing external services which pose significant security risks. Access to or from internal network resources shall be limited to that which is necessary to conduct OED business. The Security Administrator shall administer the firewall, and shall regularly audit and monitor Internet traffic to detect intrusion attempts. The firewall shall be configured to deny all services not expressly permitted. The specific **firewall rules** which have been adopted. Recommendations or requests for changes to the firewall rules shall be forwarded to the Security Administrator.

**Internet Access Exception Process.** Department of Administrative Services Policy 03-21 "Acceptable Use of State Electronic Resources" states in part: "The agency intends to trace, review, audit, access, intercept, block, restrict, screen, delete, recover, restore, publish, or disclose any information, at any time without notice."

It also states: "**Uses must be lawful and inoffensive.** Uses of agency systems must not be false, unlawful, offensive, or disruptive. Unless agency duty requires it, no use shall contain profanity, vulgarity, sexual content, or character slurs. No use shall make rude or hostile reference to race, age, gender, sexual orientation, religious or political beliefs, national origin, health, or disability. Copyrighted or licensed information shall be used only with full legal right to do so."

OED has, in accordance with this State of Oregon policy, blocked inappropriate Internet sites. Recognizing that no block list is perfect, the following exception

procedure may be followed to request a blocked site be opened for business purposes:

- When a website is blocked, a message to that effect shall be presented to the user with instructions and an option the user can select to request access to the blocked site.
- Submitted requests for access to blocked sites shall be evaluated by Information Technology Services. The requestor and requestor's supervisor shall receive an emailed response indicating either that the site was unblocked or the reason if the evaluation determines that the site should remain blocked.
- If the response from Information Technology Services indicates that the site shall remain blocked due to inappropriate content or a technical reason, and the requestor wishes to escalate the decision, requestor's next step is to take the issue to his or her supervisor for escalation to the appropriate Assistant Director for review and decision.

**Remote Access to Agency Information.** Remote external access to the OED network shall only be accomplished through approved methods implemented and maintained by the agency. The use of any non-agency system or device for remote access to OED data and information requires written approval from the Security Administrator prior to installation. Systems and devices shall be routinely (annually) evaluated for continued remote access needs, and for meeting current OED security requirements.

**Partner Networks.** Partner access to OED "partner network" systems and devices shall only be accomplished through OED approved methods implemented and maintained by the agency. Systems and devices shall be routinely (annually) evaluated for continued partner access needs, and for meeting current OED security requirements. A business case will be required for any exceptions and may only be granted through written approval from the Information Security Administrator.

#### 4. Personal Use

Information maintained in a personal computer system, including laptop computers and mobile devices, must be subjected to the same degree of management control and verification of accuracy that is provided for information that is maintained in central systems.

#### Procedural Requirements:

**Personal computer security.** Files containing confidential or sensitive data shall not be stored in personal computer systems unless it can be demonstrated that doing so is in the best interest of OED and that security measures have been implemented to provide adequate protection. Proposals to use desktop or laptop computers to maintain or access files containing confidential or sensitive data as defined in the ([Agency's Confidentiality Manual](#)), must be approved by OED's Information Security Program Manager before implementation. The Information Security Program Manager shall determine whether the proposal complies with applicable policy and law. Personal systems and devices shall be routinely (annually) evaluated for continued OED data or information access needs, and for meeting current security requirements.

#### 5. Compliance, Reporting and Enforcement

OED is required to comply with applicable laws and the information security and privacy policies, standards, and procedures issued by Department of Administrative Services. OED



shall report and file the appropriate compliance documents and shall adhere to the Information Security Reporting Requirements as identified in this policy.

### **Procedural Requirements:**

**Compliance.** All users are responsible for complying with this information security policy as well as all supporting procedures and practices. Anyone suspecting misuse or attempted misuse of information systems resources is responsible for reporting such activity to their managers and to the Security Administrator.

**Non-compliance.** Violation of standards, procedures, or practices in support of this policy may result in:

- Restriction, temporary suspension or termination of a user's access to computer and network resources.
- Disciplinary action up to and including termination in accordance with OED policy.

### **Incident Management.**

**Security Incident Reporting.** Upon discovery of any incident that meets the defined criteria below, all program areas must immediately report the incident following the OED Information Security Incident Notification and Reporting Instructions found in this policy. The [Security Incident Response](#) instructions are available via EdWEB. The report must be submitted to the Security Administrator within three working days of OED management or the Security Administrator becoming aware of an incident involving the compromised information (including information stolen in conjunction with the theft of a computer or data storage device).

OED's Information Security Program Manager must promptly investigate incidents involving loss, damage, misuse of information assets, or improper dissemination of information. All program areas are required to report information security incidents according to the security reporting requirements in this policy.

Any event which results in loss, disclosure, unauthorized modification, or unauthorized destruction of information resources constitutes a security incident. Anyone discovering a security incident shall:

- Preserve any evidence of the incident.
- Notify the appropriate supervisor/manager.
- Notify the Technical Support Center.
- Submit a Security Incident Report to the Information Security Office.

The Information Security Administrator and the appropriate system administrator for the computer system affected shall investigate the incident and make a report to the CIO with the following details:

- General nature of the security incident
- Computer systems involved in the security incident
- Details of the security incident
- Impact and potential consequences of the security incident
- Possible courses of action to prevent a repetition

**Criteria for Reporting Incidents.** The manager with oversight responsibility shall ensure that an OED Information Security Incident Report is filed for each incident. The report is signed by the responsible manager, and submitted to the Security Administrator within three business days from the date of notification. The responsible manager shall ensure that OED policy and procedure for notification to affected individuals are followed for incidents involving personally identifying information. In addition to notification, OED shall comply with all other legal requirements for incidents involving personally identifying information.

The Information Security Program Manager may require that the responsible manager provide additional information in conjunction with its assessment of the incident.

Incidents reported to the Oregon State Police Emergency Notification include, but are not limited to, the following:

- State Data (includes electronic, paper, or any other medium).
  - Theft, loss, damage, unauthorized destruction, unauthorized modification, or unintentional or inappropriate release of any data classified as confidential, sensitive or personal.
  - Possible acquisition of personal information by unauthorized persons.
  - Deliberate or accidental distribution or release of personal information by an OED employee(s), or its contractor(s), or its partner(s) in a manner not in accordance with law or policy.
  - Intentional non-compliance by the custodian of information with his/her responsibilities.
- Inappropriate Use and Unauthorized Access - This includes actions of state employees and/or non-state individuals that involve tampering, interference, damage, or unauthorized access to state computer data and computer systems. This includes, but is not limited to, successful virus attacks, web site defacements, server compromises, and denial of service attacks.
- Equipment - Theft, damage, destruction, or loss of state-owned information technology equipment, including laptops, tablets, integrated phones, personal digital assistants (PDA), or any electronic devices containing or storing confidential, sensitive, or personal data.
- Computer Crime – Use of a state information asset in commission of a crime as described in the Comprehensive Computer Data Access and Fraud Act.
- Incidents that violate OED policy.

