Oregon Medical Board

POLICY

TITLE/SUBJECT:	Information Security Policy
NUMBER:	847-206-002
SUPERSEDES:	n/a
REFERENCE:	Oregon Medical Board Information Security Plan State Policy 107-004-051, Controlling Portable & Removable Storage Devices State Policy 107-004-053, Employee Security State Policy 107-004-050, Information Asset Classification, State Policy 107-004-052, Information Security State Policy 107-004-100, Transporting Information Assets State Policy 107-004-120, Information Security Incident Response State Policy 107-009-0050, Disposal of Electronic Equipment State Policy 107-004-150, Cloud Computing ORS 646A.600 - Identity Theft Protection Act Oregon Laws 2016, Chapter 110
APPLICATION:	All Oregon Medical Board (OMB) Employees, Volunteers, Board Members, and Contractors.
INTERPRETATION RESPONSIBILITY:	OMB Business and HR Managers
EFFECTIVE DATE:	August 1, 2008
REVISED:	September 12, 2016

POLICY APPROVED BY: _____Signature on File _____
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, regardless of format.

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 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.
cloud	a paradigm for enabling network access to a scalable and elastic pool of sharable physical or virtual resources with self-service provisioning and administration on demand.
Cloud services contract	the sum total of all the documents that comprise a contract between a cloud service provider and the agency for cloud service
cloud services provider	a contractor providing cloud service to the agency.
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.
information user	all state employees, Board members, volunteers, their agents, vendors and contractors including those users affiliated with third parties who access state information assets, and all others authorized to access OMB information assets.
information 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 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.
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; 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 computer network diagrams; 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. Criminal history record information may not be disclosed or shared with external parties.

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 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; e-mails 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, media sent to consultants, archived documents, etc.); passwords and encryption system information; firewall configurations; business back-up media; court reporter recordings; 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 has been designed for each level of information asset classification. Controls are 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 must be tracked. 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.

Cloud Services

The agency will follow statewide policy 107-004-150 when considering and implementing cloud services contracts. This policy will guide the agency in evaluation of the benefits and risks of implementing the cloud service. Completion of the Cloud Planning and Readiness Assessment workbook required by that policy will help the agency understand the shared responsibility model of the cloud platform to establish data ownership to determine the security aspects for which the agency is responsible and which are the responsibility of the cloud services provider.

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.

This agency certifies that all information assets have been properly identified and 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 procedure “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 information users to protect information from unauthorized disclosure or compromise. Information users 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. Information users 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. All OMB portable devices used off premise will be encrypted. 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 details who is responsible for what response action. It includes triage, evidence preservation, forensics, communication, threat eradication, resumption of operations, postmortem discussions and awareness training.

Proper Disposal

Disposal of OMB information assets is guided by OMB Procedure 847-206-002-D. Paper files containing level 3 or level 4 data must be disposed of so that confidentiality is maintained. 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.

AGENCY OBLIGATIONS:

Employee Security Responsibilities

The agency and its employees will:

- Create and implement an Information Security and Incident Response Plan that complies 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 is not 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 information users 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 are suspected;
- The OMB Human Resources Manager performs surprise audits at least biannually to determine if doors, drawers, and cabinets that should be locked are locked 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;
- Provide access to only information that is necessary for the job;
- 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. Staff and Board members who are assigned laptops or tablets for the performance of their assigned duties must complete a Laptop and Tablet Acceptable Use agreement. Completed agreements will be stored within the agency asset tracking system.
- Ensure Level 3 information is provided to medical consultants only as necessary for them to fulfill their consultant responsibilities. Information provided will be secured using password encryption.

- Maintain a secure portal, enabling the agency to reduce the use of portable storage devices;
- The information owner will track what is stored on portable 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.

Cloud Services Information Security Responsibilities

When the agency has adopted cloud services through a cloud services contract, the agency will follow the below best practices to protect information on the cloud platform:

- Periodically review and monitor the security settings and file sharing service for cloud services to ensure that the access to documents stored in cloud remain limited to authorized users.
- Periodically change passwords for cloud services' administrative and user accounts to reduce risks of data loss from password breach.

Information Security Assessment Responsibilities

Periodically, the agency shall conduct or contract for an information security assessment of the agency's information system and information resources and shall request results from a third party's information security assessment of an information service that the third party provides and to which the agency subscribes.

An Information security assessment means:

A. An organized method to determine a risk to or a vulnerability of the agency's information system or a third party information service to which the agency subscribes; and
B. An independent examination and review of records, logs, policies, activities and practices to:
    i. Assess whether the agency's information system is vulnerable to an information security incident;
    ii. Ensure compliance with rules, policies, standards and procedures that the State Chief Information Officer; and
    iii. Recommend necessary changes to the agency's rules, policies, standards and procedures to ensure compliance and prevent information security incidents.

The agency shall notify the Legislative Fiscal Office of the information security assessment after the agency receives the results of the assessment.

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.

The following procedures describe how the OMB implements 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 Incident Procedures: 847-206-002-C
Information Asset Disposal Procedures: 847-206-002-D