

Oregon Medical Board

POLICY

TITLE/SUBJECT: Information Security Policy

NUMBER: 847-206-002

SUPERCEDES: n/a

AUTHORITY: Controlling Portable & Removable Storage Devices
DAS Statewide Policy 107-004-051

Employee Security
DAS Statewide Policy 107-004-053

Information Asset Classification
DAS Statewide Policy 107-004-050

Information Security
DAS Statewide Policy 107-004-052

Transporting Information Assets
DAS Statewide Policy 107-004-100

Information Security Incident Response
DAS Statewide Policy 107-004-120

APPLICATION: All OMB Employees, Board Members & Contractors

INTERPRETATION RESPONSIBILITY: OMB Business and HR Managers

EFFECTIVE DATE: August 1, 2008

REVISED: November 1, 2011

POLICY APPROVED BY: _____
Kathleen Haley, Executive Director

PURPOSE: The purpose of this policy is to ensure Oregon Medical Board's information assets are identified, properly classified, and protected throughout their lifecycles. Information, like other assets, must be properly managed from its creation to disposal. As with other assets, not all information has the same value or importance to the agency. Therefore, information requires different levels of protection. Information asset classification, data management, transportation and incident response are critical to ensuring that the agency's information assets have a level of protection that corresponds with the asset's sensitivity and value. This policy collectively applies to all information assets, including but not limited to paper, electronic and film.

POLICY: All OMB information assets will be identified, classified, managed, transported and responded to based on its confidentiality, sensitivity, value and availability requirements. Proper levels of protection will be implemented to protect these assets relative to their classifications. Employees will receive policy and security awareness training. This policy is subject to the limitations and conditions of the Oregon Public Records Law and the Oregon Medical Practice Act.

DEFINITIONS:

asset	anything that has value to the agency
availability	the reliability and accessibility of information assets 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 information is not disclosed to unauthorized subjects
control	means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal in nature
incident	A single or a series of unwanted or unexpected information security events (see definition of "information security event") that result in harm, or pose a significant threat of harm to information assets and require non-routine preventative or corrective action.
information owner	person that has the authority for specified information and has the responsibility for establishing the controls for its generation, collection, processing, dissemination and/or disposal
information security	preservation of confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved
info security event	An observable, measurable occurrence in respect to an information asset that is a deviation from normal operations.
integrity	a security principle that makes sure information and systems are not modified maliciously or accidentally
media	something on which information may be stored
risk	the likelihood of someone or something taking advantage of a vulnerability and the resulting business impact. A risk is the probability that a threat will exploit the vulnerability
risk assessment	overall process of risk analysis and risk evaluation
risk evaluation	process of comparing the estimated risk against given risk criteria to determine the significance of the risk
risk management	coordinated activities to direct and control the agency with regard to risk
security policy	documentation that describes senior management's directives toward the role that security plays within the organization. It is a statement of information values, protection responsibilities and the organization's commitment of managing risks
sensitive info	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
threat	a potential cause of an unwanted incident, which may result in harm to a system or the agency
vulnerability	a weakness of an asset or group of assets that can be exploited by one or more threats

GUIDELINES:

Asset Classification Levels

The Oregon Medical Board shall identify its information assets for the purpose of defining its value, criticality, sensitivity and legal implications. The agency will use the classification descriptions included in this policy to differentiate between various levels of sensitivity and value. All information assets shall be classified strictly according to their level of sensitivity as follows:

- **Level 1, “Published”** – Low-sensitive information. Information that is not protected from disclosure, that if disclosed will not jeopardize the privacy or security of agency employees, clients or partners. This includes information regularly made available to the public via electronic, verbal or hard copy media.

This level of asset contains such things as press releases; newsletters; brochures; our public access Web pages; lists of licensees; published physician’s licensing records; published budget documents; Board orders; and other materials created for public consumption.

- **Level 2, “Limited”** – Sensitive information that may not be protected from public disclosure but if made easily and readily available, may jeopardize the privacy or security of agency employees, clients, or partners. The agency shall follow its disclosure policies and procedures before providing this information to external parties.

This level of asset contains such things as disaster recovery plans; published internal audit reports; names, addresses phone numbers and e-mail addresses of licensees that are not protected from disclosure; employee salary and classification information; and other information that is not protected from disclosure.

- **Level 3, “Restricted”** – Sensitive information intended for limited business use that may be exempt from public disclosure because, among other reasons, such disclosure will jeopardize the privacy or security of agency employees, clients, partners or individuals who otherwise qualify for an exemption. Information in this category may be accessed and used by internal parties only when specifically authorized to do so in the performance of their duties. External parties requesting this information for authorized agency business must be under contractual obligation of confidentiality with the agency (for example, confidentiality/non-disclosure agreement) prior to receiving it.

Security threats at this level include unauthorized disclosure, alteration or destruction of data as well as any violation of privacy practices, statutes or regulations. Information accessed by unauthorized individuals could result in financial loss or identity theft. Security efforts at this level are rigorously focused on confidentiality, integrity and availability.