**Enforcement.** Violation of standards, policies, procedures or practices may result in:

- Restriction, temporary suspension or termination of a user's access to computer and network resources.
- Disciplinary action up to and including termination in accordance with OED policy.

## **6. Disaster Recovery Management**

OED must establish a Business Continuity Program supported by executive management with necessary resources. The program shall ensure the appropriate steps are taken to identify the impact of potential losses, maintain viable recovery strategies and plans, and ensure OED has the ability to continue its essential functions during a business disruption or major catastrophic event. The program controls shall include procedures for regular backup of automated files and databases, risk management, mitigation measures, and methods to ensure business

continuation.

**Disaster Recovery Planning.** Disaster recovery planning provides for continuity of computing operations in support of critical business functions, minimizes decision-making during an incident, produces the greatest benefit from the remaining limited resources, and achieves a systematic and orderly migration toward the resumption of all computing services within OED following a business disruption. It is essential that critical IT services and critical applications be restored as soon as possible.

It is significant to recognize that no disaster recovery program is ever complete. All disaster recovery planning is based upon available knowledge and assumptions, and must be adapted to available funding, changing circumstances and business needs, as appropriate. Strategies, procedures, and resources must be adapted as often as necessary in order to maintain the ability to recover critical applications. Recovery strategies must be developed and updated routinely to anticipate risks including loss of utility (hardware, software, power, telecommunications, etc.), loss of access to the facility, and loss of facility.

The disaster recovery planning process supports necessary preparation to identify and document procedures to recover critical operations in the event of an outage. OED shall consider the results of their risk analysis process and their business impact analysis when developing their disaster recovery plan. Each program area's process shall culminate in a viable, fully documented, and tested disaster recovery plan.

To provide for recoverability of new systems, all program areas must include disaster recovery considerations and costs in project authority documents and budget proposals.

To improve the likelihood for the full recovery of key business processes, a disaster recovery plan shall be developed as part of a complete business continuity program which includes emergency response and business resumption plans.

**Definitions:** **Asset:** Anything that has value to the agency.

**Business partners:** Other State agency staff, such as Adult and Family Services or Vocational Rehabilitation employees; One Stop partners; nonprofit organization employees; or any other individual or entity who may work off site or in a co-located facility with Agency staff.

**CESN account:** A login to the state mainframe computer that authorizes the user to access programs and data, and that establishes a printer ID for mainframe printing.

**Contractors, business partners, vendors and vendor technicians:** Employees of companies or other organizations who are working for or with OED under contract or other agreement.

**Dial-in modem:** A **modem** that connects a personal computer to a standard telephone line for the purpose of receiving incoming data or establishing computer system access from sources outside OED.

**Dial-out modem:** A **modem** that connects a personal computer to a standard telephone line for the purpose of sending data out or establishing computer system access to destinations outside OED.

**Dial-up networking:** Using a **modem** and a standard telephone line to connect one computer

to another computer.

**External network:** A network managed and operated by entities other than Department of Administrative Services, Department of Human Services, or OED.

**Information:** Any knowledge that can be communicated to documentary material, regardless of its physical form or characteristics.

**Information Security:** Preservation of confidentiality, integrity and availability of information, including authenticity, accountability, non-repudiation, and reliability.

**Integrity:** A security principle that makes sure information and systems are not modified maliciously or accidentally.

**Least privilege:** Refers to the information systems security objective and requirement of granting users only those accesses they need to perform their official duties. It requires that users be granted the lowest level of computer/system access that is consistent with job authority. Increases in privileges shall be requested and granted by written communications.

**Mission Critical Information:** Information necessary for the continued operation of any organization, its automated information resources and services. This information may not be sensitive. However, the loss, denial, or modification of such information may cause grave damage to the operation of the organization.

**Modem:** A *modulator-demodulator* device that converts a computer's data signals into a form that can be sent across a standard telephone line or other networks. A **modem** is needed at both the sending and receiving locations. The receiving **modem** converts the data from the form sent across the network back into a format recognized by the computer.

**Need-to-Know:** The necessity for access to, knowledge of, or possession of classified or other sensitive information in order to carry out officially sanctioned duties. Responsibility for determining whether a user's duties require possession or access to this information rests upon the individual having current possession (or ownership) of the information involved, and not upon the prospective recipient.

**Network:** A computer network is a data communications system that interconnects computer systems at various sites.

**Network User Change Request Form (NURF):** Electronic form located on EdWEB, used to request new user accounts, account modifications, or account deletions.

**OED network:** Any local area network (intra-office) that is managed by OED Information Technology Services staff, **and** the wide area network connections leased by OED and managed by Department of Administrative Services (DAS) **or** Department of Human Services (DHS).

**OED staff:** Employees, authorized representatives, temporary staff and volunteers.

**Proxy:** An authorized alternate user who logs in with his or her own account name and password and then is granted access by another user to his or her data or privileges by connecting to the granting user's account. The proxy does not need to know the granting user's

account name or password to gain this access.

**Risk:** The likelihood of a threat agent taking advantage of vulnerability and the resulting business impact. A risk is the loss potential or probability that a threat will exploit the vulnerability.

**Security Incident or Intrusion:** An event that has actual or potential adverse effects on computer or network operations resulting in fraud, waste, or abuse; compromise of information; or loss or damage of property or information. Examples include unauthorized penetration of a computer system, exploitation of technical vulnerabilities, or introduction of computer viruses or other forms of malicious software.

**Security Policy:** Documentation that describes management's directives toward the role that security plays within the agency. It provides a framework within which the agency establishes needed levels of information security to achieve the desired confidentiality, availability and integrity goals. A policy is a statement of information values, protection responsibilities, and agency commitment to managing risk.

**Telecommuter:** An employee who, in mutual agreement with section management, establishes a formal agreement to work away from the employee's work station with the use of standard work tools, such as a personal computer with network access.

**Virus infection:** This occurs when a purposefully destructive computer program is executed on a computer. Symptoms of an electronic **virus infection** can range from a simple message display to complete disabling of the computer and destruction of files on the hard disk. **Virus infections** typically spread from one computer to another when infected files or programs are shared with others.

**Compliance:** All users are responsible for complying with DAS and Employment Department security policies as well as procedures and practices developed in support of the policies. Anyone suspecting misuse or attempted misuse of information systems resources is responsible for reporting such activity to their managers and to the Security Administrator.

**Non-Compliance:** Violation of standards, policies, procedures, or practices may result in:

- a. Restriction, temporary suspension or termination of a user's access to computer and network resources.
- b. Disciplinary action up to and including termination in accordance with Department policy.

**Exception Process:** Exceptions may be granted when a business case constitutes a given business need. All exceptions must go through the Information Security Office for approval.