This level of asset contains such things as computer network diagrams; in-process investigations; personally identifiable information (Social Security numbers, employee ID numbers, home address and phone, etc.); personnel and payroll records and files; licensing background checks; emails and regular mail containing case related information; orders for evaluations; proprietary business information; employee and licensee health-related information contained in a variety of formats (paper, fax, e-mail, FMLA files, USB drives, servers, CD’s sent to consultants, archived documents, etc.); passwords and encryption system information; firewall configurations; business back-up tapes; court reporter tapes; finger print cards; regulated information with significant penalties for disclosure such as information covered by the Health Information Portability and Accountability Act; and any

other information that is typically exempt from public disclosure; generally, all medical records; and any other information that is typically exempt from public disclosure.

- **Level 4, “Critical”** – Information that is deemed extremely sensitive and is intended for use by named individual(s) only. This information is typically exempt from public disclosure because, among other reasons, such disclosure would potentially cause major damage or injury up to and including death to the named individual(s), agency employees, clients, partners, or cause major harm to the agency.

This level of asset contains such things as medical records and investigation documents that are extremely sensitive and could lead to dangerous physical situations. These are exceptions to those normally found at Level 3.

Information Asset Protection

A range of controls will be designed for each level of information asset classification. Controls will be commensurate with the sensitivity of the information in each classification. This policy also provides guidelines for the transportation of sensitive assets.

Level 4 data that exists in physical form (e.g. paper, removable thumb drives, CD's, DVD's, etc.) must always be kept locked in a secure location when not being used. A secure location is one that has at least two layers of control. These controls can include locked doors, locked file cabinets and secure buildings. An example of two layers of control is a paper file secured within a locked file cabinet within a locked office or in secured building that has access controls.

Level 4 data that exists in electronic form (e.g., databases, hard drives, agency or statewide applications, etc.) must always be protected by two layers of control. These controls can include secure buildings; secure rooms within the building that has very limited access and is password controlled; encryption; tamper-proof packaging; limited electronic access; passwords; etc.

Electronic transmission of level 4 data must be electronically safeguarded using such tools as encryption or password-protected zip files. Level 4 data sent by state shuttle must be secured in tamper-evident envelopes and tracked. Level 4 data sent by third party mail (e.g., USPS, UPS, etc.) must use standard certified processes. The Executive Director must authorize disclosure, transmission or dissemination of level 4 data.

Level 3 data must always be protected by at least one layer of control when not being used. These controls can include a locked cabinet, desk or file drawer, a secure location such as within a locked office, encryption, tamper-proof packaging or password protection.

Electronic transmission of level 3 data may be electronically safeguarded using tools such as encryption or password-protected zip files if the data owner deems it necessary. Level 3 data sent by state shuttle may be secured in tamper-evident envelopes and tracked if the information asset owner deems it necessary. Level 3 data sent by third party mail may use standard processes unless the data owner determines a higher level of security is needed. The owner or designee of the information asset must authorize disclosure, transmission or dissemination of level 3 data.

Level 2 data must have reasonable safeguards such as filing in a drawer or other area not in public view. Level 2 data may be sent electronically or mailed without special security controls at the discretion of the information asset owner.

Level 1 data does not require any special handling or safeguards.

Compliance

The agency may, based upon individual business needs or legal requirements, exceed the security requirements put forth in this document but must, at a minimum, achieve the security objectives defined in this document. To reduce the state's risk exposure, the agency will focus initially on classifying and protecting Level 3, "Restricted" and Level 4, "Critical" information.

Notwithstanding the timelines outlined in this policy, the agency will properly identify and protect information meeting the definitions, requirements and effective dates outlined in the Oregon Consumer Identity Theft Protection Act (ORS 646A.600-628) as they relate to personal information by January 2008.

The agency has until July 1, 2008 to identify and protect information assets classified at Level 4, "Critical".

The agency has until January 1, 2009 to identify and protect information assets that are classified at Level 3, "Restricted".

The agency has until July 1, 2009 to identify and protect information assets that are classified at Level 2, "Limited."

This agency certifies that all information assets have been properly classified as of October 1, 2011 and will continue to classify new information assets as they are obtained in compliance with our Information Asset Identification Tables and Protection Procedures 847-206-002-A.

Labeling Limited, Restricted or Critical Information

Proper labeling enables all parties to correlate the information with the appropriate information handling guidelines. Information should be properly labeled so that users are aware of classification.

The attachment "OMB Information Asset Identification Table and Protection Procedures" shall be the document that identifies information classifications at all levels. Owners of the information assets will determine where those assets fit. OMB management will review and approve or deny the risk level assigned to the asset. Information classified at level 3 will be labeled "restricted" and information classified at level 4 will be labeled as "critical".

Information Handling

Information assets must be handled in a manner to protect the information asset from unauthorized or accidental disclosure, modification or loss. All information assets should be processed and stored in accordance with the information asset classification levels assigned in order to protect the confidentiality, integrity, availability, and level of sensitivity.

It is the responsibility of all OMB employees to protect information from unauthorized disclosure or compromise. Employees are responsible to protect all sensitive information that if inappropriately disclosed could cause damage, financial harm, physical harm, death or political harm to an individual, agency employees, licensees, or the agency itself.

Securing information means protecting all forms of confidential and sensitive information. Verbal conversations and paper information are equally as important as the information on an employee's computer. Employees will protect their computer screens from unauthorized viewers. Desks will be kept clear of sensitive information when not being used. Confidential conversations will be held in non-public areas.

Due to the transportability of portable devices, they are particularly vulnerable to loss or theft because they may be taken out of the normal work environment. As such, no portable storage device will store any level 3 or level 4 assets without suitable physical and technical protective measures in place. The OMB will take steps to physically control and protect these portable devices by tracking when, where, how and who is using the devices. It will also document what information is stored on them. The information owner must approve the release of portable devices.

Information coming from another agency should be properly classified by the originating agency. OMB recipients of such information must observe and maintain appropriate security for the classification assigned by the owner agency. The OMB reserves the right to upgrade the classification level if necessary.

In accordance with Statewide Policies and the OMB's Security and Incident Plan, recipients of OMB information assets are responsible for complying with the Information Security Policy and Procedures.

Information Isolation

Information belonging to different information asset classifications will be logically or physically separated or the aggregate information protected at the highest classification level. Whenever and wherever possible, information assets classified as "Critical" will be stored in a separate, secure area.

Incident Response

Identification of an incident is the process of analyzing an event and determining if that event is normal or not. The term "incident" refers to an adverse event impacting one or more of OMB's information assets or to the threat of such an event. Examples may include:

- Unauthorized use
- Denial of service (blocking access to our own systems)
- Malicious code (viruses, spyware, etc.)
- Network and application system failures (widespread)
- Unauthorized disclosure or loss of information
- Information security breach

Incidents can result from many things. Examples may include:

- Intentional and unintentional acts
- Actions of employees, vendors, contractors or third parties
- External or internal acts
- Credit card fraud
- Potential violations of Statewide or OMB's policies
- Natural disasters and power failures
- Acts related to violence, warfare or terrorism
- Serious wrongdoing

When an incident occurs, OMB Procedure 847-206-002 C will detail who is responsible for what response action. It includes triage, evidence preservation, forensics, communication, threat eradication, resumption of operations, postmortem discussions and awareness training.

Incident Classification

The classification of an incident will be determined by the Information Asset Classification that has been assigned to the information. The OMB will immediately initiate its incident response procedures for Levels 3 and 4 information assets. Levels 1 and 2 incidents will be reviewed for required action as appropriate. Some factors that were considered when assigning asset classification levels were:

- Criticality of systems that could be made unavailable
- Value of the compromised information
- Number of people or functions impacted
- Business considerations and public relations
- Enterprise impact
- Multi-agency scope

Proper Disposal

All electronic, removable media, paper and physically recorded information assets must be permanently destroyed or rendered unrecoverable in a manner consistent with the information asset classification of the information and comply with established State of Oregon archive laws, rules and regulations.

Paper files containing level 3 or level 4 data must be disposed of so that confidentiality is maintained. Confidential shredding bins or shredding by staff are acceptable means of disposal.

For disposal of electronic equipment, refer to Statewide Policy 107-009-0050 on Sustainable Acquisition and Disposal of Electronic Equipment (E-Waste/Recovery Policy).

Additional Resources

The Department of Administrative Services developed a set of resources to help agencies implement information asset classification and incident response requirements. Those resources can be found at: <http://oregon.gov/DAS/EISPD/ESO/IAC.shtml> and <http://oregon.gov/DAS/EISPD/ESO/SIRT.shtml>

AGENCY OBLIGATIONS:

Employee Security Responsibilities

The agency and its employees will:

- Create and implement an Information Security and Response Plan that will comply with relevant laws and policies;
- Ensure employees and volunteers are presented with this policy and procedures at time of hire and during annual refresher training sessions;
- Ensure all employees and volunteers understand their roles as owners and/or protectors of sensitive information and how that information is handled;
- Train employees at least annually on a variety of topics (asset identification, security options, technical security systems, incident response, etc.) and using a variety of techniques (on-line tutorials, guest speakers, in-house IT trainer, procedural and policy updates, DAS sponsored classes, etc.);
- Access only the information that is necessary to do their jobs;
- Obtain appropriate authorization before providing information to third parties;
- Take all reasonable precautions to assure that information maintained by OMB will not be disclosed to unauthorized persons;
- Promptly report all violations or suspected violations of information security and privacy policies to the Business Manager or designee;