**Inventory:** N/A

**Policy Link:** [Information Security Policy IRM 7 \(2\)](#)

# Administrative Procedures

Procedure Name: Incident Response  
Accompanying Policy: Information Security Policy, IRM 7 (2)  
Issuing Section: IT Services  
Revision Date: 12/03/08

Issue Date: 12/03/08

Policy & Procedure Administrator: Leslie Cummings  
Information Security Program Manager  
Contact Information: (503) 947-1622

Approval: Leslie Cummings  
Information Security Program Manager  
Date: \_\_\_\_\_

**Summary:** The purpose of this procedure is to provide quick, effective and orderly response to privacy and information security incidents ranging from unauthorized intrusions into OED network systems to the mishandling of data in such a way that the privacy, integrity, or availability of confidential information is at risk; and to ensure the proper investigation of incidents involving loss, damage, misuse of Oregon Employment Department (OED) information assets, or improper dissemination of that information.

OED and State policy requires OED to establish an incident response team to address the handling of privacy and information security incidents. It requires OED managers, staff, and other authorized information users to report privacy and information security incidents. An incident is a threat or event that compromises, damages, or causes a loss of confidential or protected information (e.g. unauthorized disclosure of information, failure to protect user ID's, theft of computer equipment or client files, unexplained changes to a systems file, viruses, etc.). Agency management must promptly investigate incidents involving loss, damage, misuse of information assets, or improper dissemination of information. All program areas are required to report information security incidents according to the security reporting requirements in this policy.

All individuals granted access to OED information or systems are covered by this policy procedure and shall comply with this and associated policies, procedures and guidelines. These individuals include full and part-time employees, volunteers, contractors, temporary workers, those employed by others to perform OED work, and others authorized to access OED information, network and/or systems.

ISIRP is an Information Security "Incident Response" program, which captures both Privacy and Information Security Incidents. The OED Information Security Office (ISO) is responsible for receiving, reviewing, and responding to privacy/information security incidents, with involvement from department representatives in the resolution process.

## Procedure:

**How to Report and Incident:**

1. OED Workforce Individuals: Immediately report any privacy or information security incident to the manager/supervisor, if available.

If the manager/supervisor is not available, workforce individuals should proceed to steps 2 and 3 of this procedure and report the incident to the manager/supervisor in a timely manner.

2. Manager/Supervisor: Gather privacy/information security incident information.

**Reporting individual's:** Name, Agency, Department and Work Unit , Position, Address, City, Email Address, Phone Number

**Incident Information:** Date, Time, Location

**Description/Action:** Brief description of the incident, parties and/or information systems involved and any action taken.

Manager/Supervisor: Submit report to the OED Customer Service and Support Office (Help desk) or the Information Security Office. The report may be made verbally or electronically, printed or by fax.

**Incident Examples:**

A Privacy or Information Security incident has four key elements: (a) it involves security of information; (b) it is unwanted or unexpected; (c) it shows harm or significant threat of harm; and (d) it requires non-routine response. An incident may occur in one or more of the following situations:

- Confidential or protected Wage Information is accidentally or intentionally disclosed to unauthorized persons
- An unauthorized person asks for or is given access to OED systems
- Unauthorized reproduction of confidential or protected information
- Unauthorized persons found in confidential area
- Confidential or protected documents are not disposed of properly when no longer needed
- Loss or Theft of physical or electronic media containing confidential or protected information
- Confidential or protected information is not protected as it should be or is mishandled in some manner
- Confidential or protected information is falsified
- Computer equipment (laptop, personal digital assistants (PDAs), desktop workstation) containing confidential or protected information is lost or stolen
- Employees share logins and/or passwords

- Someone asks for someone else's password
- Data is defaced or destroyed
- Data is modified for unexplained reasons
- A workstation or notebook computer is found with a virus
- Equipment misuse or tampering
- Any violation of OED security or privacy policies

**Steps Taken when an Incident is Reported:**

In the event of an information security incident that affects the availability, integrity or confidentiality of agency's information assets, the following Information Security Incident Response Program (ISIRP) will be activated. This program establishes a response capability to handle information security incidents. It addresses internal and external communication, identifies roles and responsibilities for Information Security Incident Response Team (ISIRT), and establishes guidelines for monitoring, controlling, reporting, and following up on an incident.

**Information Security Incident Response Team:** For an information security incident involving computer or network security, the Information Security Program Manager (ISPM) typically receives the first reports, either from internal staff, State Data Center, or Enterprise Security Office. If a security breach has occurred, the ISPM assembles an Information Security Incident Response Team (ISIRT). Members will be the ISPM, Program Area Leader for the affected area, and Communications Manager.

**Roles and Responsibilities:** If the incident involves computer or network security, the ISPM will have responsibility for: (a) securing the technical environment; (b) working with the State Data Center and DAS Enterprise Security Office state incident response team; (c) convening the ISIRT; and (d) communicating a summary of the results of forensics and traffic logs to the ISIRT.

If the incident involves loss or compromise of non-electronic confidential material only, the site or section manager will have responsibility for: (a) securing the physical environment; (b) working with the appropriate local authorities; (c) requesting the Program Area Leader to convene the ISIRT; (d) communicating a summary of the results of forensics and traffic logs to the ISIRT; and (e) providing the Communication Manager with necessary materials to inform the DAS Enterprise Security Office state incident response team.

The Communication Manager will have the responsibility for: (a) engaging the services of an identity security vendor, if necessary; (b) obtaining approval for notification letter; and (c) managing the communication with affected individuals, media, and public.

The Program Area Leader will have responsibility for: (a) coordinating any HR involvement regarding the actions of staff whose equipment was involved in the breach; (b) determining if business practices need to be modified to prevent future incidents; and (c) paying for the cost of vendor services for ID protection and ID recovery.

The ISIRT will examine a summary of the results of the forensics and logs to determine notification requirements per SB583 (Oregon Consumer Identity Theft Protection Act) and state policy. The ISPM notifies the Director's Office of the scope and nature of the security breach, and provides updates until the incident is closed.



After the environment is secure and notifications have been sent, the ISIRT writes an incident report describing: (a) the nature of the event; (b) the scope and impact; (c) the immediate actions that were taken to control and notify; and (d) the actions that will be taken to reduce risk of repetition of the event.

**Operational Controls:** Security Breaches are to be kept confidential; information about any breach is provided outside of the ISIRT and Director's Office only on a "need to know" basis. Senate Bill 583 (Oregon Consumer Identity Theft Protection Act) and statewide/agency policies, including DAS Incident Response policy, guide decisions on an action plan for each incident. Resolution of any event assumes highest priority for the ISIRT.

**Resolution:** An incident will be considered "closed" when: (a) the technical environment is secured against any further action by the virus, malware, or breach; (b) all notifications, if required, have been sent; (c) all incident response reports have been delivered to the Director's Office; and (d) the Director's Office may request that the ISIRT debrief the Executive Team on the incident, providing recommendations for changes in business practices designed to reduce risk or repeat occurrences.

**Guidelines:** The following information should also be applied to protect OED information assets during security incidents:

Roles and Responsibilities

1. ISPM
  - Publish and maintain policy procedures and guidelines for handling computer security incidents.
  - Provide management oversight of the process for handling computer security incidents.
  - Immediately inform OED management of significant incidents (major compromise of data, denial of service); update as necessary.
  - Work with the ISIRT, users and/or system administrators, the network manager/administrator, and if necessary law enforcement officials to formulate an initial response plan, and modify the plan as needed.
  - Ensure appropriate reports are prepared and submitted within established timelines.
  