- Show employees how important this policy is by including performance measures in their annual appraisals and holding OMB management accountable for compliance;
- Have them sign their acknowledgement and understanding of the policy;
- Give new employees and volunteers user awareness and security training;
- Identify the appropriate security levels for employees based on their role in the agency;
- Ensure access to information systems and assets are removed promptly when transfer or termination occurs;
- Maintain records according to Public Records and Retention Schedules;
- Identify information security risks;
- Contact manager and/or Incident Response (Business) Manager when breaches of security occur or suspected;
- Managers will perform surprise audits at least biannually to assess the sufficiency of safeguards currently in place, communicate with staff both one-on-one and in group meetings on how processes and procedures are working, and review risk levels at least annually; and
- Select service providers capable of maintaining safeguards and those safeguards are addressed in contracts.

Security & Information Asset Classification Responsibilities

The agency and its employees will:

- Designate the information and technology representative, the business manager and the human resource manager to coordinate the security program;
- Assess risk and vulnerability in network and software design as well as information processing, transmission and storage by reviewing new products for security standards and annual auditing;
- Detect, prevent and respond to intrusions or failures;
- Test and monitor the effectiveness of key controls, systems and procedures;
- Establish written procedures for identifying and inventorying division information assets and assigning classification levels to all data;
- Identify the owners of each information asset and document what they do with the information;
- Establish written procedures in support of decision-making regarding controls, access privileges of users, and ongoing information management;
- The Procedures will be an addendum to the Policy rather than a part of the Policy for ease of editing;
- Information handling procedures will become part of each position's desk manual;
- Restrict or revoke a user's access when termination or job change occurs;
- Ensure the information is regularly reviewed for value and updated to manage changes to risks due to new threats, vulnerabilities or changes in the environment;
- Establish practices for periodic reviews based on business impact analysis, changing business priorities or new laws, regulations and security standards;
- Enforce state archive document retention rules regarding proper disposition of all information assets;
- When risk assessments are conducted, each employee will address how sensitive information is stored and/or disposed of and will include them in their operating procedures;
- Securely dispose information that is no longer needed according to local, state or federal law; and
- Ensure that recipients of OMB-owned information assets understand the classification and handling requirements of each asset, understand the elements of our policy, ensure this requirement is included in vendor contracts, and determine whether formal interagency agreements are needed when exchanging information assets between state agencies.

Transporting Information Asset Responsibilities

The agency and its employees will:

- Review sensitive information before transport and identify the risk level, inform the information owner of the transporting action, redact information as required, and transport according to established procedures;
- Ensure only personnel who have been authorized by the Executive Director take portable and removable information and equipment off-site, and use a sign-in/sign-out process for tracking their whereabouts;
- Establish a secure portal that will enable the agency to reduce the use of portable storage devices;
- The information owner will track what is stored on those devices and inform the Business Manager or designee of any security breaches;
- Ensure the appropriate and most reliable method of secure transport is used that may include State Shuttle, USPS, Fed-Ex, UPS, courier, hand delivery, etc.;
- Incorporate security and liability language into contracts with vendors that transport sensitive information, including transit to destruction facilities;
- Package the information to protect it against physical damage and environmental factors such as heat, moisture or electromagnetic fields;
- Employ the use of tamper-evident packaging with secure and clear address labeling;
- Store information waiting for pick up in a secure location; and
- Maintain a log process that shows the chain of custody at each transfer point.

Failure to Comply

Failure to comply with this information security policy and other associated policies and procedures may result in disciplinary action up to and including termination of employment or termination of contracts for contractors, consultants and other entities. Legal actions may be taken for violations of applicable regulations and laws.

PROCEDURES:

The Oregon Medical Board Information Asset Procedures must have maximum flexibility to keep up with changes that, at times, occur rapidly. As this Policy is implemented and the Procedures applied, adjustments will be easier to make if the Procedures are kept separate from the Policy.

The following procedures will describe how the OMB will implement this policy:

Information Asset Identification Tables and Protection Procedures: 847-206-002-A

Information Asset Training and Monitoring Procedures: 847-206-002-B

Information Asset Security Breach Procedures: 847-206-002-C

Information Asset Disposal Procedures: 847-206-002-D

Oregon Medical Board

PROCEDURES

TITLE/SUBJECT: Information Asset Identification Tables and Protection Procedures
NUMBER: 847-206-002-A
SUPERCEDES: n/a
REFERENCE: Information Security Plan and Policy
APPLICATION: All OMB staff and Board members, temporaries, volunteers and contractors
INTERPRETATION RESPONSIBILITY: Business and HR Managers
EFFECTIVE DATE: August 1, 2008
REVISED: November 1, 2011

PURPOSE:

To establish how information assets will be identified and assigned a security risk level, who the owner(s) of the assets are, and what the protection standard is for the asset.

DEFINITION:

information owner person that has the authority for specified information and has the responsibility for establishing the controls for its generation, collection, processing, dissemination and/or disposal.