2. OED Managers
  - Communicate to employees the information security response requirements outlined in this procedure.
  - Contact the ISPM within one working day after an incident.
  - Work with the ISIRT, users and/or system administrators, the network manager/administrator, and if necessary law enforcement officials to formulate an initial response plan, and modify the plan as needed.
  - Ensure appropriate reports are prepared and submitted within established timelines.
  
3. User/System Administrator – the user or system administrator should perform the following if there are suspicions that an incident has occurred.
  - Investigate briefly.
  - If suspicion is ungrounded, log and share knowledge with ISPM and networking manager/administrator.
  - If suspicion is confirmed or indeterminate, confer with manager, ISPM and networking manager/administrator.
  - Start an event log by noting date and time of all actions.

- Take snapshot of pertinent files and document other evidence as appropriate within the first half hour of incident investigation.
  - Identify risk to system or information.
  - Confer with ISPM, ISIRT, and networking manager/administrator.
  - Implement response plan within forty-five minutes of incident discovery.
  - Notify management of significant incident and response plan.
  - Monitor and study situation.
  - Assist manager in preparing preliminary and final reports.
4. Networking Manager/Administrator
- Work with the ISIRT, users and/or system administrators and the ISPM to formulate an initial response plan.
  - Assist when necessary to evaluate and mitigate incident.
  - Review response plan and if necessary assist in modifying the plan.

**Definitions:**

**Asset:** Anything that has value to the agency

**Confidentiality:** A security principle that works to ensure that information is not disclosed to unauthorized subjects.

**Information:** Any knowledge that can be communicated to documentary material, regardless of its physical form or characteristics.

**Information Security:** Preservation of confidentiality, integrity and availability of information, including authenticity, accountability, non-repudiation, and reliability.

**Information Security Office (ISO):** OED Information Security Office; responsible for receiving, reviewing, and responding to privacy/information security incidents.

**Compliance:** All users of OED data and/or information are responsible for complying with DAS and Oregon Employment Department security policies as well as procedures and practices developed in support of the policies. Anyone suspecting misuse or attempted misuse of information systems resources is responsible for reporting such activity to their managers and to the Security Administrator.

**Non-Compliance:** Failure to comply with this policy procedure and associated policies, standards, and guidelines, may result in disciplinary actions up to and including dismissal from state service for employees, volunteers or termination of contracts for contractors, partners, consultants, and other entities. Legal actions may also be taken for violations of applicable regulations and laws.

**Exception Process:** None.

**Inventory:** N/A

**Policy Link:** Information Security Policy IRM 7 (2): (link)

# Administrative Procedures

Procedure Name: Employee Security  
 Accompanying Policy: Information Security Policy, IRM 7 (2)  
 Issuing Section: IT Services  
 Revision Date: 11/30/08  
  
 Issue Date: 11/30/08  
  
 Policy & Procedure Administrator: Leslie Cummings  
 Information Security Program Manager  
 Contact Information: (503) 947-1622  
  
 Approval: Leslie Cummings  
 Information Security Program Manager  
 Date: \_\_\_\_\_

**Summary:** The purpose of this procedure is to protect information assets and reduce the risk of human error and misuse of enterprise information and equipment. It describes the methods whereby OED will:

1. Require pre-employment screening, employment history and/or background checks of employees commensurate with the value and risk of the information assets to which they will have access; (link: Criminal Background Check Policy)
2. Establish accountability and responsibility to all employees who have access to the agency's information assets, and annual signing of acknowledgements of these security responsibilities and policies; (link: Commitment to Confidentiality Form 0100)
3. Establish processes for timely removal of all permissions for employees who have access to agency information assets and return of agency assets at termination or reassignment; (link: Separation Procedure) and
4. Establish security awareness training for employees, contractors and third parties with respect to agency, individual and statewide security responsibilities and policies. (link: Security Awareness Training Module)

**Definitions:**

**Asset:** Anything that has value to the agency

**Information:** Any knowledge that can be communicated to documentary material, regardless of its physical form or characteristics.

**Information Security:** Preservation of confidentiality, integrity and availability of information, including authenticity, accountability, non-repudiation, and reliability.

**Integrity:** A security principle that makes sure information and systems are not modified maliciously or accidentally.

**Risk:** The likelihood of a threat agent taking advantage of a vulnerability and the resulting business impact. A risk is the loss potential or probability that a threat will exploit the vulnerability.

**Security Policy:** Documentation that describes management's directives toward the role that security plays within the agency. It provides a framework within which the agency establishes

needed levels of information security to achieve the desired confidentiality, availability and integrity goals. A policy is a statement of information values, protection responsibilities, and agency commitment to managing risk.

- Compliance:** All users are responsible for complying with DAS and Employment Department security policies as well as procedures and practices developed in support of the policies. Anyone suspecting misuse or attempted misuse of information systems resources is responsible for reporting such activity to their managers and to the Security Administrator.
- Non-Compliance:** Violation of standards, policies, procedures, or practices may result in:
- a. Restriction, temporary suspension or termination of a user's access to computer and network resources.
  - b. Disciplinary action up to and including termination in accordance with Department policy.
- Exception Process:** Exceptions may be granted when a business case constitutes a given need. All exceptions must go through the Information Security Office for approval.
- Inventory:** N/A
- Policy Link:** Information Security Policy IRM 7 (2): [\(link\)](#)

# Administrative Procedures

Procedure Name: Transporting Information Assets  
Accompanying Policy: Information Security Policy, IRM 7 (2)  
Issuing Section: IT Services  
Revision Date: 12/03/08

Issue Date: 12/03/08

Policy & Procedure Administrator: Leslie Cummings  
Information Security Program Manager  
Contact Information: (503) 947-1622

Approval: Leslie Cummings  
Information Security Program Manager  
Date: \_\_\_\_\_

**Summary:** The purpose of this procedure is to ensure the security of Oregon Employment Department information assets when in transit. Information assets can be vulnerable to unauthorized access, misuse or corruption during physical transport. Minimum safeguards must be implemented to protect sensitive information from accidental or intentional unauthorized access, modification, destruction, disclosure, misplacement or permanent loss throughout the delivery/transport cycle.

**Procedure:** OED will use appropriate security controls for transportation of sensitive information assets (physical media such as tape, disk or paper) during transit and beyond the physical boundaries of a facility from loss, destruction or unauthorized access. Each individual or program area that sends, receives or transports confidential or sensitive information to or from another facility or agency/entity is responsible to assure that the sensitivity level of an asset is governed by the statewide policy 107-004-050 Information Asset Classification in which it is the responsibility of the information owner to identify sensitive information and ensure appropriate protection.

**Detail:** The following requirements should be applied to protect OED information assets during transport:

Carrier Considerations

1. Use reliable, reputable transport or carriers.
2. Program areas will identify and approve carriers appropriate for asset transport based on the risk, volume, and sensitivity of the asset being transported. For instance, the US Postal Service may be appropriate for delivery of documents such as checks but not be appropriate for transporting data backup media with large volumes of sensitive information.
3. Check the identification of carriers where appropriate.
4. Incorporate security and liability language into contracts with vendors transporting sensitive OED information, including transit to destruction facilities.
5. Sensitive information transported in vehicles by employees will be logged, inventoried,

and kept locked and out of sight when the employee is not in the vehicle.

#### Packaging considerations

1. Packaging will be sufficient to protect the contents from any physical damage likely to arise during transit and in accordance with any manufacturer specifications (example: software), protecting against any environmental factors that may reduce the media's restoration effectiveness such as exposure to heat, moisture or electromagnetic fields.
2. Employ the use of tamper-evident packaging (which reveals any attempt to gain access).
3. Clearly describe on a form inside the package the number, type and destination of the media.
4. Use secure and clear address labeling.

#### Storage considerations

1. Store packages containing sensitive information in a secure location prior to pick up for transport.
2. Store packages containing sensitive information in a secure location / compartment inside the delivery vehicle.
3. Sensitive packages should be stored in a secure location by receiving entity.

#### Transfer of custody considerations

1. Where feasible and appropriate, the person releasing and the person receiving the package should sign a log to maintain a chain of custody at each point of transfer. In some cases, e.g. the retrieval of assets from a lock box, it may be appropriate that the receiving person should log the pick up of the asset.
2. The log will include date and time picked up, number of packages and destination.
3. The receiving delivery driver or OED representative will validate the information on the log and sign it.
4. Packages or containers of sensitive information received by OED will be distributed to appropriate program area in accordance with established business rules.

#### Additional considerations, where and when appropriate

1. Locked containers will be used.
2. Data will be encrypted.
3. Delivery will be by hand.
4. Consignment will be split into more than one delivery and dispatched by different routes.
5. An after hours delivery will be deposited into a secure lockbox along with shipping receipt.
6. Delivery notification and acknowledgement receipts will be documented and retained.

#### Definitions:

**Asset:** Anything that has value to the agency

**Availability:** The reliability and accessibility of data and resources to authorized individuals in a timely manner.

**Classification** A systematic arrangement of objects into groups or categories according to a set of established criteria.

**Confidentiality:** A security principle that works to ensure that information is not disclosed to unauthorized subjects.

**Information:** Any knowledge that can be communicated to documentary material, regardless of its physical form or characteristics.

**Information Owner:** A person or group of people with authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

**Information Security:** Preservation of confidentiality, integrity and availability of information, including authenticity, accountability, non-repudiation, and reliability.

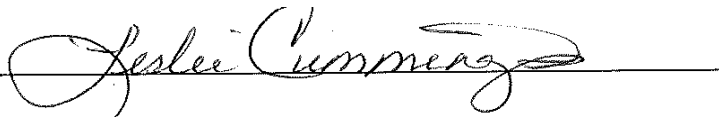
**Integrity:** A security principle that makes sure information and systems are not modified maliciously or accidentally.

**Sensitive Information:** Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the interest or the conduct of programs, or the privacy to which individuals are entitled.

**Sensitivity:** A measure of the importance assigned to information by its owner, for the purpose of denoting its need for protection.

- Compliance:** All users of OED data and/or information are responsible for complying with DAS and Oregon Employment Department security policies as well as procedures and practices developed in support of the policies. Anyone suspecting misuse or attempted misuse of information systems resources is responsible for reporting such activity to their managers and to the Security Administrator.
- Non-Compliance:** Failure to comply with this policy procedure and associated policies, standards, and guidelines, may result in disciplinary actions up to and including dismissal from state service for employees, volunteers or termination of contracts for contractors, partners, consultants, and other entities. Legal actions may also be taken for violations of applicable regulations and laws.
- Exception Process:** Exceptions may be granted if a business case can be made. All approvals for exceptions must go through the Information Security Officer.
- Inventory:** N/A
- Policy Link:** Information Security Policy IRM 7 (2): [\(link\)](#)

# Administrative Procedures

<b>Procedure Name:</b> Mobile Communications/Computing Devices		<b>Accompanying Policy:</b> Information Security Policy, IRM 7 (2)	
<b>Issuing Section:</b> IT Services (ITS)		<b>Revision Date:</b> 10/07/08	<b>Issue Date:</b> 04/30/2008
<b>Policy &amp; Procedure Administrator:</b>		Leslie Cummings, Information Security Program Manager	
<b>Contact Information:</b>		(503) 947-1622	
<b>Approval:</b>			<u>10/07/08</u> Date
<b>Summary:</b>	The purpose of this procedure is to establish a process for the acquisition and use of mobile communications/computing devices for agency business.		
<b>Definitions:</b>	<p><b>Asset:</b> Anything that has value to the agency</p> <p><b>Information:</b> Any knowledge that can be communicated to documentary material, regardless of its physical form or characteristics.</p> <p><b>Information Security:</b> Preservation of confidentiality, integrity and availability of information, including authenticity, accountability, non-repudiation, and reliability.</p> <p><b>Integrity:</b> A security principle that makes sure information and systems are not modified maliciously or accidentally.</p> <p><b>Risk:</b> The likelihood of a threat agent taking advantage of a vulnerability and the resulting business impact. A risk is the loss potential or probability that a threat will exploit the vulnerability.</p> <p><b>Security Policy:</b> Documentation that describes management's directives toward the role that security plays within the agency. It provides a framework within which the agency establishes needed levels of information security to achieve the desired confidentiality, availability and integrity goals. A policy is a statement of information values, protection responsibilities, and agency commitment to managing risk.</p>		
<b>Procedure:</b>	<ol style="list-style-type: none"> <li>1. Mobile communications/computing devices will be used only for state business.</li> <li>2. Users will comply with applicable laws and administrative policies (including copyright and license requirements), as well as any additional security policies and procedures established by the owner of the information and the agency Information Security Officer.</li> </ol> <p>Users will notify the owner of the information and the agency Information Security Officer of any actual or attempted violations of security policies, practices and procedures.</p>		