PROCEDURE:

- 1) Each information owner shall identify the information they work with.
- 2) Once identified, each information owner will determine what specific data is found within that information.
- 3) Based on the specific data, each information owner shall assign a risk level to the information asset.
- 4) Each information owner is responsible for informing the Business and/or HR Manager of the information asset and the risk level assigned to it.
- 5) The Business and/or HR Manager will update the Information Asset Classification and Protection tables located in this procedure and set the standard of protection for the asset.
- 6) The information owner is responsible for implementing the standard of protection and communicating it to others who use or have access to the information.
- 7) As information assets are received, modified or eliminated, the same evaluation and reporting procedures will occur.

INFORMATION ASSET CLASSIFICATION TABLES:

Risk Level 1 – Published, Low Sensitivity

Risk Definition: Information that is not protected from disclosure, that if disclosed will not jeopardize the privacy or security of agency employees, clients, and partners. This includes information regularly made available to the public via electronic, verbal, or hard copy media.

Information Asset	Owner(s)	Protection
Brochures and Pamphlets	Assistant to the Director	No special handling or safeguards required
Lists of licensees	Licensing Department staff	No special handling or safeguards required
Other materials created for public consumption	All OMB staff	No special handling or safeguards required
Press releases	Executive Director and Assistant to Director	No special handling or safeguards required
Public web pages	Information Systems Specialist 3	No special handling or safeguards required
Public Board disciplinary orders	Investigations Department staff	No special handling or safeguards required
Published annual performance progress reports	Business Manager	No special handling or safeguards required
Published budget documents	Business Manager	No special handling or safeguards required
Published physician's licensing records	Licensing Department staff	No special handling or safeguards required

Risk Level 2 - Limited, Sensitive

Risk Definition: Information that may be protected from public disclosure, but if made easily and readily available, may jeopardize the privacy or security of agency employees, clients, or partners. Agency shall follow its disclosure policies and procedures before providing this information to external parties.

Information Asset	Owner(s)	Protection
Agency risk management planning documents	Business Manager	Not in public view. May be sent electronically or mailed without security controls
Names, addresses & phone numbers of licensees that are coded with a "yes" (consent for disclosure) on the client information screen	Licensing Department staff	Not in public view. May be sent electronically or mailed without security controls
Personal employee information that is not confidential (e.g. salary, classification, status, etc.)	HR Manager	Not in public view. May be sent electronically or mailed without security controls
Published internal audit reports	Business Manager	Not in public view. May be sent electronically or mailed without security controls

Regular outgoing checks	Accounting Manager	Not in public view. May be mailed without security controls
-------------------------	--------------------	---

Risk Level 3 – Restricted, High Sensitivity

Risk Definition: Information intended for limited business use that may be exempt from public disclosure because, among other reasons, such disclosure will jeopardize the privacy or security of agency employees, clients, partners, or individuals who otherwise qualify for an exemption. Information may be accessed and used by internal parties only when specifically authorized to do so in the performance of their duties. External parties requesting this information for authorized agency business may be under contractual obligation of confidentiality with the agency prior to receiving it.

Information Asset	Owner(s)	Protection
Board and Committee Member's applications containing personal information	Assistant to the Director	Locked cabinet or drawer when not in use
Cash receipts – anything of monetary value including credit card transactions	Accounting Manager	Locked cabinet or drawer when not in use
Contracts with vendors that handle sensitive information	Business Manager	Contracts must contain security language and stored in a secure location.
Correspondence containing case related information	Investigations Department staff	Locked cabinet or drawer when not in use
Court reporter tapes, voice files, transcripts and CD's	Investigations Administrative Specialist 2 Naegeli Reporting Corporation Contact is Brad Lewallen 503-227-1544	Tapes must be protected at all times with at least one level of security. The OMB information owner must authorize disclosure, transmission or dissemination of this information. Transcripts and CD's mailed using signature tracking process. Secretaries transcribing the Board actions do so at their homes. Their home computers must have secure firewalls and be password or encryption protected. Retention and destruction of the information must meet state, federal and State Archive requirements. Contractor maintains information on secure server backed up by a secure repository that is

		protected by encryption or digital certificates. All of these security requirements will be placed in the contract.
Employee and licensee health related information in formats such as paper, fax, e-mail, FMLA files, CD's and flash drives sent to consultants, archived documents, etc.	All OMB staff	Locked cabinet, drawer or room when not in use. If mailed, signature tracking process and logging system will be used. If electronically transmitted, encryption will be required and the OMB security statement will be used. No downloading of sensitive information onto personally owned computers or wireless storage devices.
Fingerprint cards and application forms from licensees as well as the results	Office Specialist 2, Licensing Assistant	Locked cabinet or drawer when not in use
Firewall configurations	Information Systems Specialist 5 & 7	Establish a formal process for approving and testing all external network connections. Establish a firewall at each internet connection. Use multi-layered firewall configurations to protect sensitive information. Validate firewall configurations with vulnerability tools. Detect traffic anomalies and record them.
Incoming mail that contains checks	Accounting Technician 2	Locked cabinet or drawer when not being processed
Investigations that are in process and the permanent investigation files	Investigations Department staff	Locked cabinet, drawer or room when not in use
IT business security back-up procedures and tapes	Information Systems Specialist 7, 5 and 3	Establish physical access controls to server room. Implement security software updates and patches timely.