<b>Process</b>	<p><u>Description of Mobile Communications/Computing Devices</u></p> <p>Mobile Communications/Computing Devices are defined as any device capable of transmitting voice communications, email or data via the airways without the need of a connecting cable; or any removable or portable device used for storage of data. This includes cellular phones, BlackBerry™, laptops or notebooks, PDA's, diskettes, CD's, DVD's, flash or thumb drives, and recording devices.</p> <p><u>Acquisition / Approval</u></p> <ol style="list-style-type: none"> <li>1. Approval for acquisition and use of OED issued BlackBerry™ devices for agency business is limited to the Director, Deputy Director and Assistant Director; approval for all other MCD's is through the Assistant Director or Manager.</li> <li>2. The employee and Manager will be required to complete and sign "<a href="#">Mobile Communications/Computing Device Approval/Agreement Form</a>."</li> <li>3. Managers will keep the original Mobile Communications/Computing Device Approval/Agreement Form, forward one copy to the Information Security Officer and a second copy to the Office of Human Resources for the user's personnel file.</li> <li>4. Requests for acquisition and use of OED issued MCD's for agency business must be accompanied by appropriate justification. Written justification will be prepared by the Manager and should include consideration of other less expensive technologies.</li> </ol> <p><u>Acceptable Use</u></p> <ol style="list-style-type: none"> <li>1. OED issued MCD's are to be used for work related or emergency purposes.</li> <li>2. Work related or emergency use of MCD's includes but is not limited to:       <ol style="list-style-type: none"> <li>a. contacting clients, office and other pertinent staff;</li> <li>b. reporting emergency situations;</li> <li>c. summoning assistance or receiving emergency calls or emails;</li> <li>d. telephone calls or emails to report a delayed return; and</li> <li>e. accessing or storing OED data for work related purposes.</li> </ol> </li> </ol> <p>An occasion when an employee's personal use of an OED issued device is acceptable would be the need to contact a spouse or child care giver to advise that the employee is going to be late getting home or picking up children for a reason <u>directly</u> related to official duties such as a meeting which ran later than expected or a last minute change of schedule. Another permitted personal use of an OED issued MCD would be receiving an incoming call or email regarding a family emergency. Such use should be of brief duration and should occur infrequently.</p> <p><u>Standards</u></p> <p>All MCD's will comply with current OED technical standards. For current standards on your device see:</p> <p><a href="#">OED BlackBerry™ and Cell Phone Standards</a>  <a href="#">OED Laptop Standards</a>  <a href="#">OED Storage Device Standards</a></p>
----------------	---

<b>Process</b> (con't)	<p><u>Support</u></p> <ol style="list-style-type: none"> <li>1. OED issued MCD's will be eligible for full technical support pursuant to current OED standards, including backup of data.</li> <li>2. ITS will retain custody of unassigned agency owned MCD's.</li> <li>3. ITS will maintain a master file of all OED issued MCD's.</li> <li>4. For BlackBerry™ devices there will be a one time nonrefundable charge to the employee's program area to cover license fees.</li> </ol> <p><u>Security</u></p> <ol style="list-style-type: none"> <li>1. Employees using OED issued MCD's for agency business are reminded that confidential information should not be discussed or shared when using MCD's. Because cellular telephone conversations and data are transmitted over airways, they are <i>not secure</i> and can be monitored. Any data contained within an email or other retrieved formats viewed on an OED issued MCD should be handled in the same manner as any other confidential OED data.</li> <li>2. All OED issued MCD's used for agency business shall be password protected and locked when not in use.</li> <li>3. Any device that is to be synchronized with OED data must be encrypted.</li> <li>4. ITS will at its discretion permanently and completely erase the memory and data from the device through a remote process to protect OED from loss of confidential information.</li> </ol> <p><u>Manager (or Designee) Responsibility</u></p> <ol style="list-style-type: none"> <li>1. Managers are responsible for maintaining a file for each OED issued MCD containing: <ol style="list-style-type: none"> <li>a. Original approval/agreement form; and</li> <li>b. Verification of monthly bills, if applicable.</li> </ol> </li> <li>2. Once each year Managers will evaluate the need for continued use of OED issued MCD's.</li> <li>3. Managers will report user name changes to ITS.</li> <li>4. Invoices associated with OED issued MCD's shall be reviewed regularly by the Managers. Managers will distribute copies of each user's bill to the user on a monthly basis and request signed verification of work related use by the user.</li> <li>5. Managers are responsible for recovering OED issued MCD's from employees and immediately forwarding to ITS for deactivation. OED issued MCD's shall not be reassigned to other employees by the Manager or at the section level.</li> </ol> <p>Managers must immediately notify ITS when an OED issued MCD is lost, stolen, or becomes inoperative so that it may be deactivated.</p>	
	<b>Compliance:</b>	<p>All users are responsible for complying with DAS and Employment Department security policies as well as procedures and practices developed in support of the policies. Anyone suspecting misuse or attempted misuse of information systems resources is responsible for reporting such activity to their managers and to the Security Administrator.</p>
	<b>Non-Compliance:</b>	<p>Violation of standards, policies, procedures, or practices may result in:</p> <ol style="list-style-type: none"> <li>a. Restriction, temporary suspension or termination of a user's access to computer and network resources.</li> <li>b. Disciplinary action up to and including termination in accordance with Department policy.</li> </ol>

**Exception Process:**

Exceptions may be granted if a business case can be made. All approvals for exceptions must go through the Information Security Officer.

A personally owned MCD may be used to access OED information for business use. To request access follow the process outlined below.

Acquisition / Approval

- 1. Approval for acquisition and use of personally owned BlackBerry™ devices for agency business is limited to the Director, Deputy Director and Assistant Director; approval for all other MCD's is through the Assistant Director or Manager.
- 2. The employee and Manager will be required to complete and sign "Mobile Communications/Computing Device Approval/Agreement Form."
- 3. Managers will keep the original Mobile Communications/Computing Device Approval/Agreement Form, forward one copy to the Information Security Officer and a second copy to the Office of Human Resources for the user's personnel file.
- 4. Requests for permission to use personally owned MCD's for agency business must be accompanied by appropriate justification. Written justification will be prepared by the Manager and should include consideration of other technologies such as standard phones and pagers, or assignment of a similar OED issued device.

Acceptable Use

- 1. Personally owned MCD's may be used for work related purposes.
- 2. Work related use of personally owned MCD's includes but is not limited to:
  - f. contacting clients, office and other pertinent staff;
  - g. telephone calls or emails to report a delayed return; and
  - h. accessing OED data for work related purposes.
- 3. Employees will not be reimbursed by OED for any work related charges incurred while using a personally owned device for agency business.

Standards

All personally owned MCD's will comply with current OED technical standards. For current standards on your device see:

- [OED BlackBerry™ and Cell Phone Standards](#)
- [OED Laptop Standards](#)
- [OED Storage Device Standards](#)

Support

- 1. If an OED employee is approved to use a personally owned MCD for agency business, the device must be evaluated by ITS support staff (iHelp) prior to being given access to secure OED data.
- 2. The evaluation will involve a technical and security assessment to determine if the device conforms to standards established for issuance and support of OED issued devices as outlined above.
- 3. If the device does not conform to established technical standards, it may be approved for use but will not be supported by ITS support staff (iHelp).
- 4. Users of personally owned MCD's will be responsible for their own backups of data.
- 5. ITS will maintain a master file of all personally owned MCD's.
- 6. For BlackBerry™ devices there will be a one time nonrefundable charge to the employee's program area for license fees.