		<p>Subscribe to alert services that report external threats.</p> <p>Ensure all servers are up to date with the appropriate application version and security patches.</p> <p>Scan servers for configuration issues and implement fixes.</p> <p>Change passwords and access lists in response to security concerns.</p> <p>Establish formal data backup processes and conduct periodic tests.</p>
IT systems access	Information Systems Specialist 7, 5 and 3	<p>Level of access is based on the employee's job functions.</p> <p>Force system timeouts after 15 minutes of non-use and password expirations.</p> <p>Shut down accounts within 24 hours of an employee termination or illegal activities are detected.</p> <p>Monitor software licenses for inactive or pirated copies.</p> <p>Conduct surveillance of internet activities and e-mail usage.</p> <p>Perform random reviews of documents and software contained on agency-issued laptops.</p>
Legal Board orders that contain patient names	Investigations Department staff	Locked cabinet, drawer or room when not in use
Licensing applications and all their inclusions – passport copies, birth certificates, etc.	Licensing Department staff	Locked cabinet or drawer when not in use
Medical practice reports from various medical organizations	HPP and Investigations staff	Locked cabinet or drawer when not in use
Network and system configurations	Information Systems Specialist 7 and 5	Document all system and network configurations.

		<p>Establish and follow a formal configuration/change control process that includes vulnerability identification and patching.</p> <p>Document the responsibilities and show a separation of duties between the system administrator and the security administrator (Business Manager).</p>
Passwords	All OMB staff	<p>Changed at least every three months using a variety of character types – lower and upper case letters (A, b, C, d....), digits (0, 1, 2...), special characters (*, &, \$, etc.) and be at least 8 characters long.</p> <p>They may not be dictionary words or a sequence of characters from the keyboard (e.g. qwerty).</p> <p>Passwords may not be reused within two years.</p> <p>Passwords must be changed when they may have been compromised.</p>
Payroll records	Payroll Technician	Locked cabinet or drawer when not in use
Personally identifiable information – SSN, home address, etc. of licensees that are coded with a “no” (disclosure not allowed) on the client information screen	Licensing Department staff	The information owner must authorize disclosure, transmission or dissemination of this information.
Personnel files and other related human resource information	HR Manager	Locked cabinet or drawer when not in use
Police reports and court records	Investigations Department staff	Locked cabinet or drawer when not in use
Proprietary business information	Business Manager	Locked cabinet or drawer when not in use

<p>Regulated information covered under the Health Information Portability Act - generally all medical records</p>	<p>All OMB staff</p>	<p>Locked cabinet or drawer when not in use</p>
<p>Storage devices such as servers, desktop PC's, laptops, and portable devices.</p>	<p>Information Systems Specialist 7, 5 and 3</p>	<p>Always under at least one locked control – servers, laptops and portable devices in a room protected by a coded locking system.</p> <p>Desktop PC's are in a locked office after hours.</p> <p>Maintain an inventory of IT equipment that identifies who has the equipment and what information is on it.</p> <p>Ensure environmental protections are adequate- AC, fire detection, uninterrupted power supplies, etc.</p> <p>Disable unused ports.</p> <p>Know what applications are running and validate new applications against change management processes.</p> <p>Ensure appropriate wireless encryption protocol is enabled prior to the devices being connected to enterprise systems.</p> <p>Install and configure end-point protection software and ensure automatic updates are processed.</p> <p>Routinely check for unauthorized external access capability.</p> <p>Perform frequent scans to detect and remove viruses, worms and Trojans.</p>
<p>Portable media devices containing case information</p>	<p>All staff Board and Committee Members</p>	<p>Locked cabinet or drawer when not in use.</p> <p>When removed from the office,</p>

		<p>the devices must be both physically and technically protected. The protections would include:</p> <ul style="list-style-type: none"> • Permission from the information owner; • What information is on the device; • Who is in possession of the device; • If mailed, signature tracking is required; • Information transmitted via any type of portable media device must be encrypted; and • The users have been trained on protecting the devices which includes shelter from extreme temperatures and how to secure them using passwords and/or encryptions.
--	--	---

Risk Level 4 – Critical

Risk Definition: Information that is deemed extremely sensitive and is intended for use by named individual(s) only. This information is typically exempt from public disclosure because, among other reasons, such disclosure would potentially cause major damage or injury up to and including death to the named individual(s), agency employees, clients, partners, or cause major harm to the agency.