<p><b>Exception Process:</b> (con't)</p>	<p><u>Security</u></p> <ol style="list-style-type: none"> <li>1. Employees using MCD's for agency business are reminded that confidential information should not be discussed or shared when using MCD's. Because cellular telephone conversations and data are transmitted over airways, they are <i>not secure</i> and can be monitored. Any data contained within an email or other retrieved formats viewed on an MCD should be handled in the same manner as any other confidential OED data.</li> <li>2. All personally owned devices will be subject to the same security and confidentiality restrictions as similar OED issued devices.</li> <li>3. All MCD's used for agency business shall be password protected and locked when not in use.</li> <li>4. ITS will at its discretion permanently erase the memory and data from the device to protect OED from loss of confidential information.</li> <li>5. Any device that is to be synchronized with OED data must be encrypted. Encryption is the responsibility of the device owner.</li> </ol> <p><u>Manager (or Designee) Responsibility</u></p> <ol style="list-style-type: none"> <li>1. Managers are responsible for maintaining a file for each personally owned MCD used for agency business containing the original approval/agreement form.</li> <li>2. Once each year Managers will evaluate the need for continued use of personally owned MCD's for agency business.</li> <li>3. Managers will report user name changes to ITS.</li> </ol> <p>Managers must immediately notify ITS when a personally owned MCD approved for business use is lost, stolen, inoperative, or no longer qualifies for use so that access to OED data may be revoked.</p>
<p><b>Inventory:</b> (as needed)</p>	<p>Not applicable</p>
<p><b>Policy Link:</b></p>	<p>The Information Security Policy (IRM 7(2)) is available in the <a href="#">Information Security Program</a> Section of the Policies section on EdWeb.</p>
<p><b>Notes:</b></p>	<p>Modifications of this process is at the discretion of the Policy Administrator. Changes must be in writing, signed by the Policy Administrator and kept in the procedure files of the Policy Administrator.</p>

# Information Security

Security Awareness Updates



November 2008

# OED Security Management Overview

- In November 2007 OED completed an Information Security Business Risk Assessment (ISBRA) which resulted in the identification of several risks including:
  - **No removable/portable media policy in place; Absence of information classification policy; Absence of tracking procedures for transported information;**
  - **Inter-agency information exchange is poorly controlled;**
  - **Roles and responsibilities of information owners not clearly defined across divisions;**
  - **Business Continuity Plans and Disaster Recovery Plans not developed;**
  - **Not all employees require a criminal history background check (Currently limited to Child Care Division);**
  - **Personal Internet misuse: Concern that acceptable use policies are inconsistently adhered to by employees;**
  - **OED operational procedures not documented (with regard to information security);**
  - **Lack of awareness of security incident procedures; and**
  - **Access Control lacks necessary checks and balances.**

# OED Security Management Overview (continued)

- **Steps taken since ISBRA findings to mitigate risks:**

- *Establishment of a **Security Program Office** and program framework developed;*
- ***Laptop encryption** is 90% complete, desktops encryption and mobile computing device encryption is in progress (action plan developed which includes requirements of work units, testing, and procedures development);*
- *As of Aug. 8th **OED has a removable and portable computing device policy in place** with procedures under development (planned review 10/01/08);*
- ***A policy framework** has been built to cover DAS mandates, OED needs and prudent measures for Employee Security (criminal background checks), Information Asset Classification, Transporting Information Assets, Security Program, and Incident Response. OED policy, procedures, and implementation plan, are under development; roles and responsibilities of information owners is clearly defined in updated OED security policy;*
- ***Business Continuity and Disaster Recovery Plans** are under development with a due date of December 31, 2009 (progress reports are now posted on EdWeb); Also created is a security framework which identifies each program area - safety, emergency management, business continuity, disaster planning, and information security – and shows how these programs interact with one another. Collaboration among programs is not only fostering security awareness, but also improving functionality and efficiencies;*

# OED Security Management Overview (continued)

- **Security Incident Response procedures are currently available on EdWeb** under OED's Information Security policy. Updates are under development to include Investigation Procedures and other compliance, reporting and enforcement;
- **Staff are receiving updated training** on security risks, preventative measures, detection methods, and compliance, investigation and forensics;
- **Security Awareness** to include:
  - (a) ISPM meeting with key business areas to assist in meeting current security needs;
  - (b) An Information Security Program updates and related program documents via EdWeb;
  - (c) ISPM is working with DAS/ESO to tap into general security awareness training for OED staff. The security office will also be working with HR to ensure all staff are kept informed of key security policies, procedures, and other important security updates;
  - (d) OED is launching security awareness training on **iLearn Oregon** where staff will be required to take the mandated DAS security training (a five part series);
  - (e) Long-term security awareness will be ensured through annual staff training on policies and procedures, program updates, and team collaboration with regular visits to OED customers and stakeholders.
- **Content Filtering** of high risk internet sights has been implemented (8e6 tool). Exceptions are handled though the Information Security Office when a compelling business case is made. Some categories we are continuing to monitor and may still need to be blocked include: Web-based email, Internet Radio, Streaming Media, Web-logs/personal pages, Shopping (currently only online auctions is blocked), and Travel.



# Industry Security Trends & Concerns

- **IT governance, IT risk management, and IT compliance (GRC) converging into one discipline, with greater attention paid to metrics, staffing, and optimal organizational structure.**
- **IT organizations consider security, server virtualization, and business-related technologies to be their top priorities for 2009 according to research released by the Society for Information Management.**
- **Data centric security - a mammoth effort to classify data in order to determine who gets to see it and how to protect it. It requires close communication with business leaders.**
- **Storm Worm on the rise - orchestrated attacks are expected across multiple platforms.**
- **Phishing, Bandwidth usage, Social Network sites, and Hacking still remain large areas of concern for organizations.**
- **Web exploits targeting trusted web sites and web-based social engineering attacks.**
- **Critical infrastructure often under cyber attack.**
- **Increased attacks on applications because they deal with sensitive data. A "fix it when danger strikes" approach is giving way to proactive security programs that span the application lifecycle, from bright idea to operation.**
- **Digital investigations, forensics, and e-discovery.**

# Industry Internet Security Concerns

- More event-driven, targeted email containing malware - Although employees have been educated on the dangers of malicious email attachments, email attachments remain the biggest hazard. New malicious technology is used directly in messages, where just reading -- or pre-viewing -- the message launches an attack. In July, OED had one such virus breach which phoned home to Russia and tried to transmit data.
- Identity Theft continues to gain momentum - employee's personal use of the internet such as shopping or banking, increases the risk for theft of personal banking, credit card, and/or other personal information of employees who use such services.
- Internal employee threats are on the rise (ie: A staggering 88 percent of IT administrators admitted they would take corporate secrets, if they were suddenly made redundant. The target information included CEO passwords, customer database, research and development plans, financial reports, M&A plans, and the company's list of privileged passwords.)
- State governments are making every effort to stay ahead of the ever increasing list of security threats facing their residents. The State Cyber Security Protection Act of 2008 recently introduced, is one such effort to protect state governments from the daily barrage of attacks that threatens their cyber infrastructure and sensitive personal information. This new legislation establishes a State Cyber Security Pilot Program within the Department of Homeland Security to provide money to strengthen cyber security within state governments across the country.