Information Asset	Owner(s)	Protection
None	N/A	If the OMB had Level 4 information assets, it must be protected at all times by two layers of control – in a locked cabinet in a locked room or office; transported using tamper-evident packaging and signature tracked; electronically by password protected zip files and encryption; and any disclosure must have Executive Director approval.

Oregon Medical Board

PROCEDURES

TITLE/SUBJECT: Information Asset Training and Monitoring Procedures
NUMBER: 847-206-002-B
SUPERCEDES: n/a
REFERENCE: Information Security Plan and Policy
APPLICATION: All OMB staff and Board members, temporaries, volunteers and contractors
INTERPRETATION RESPONSIBILITY: Business and HR Managers
EFFECTIVE DATE: August 1, 2008
REVISED: November 1, 2011

PURPOSE:

To establish how employees, Board Members, temporaries, volunteers and contractors will be instructed on information asset security.

PROCEDURE:

- 1) Each person shall be given a copy of the Information Security Policy and Procedures to review.
- 2) Each person will acknowledge receipt of the policy/procedures and they understand them. The signed document will reside in their personnel or contractor file.
- 3) At time of policy presentation, each person shall take an on-line training class. The course content is maintained by the Department of Administrative Services.
- 4) At least annual training shall occur on the subject of information security. The training will consist of a variety of topics based on current security threats as well as refresher education. For example, when new information assets arrive or change risk levels; when changes are made to transporting or destruction procedures; when new or updated training courses are offered; or simply taking the on-line training classes.
- 5) Managers will be responsible for their employee's participation in the training. They will also monitor compliance with information security policies and procedures by encouraging their employees to identify risk threats; taking personal responsibility for information security; engaging them in security processes; performing spot checks on locked file cabinets and doors, secure mailings follow process, auditing e-mail and internet usage, etc.; and evaluating their security performance on annual evaluations.
- 6) Contractors will be given a copy of OMB's Information Security Policy and Procedures. Final contracts will include language that requires business owners and their employees to meet the minimum security standards outlined in the Policies and Procedures.

Oregon Medical Board
PROCEDURES

TITLE/SUBJECT: Information Asset Security Incident Procedure
NUMBER: 847-206-002-C
SUPERCEDES: n/a
REFERENCE: Information Security Plan and Policy
APPLICATION: All OMB staff and Board members, temporaries, volunteers and contractors
INTERPRETATION RESPONSIBILITY: Business and HR Managers
EFFECTIVE DATE: August 1, 2008
REVISED: November 1, 2011

PURPOSE:

The Oregon Medical Board's information assets are critical to agency operations. All people who work for or transact business with the OMB are expected to protect and secure our information assets. In the event of a failure, this procedure will establish how information security incidents will be handled.

PROCEDURES:

- 1) What employees will do to help protect and secure OMB confidential information:
 - Secure confidential papers in your cubicle, in a locked file when not in use and when you leave for the day;
 - Do not leave confidential papers unattended on your desk, in the fax, printer or copy machine;
 - Make sure your computer screen is clear of sensitive information when you leave it, even for a minute;
 - Change your password at least every three months and use a password that complies with the password procedure found in 847-206-002-A;
 - Guard your password carefully. Do not share it with anyone else or post it in a visible area that others can easily see or access;
 - Make sure your data files are stored on the network server and not on your hard drive;
 - Take necessary precautions when sending sensitive or proprietary information via e-mail, shuttle, regular mail and portable electronic devices following the procedures found in 847-206-002-A;
 - Do not print licensee Social Security numbers on wallet cards, engrossed licenses, certificates, electronic lists, etc.
 - Verify fax numbers and addresses before sending information;
 - Do not talk about confidential information in a public area whether it is inside or outside the office;
 - Exercise care if you give talks or publish articles;
 - Do not leave messages regarding confidential information on answering machines;

- Check door pockets for sensitive information throughout the day and before leaving at night. Remove and secure the information.
 - Make sure discarded confidential documents are placed face down in shred barrels before leaving at night;
 - If a virus or unauthorized intrusion is detected or simply suspected on your computer, immediately turn it off and report it to your manager and the IT staff;
 - Lock or log off your computer prior to leaving for the day;
 - Never post confidential or personal information on Web pages;
 - Be aware of unfamiliar people in your work area; and
 - Report any suspicious activity to your manager or the Business Manager.
- 2) It is the objective of the Oregon Medical Board to safeguard all sensitive information. In the event safeguards fail or the confidentiality of information may have been compromised in any way, the OMB and its staff will respond to information security incidents as follows:
- a) The employee immediately notifies Section Manager or designee of the incident. A reportable incident is one that:
 - Involves information security;
 - Is unwanted or unexpected;
 - Shows harm, intent to harm, or a significant threat of harm; and
 - Response requires non-routine action.
 - b) The Section Manager immediately notifies the Executive Director, the Business and/or HR Managers and the Information Systems Specialist 7 (ISS7) technical expert.
 - c) The Business and/or HR Manager and the ISS7 perform an initial triage. They gather information, assess the nature of the incident and determine the information asset classifications involved. This is a critical step in ensuring the situation does not become more severe. Questions to ask are:
 - What type of incident has occurred?
 - What information asset classification has been jeopardized?
 - Who is involved?
 - What is the scope?
 - What is the urgency?
 - What is the impact so far?
 - What projects are impacted?
 - What can be done to contain the incident?
 - Are there other vulnerable or affected systems?
 - What are the effects?
 - What actions have been taken?
 - Has every action been documented?
 - Has evidence been gathered and preserved?
 - What are the recommendations for proceeding?
 - Who needs to know the details?
 - d) Communication is vital to incident response. The following details who is responsible for contacting whom:
 - The Business Manager is the designated point of contact for the Statewide Incident Response Team (SIRT) (503-378-5930). The backup point of contact is the HR Manager. If necessary, s/he will