# Security Breach Examples

- OR Veterans Affairs Medical Center **inadvertently posted personal information** on public website (Nov 2008)
- OSU Corvallis experienced **compromised credit card numbers** for 4700 online customers (June 2008)
- **Computer virus** exposed credit card numbers, birth dates and home addresses of 11,500 Cascade Healthcare Community customers (Mar 2008)
- **Over half of U.K. firms have lost data (October)** An astonishing 55% of British companies have lost data, according to a new report of 785 IT professionals in the U.K.
- **Data Breaches at State, Local Agencies Expose Data About Millions (October)** During the first three quarters of the year, there were 20 security breaches at state and local government agencies that resulted in the exposure of the personal information of almost 3.8 million Americans
- **Cybergang moles steal company data (October)**
- **Tough economic climate can heighten insider threat (October):** one of the biggest threats to corporate data and systems traditionally has come from insiders, who with their privileged access to data and systems, have the potential ability do more accidental or malicious damage than even the outside attacker:
  - In July, for instance, a disgruntled administrator for the city of San Francisco locked access to a critical network by resetting administrative passwords to its switches and routers and then refusing to divulge them to officials for days.
  - In a similar incident, a Unix systems administrator at Medco Health Solutions Inc. who was concerned about being laid off, planted a logic bomb on an internal system that, had it gone off, would have deleted data on 70 servers.
  - While both incidents involved technically savvy insiders, similar threats can come from non-IT staff as well. A scientist working at DuPont admitted to stealing corporate data valued at around \$400 million shortly before he left the company to work at a rival.
- **Report: Malicious Spam Spikes in the Enterprise:** New survey results from Sophos find the number of spam emails with dangerous attachments have soared. The report reveals the malicious messages rose eight-fold in just three months.

# Bringing It Home to OED

## INFORMATION SECURITY is important...

- Since mid-July, OED has experienced 13 Information Security Incidents:
  - 3 Security Breaches;
  - 4 Confidentiality Breaches;
  - 2 Lost/Stolen Records;
  - 2 Misuse of State Resources violations;
  - and 2 Virus Breach.
- In addition to state mandated security policies (i.e. DAS Acceptable Use Policy), such misuse of state resources and breaches, has required OED to “tighten up” information security measures and enforcement.
- OED has a zero tolerance for confidentiality breaches (immediate termination), and is taking a strong stance on security breaches and/or misuse of state resources. As an OED user, it is critical that you KNOW and abide by your policies and policy procedures.
- OED employees have been terminated for policy violation involving these types of misuse and abuses.

# Security Incident Reporting is Everyone's Concern

OED and State policy requires OED to establish an incident response team to address the handling of privacy and information security incidents. It requires OED managers, staff, and other authorized information users to report privacy and information security incidents.

An incident is a threat or event that compromises, damages, or causes a loss of confidential or protected information (e.g. unauthorized disclosure of information, failure to protect user ID's, theft of computer equipment or client files, unexplained changes to a systems file, viruses, etc.). Agency management must promptly investigate incidents involving loss, damage, misuse of information assets, or improper dissemination of information. All program areas are required to report information security incidents according to the security reporting requirements in this policy.

## How to Report and Incident?

1. OED Workforce Individuals: Immediately report any privacy or information security incident to your manager/supervisor, if available. If your manager/supervisor is not available, workforce individuals should proceed to steps 2 and 3 of this procedure and report the incident to their manager/supervisor in a timely manner.
2. Manager/Supervisor: Gather privacy/information security incident information.
  - Reporting individual's:** Name, Agency, Department and Work Unit , Position, Address, City, Email Address, Phone Number
  - Incident Information:** Date, Time, Location
  - Description/Action:** Brief description of the incident, parties and/or information systems involved and any action taken.
3. Manager/Supervisor: Immediately submit report. Reports must be submitted to the OED Customer Service and Support Office (Help desk) or the Information Security Office. The report may be made verbally or electronically, printed or by fax.

# Incident Examples

A Privacy or Information Security incident may occur in one or more of the following situations:

- Confidential or protected Wage Information is accidentally or intentionally disclosed to unauthorized persons
- An unauthorized person asks for or is given access to OED systems
- Unauthorized reproduction of confidential or protected information
- Unauthorized persons found in confidential area
- Confidential or protected documents are not disposed of properly when no longer needed
- Theft of documents containing confidential or protected information
- Confidential or protected information is not protected as it should be or is mishandled in some manner
- Confidential or protected information is falsified
- Computer equipment (laptop, personal digital assistants, desktop workstation) containing confidential or protected information is stolen
- Employees share logins and/or passwords
- Someone asks for someone else's password
- Data is defaced or destroyed
- Data is modified for unexplained reasons
- A workstation or notebook computer is found with a virus
- Equipment misuse or tampering
- Any violation of OED security or privacy policies

# Staff/User Responsibilities

- Know your Security policies and procedures, and abide by them. You will be required to read and sign security policy agreements annually (or when a major change has been made). Failure to comply with OED policies, procedures may result in disciplinary actions up to and including dismissal from state service for employees, volunteers; or termination of contracts for contractors, partners, consultants, and other entities. Legal actions may also be taken for violations of applicable regulations and laws.
- Check out your Security Resources
  - EdWeb now hosts a growing body of information on OED's Information Security Program.
  - iLearn had Security Awareness Training (5 modules) that provides the State required understanding and knowledgebase for all staff and users of OED data and information.
  - DAS sponsors Security training through the state web site.
- Managers understand that although your employees are responsible for their own personal behavior and actions, you are ultimately responsible and can also be held liable for their behavior and actions. Ensure you have done your due diligence in mitigating risks by being familiar with current security policies, procedures, by providing guidance to OED security measures and controls to your staff, and by modeling appropriate behaviors and actions.

# Information Security Program Mgmt

OED is in the process of developing and implementing an enterprise Security program. Information Security Program Management integrates with Safety, Emergency Management, Business Continuity and Disaster Recovery, and Incident Response programs.

- Information Security Program Components
  - Program components include administration, monitoring and assessment, identification and classification of assets-users-threats, risk management, compliance and investigation, change management, architecture design review and maintenance, training and education.
- The program covers each of the common security domains defined by ISO, NIST, and other professional security organizations:
  - Risk Management
  - Access Control
  - Application Security
  - Operations Security
  - Physical Security
  - Security Architecture and Design
  - Telecommunication & Network Security
  - Cryptography
  - BCP and Disaster Recovery
  - Legal and Regulatory Compliance



# Next Steps

- ISBRA Refresh: OED to meet with DAS and KPMG for a refresh of risk and vulnerability assessment completed in November 2007; review changes OED has made, and update security concerns, needs and goals.
- Team with DAS/SDC for enterprise Identity and Access Management controls.
- Encryption of mobile computing devices (laptops, PDAs, diskettes, CDs, DVDs, flash drives, etc.)
- Information Security policy and procedures developed/updated and implemented (*in progress*).
- Security Team (Safety, Emergency Management, Business Continuity & Disaster Planning, Information Security)
  - Monthly meetings
  - Status reports on EdWeb
- Security Awareness Training
  - DAS Security Training on iLearn
  - OED Management (December)
  - HR Training Plan for OED Staff
  - Security Awareness on EdWeb

***Thank you...***