notify the SIRT within 24 hours of the incident and inform the appropriate staff what actions are being taken.

- The Business Manager will also contact DAS's Risk Management Division (503-373-7475) and the Department of Justice (503-947-4520) if claims or legal action may arise from the incident.
- The Business Manager may need to contact the Criminal Lieutenant at Oregon State Police (503-378-3720) if criminal activity is suspected.
- The Executive Director is the designated point of contact for the Department of Administrative Services, Director's Office (503-378-3104). S/he will notify DAS based on the seriousness of the situation and keep the appropriate OMB staff updated. The backup point of contact is the Business Manager.
- The Executive Director is also the Communications Coordinator for the agency. It is important to control communications to ensure it is appropriate and effective. S/he will disclose incident information on a need-to-know basis. S/he will determine what should be released and when and whom it is released to.

e) Gathering and preserving evidence is critical. The Business and/or HR Manager and the Executive Director will carefully balance the need to restore operations against the need to preserve evidence.

- If the incident involves OMB's electronic systems, the ISS7 and affected management staff will gather and preserve evidence. The following forensic guidelines will be used:
 - Keep good records of observations and actions taken;
 - Make forensically-sound images of systems and retain them in a secure place;
 - Establish a chain of custody; and
 - Provide basic forensic training to staff that is assisting in the preservation of evidence.
- If the incident involves paper or transportation issues, the affected management staff will gather and preserve evidence and document actions.
- All information gathered will be conveyed to the Business and/or HR Manager and the Executive Director. Follow-up activities, such as personnel actions or criminal prosecution, rely on this evidence preservation.

f) After an incident, the affected staff, the ISS7, and the Business and/or HR Manager will focus on identifying, removing and repairing the vulnerability that led to the incident. They will pinpoint the cause and remove or eradicate it. The goal is to prepare for the resumption of normal operations with confidence that the initial problem has been fixed.

g) Within one week of the incident closure, a postmortem will be conducted. This analysis will allow all participants an opportunity to share and document details about the incident and to facilitate lessons learned.

3) The Oregon Medical Board shall inform all employees of the Information Security Policy and the accompanying Procedures at new employee orientation as well as annual training. Training can occur more often should the need arise. Training topics will also vary based on the needs at the time. For example, sharing lessons learned from an incident is invaluable and will be given as soon as possible after the incident.

Oregon Medical Board

PROCEDURES

TITLE/SUBJECT: Information Asset Disposal Procedures
NUMBER: 847-206-002-D
SUPERCEDES: n/a
REFERENCE: Information Security Plan and Policy
Statewide Policy 107-009-0050
APPLICATION: All OMB staff and Board members, temporaries, volunteers and contractors
INTERPRETATION RESPONSIBILITY: Business and HR Managers
EFFECTIVE DATE: August 1, 2008
REVISED: November 1, 2011

PURPOSE:

To establish how information assets will be disposed of to prevent the release of sensitive or protected information.

PROCEDURES:

Electronic waste (E-waste) is defined as excess, surplus, obsolete or non-working electronic equipment. Samples of E-waste equipment are desktop and laptop computers, monitors, copiers, fax machines, telephones, etc. E-waste can be returned to any vendor that meets the criteria for disposal which is described in State Policy 107-009-0050. Certified vendors remove, sanitize, overwrite or destroy information contained in those devices as required by this policy. E-waste may also be transferred to State Surplus who will remove sensitive, proprietary and licensed data according to State Policy and the Department of Defense standards.

Risk Level 1 information requires no special disposal protocol.

Risk Level 2 information requires shredding, placement in shredding barrels, and/or adherence to State Archive retention schedules and processes.

Risk Levels 3 and 4 information requires shredding, placement in shredding barrels, adherence to State Archive retention schedules and processes, and sanitation of hard disks, tapes, and other portable devices before being reused or disposed of. For detailed disposal steps, refer to the Sustainable Acquisition & Disposal of Electronic Equipment Statewide Policy 107-009-0050.