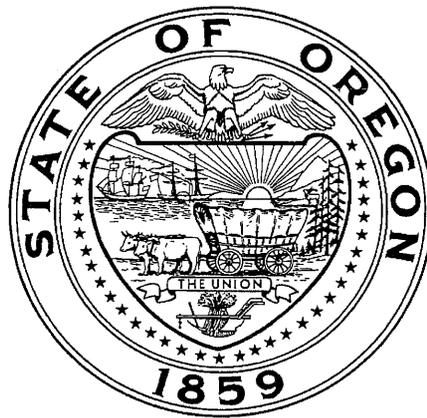


State of Oregon Information Security Plan & Risk Management Policies

Oregon Mortuary & Cemetery Board



Updated: January 17, 2013

***Portland State Office Building Suite 430
Portland, Oregon***

TABLE OF CONTENTS

1. Introduction.....	3
2. Terms and Definitions	3
3. Authority.....	4
4. Roles and Responsibilities.....	5
5. Security Program	5
6. Security Components.....	6
<u>Risk Management</u>	6
<u>Security Policy</u>	6
<u>Organization of Information Security</u>	7
<u>Asset Management</u>	7
<u>Human Resources Security</u>	7
<u>Physical and Environmental Security</u>	8
<u>Communications and Operations Management</u>	8
<u>Access Control</u>	9
<u>Information Security Incident Management</u>	9
<u>Business Continuity Management</u>	10
<u>Compliance</u>	10
7. Implementation.....	10
8. Approval	11

1. Introduction

Information is an asset that, like other important business assets, is essential to the Health Related Licensing Boards (HRLB) and consequently needs to be suitably protected. Information can be printed or written on paper, stored electronically, transmitted by post or by using electronic means, recorded photographically, or spoken in conversation. In whatever form the information takes, or means by which it is shared or stored, it should always be appropriately protected.

Information security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and protect the personal information of the Health Board's staff, licensees and clientele. Information security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures, and software and hardware functions. These controls need to be established and implemented. To ensure that the security and business objectives of the organization are met, these controls need to be reviewed frequently and updated as necessary.

The objectives identified in this plan represent commonly accepted goals of information security management as identified by the ISO/IEC 27002:2005 *Information technology – Security techniques – Code of practice for information security management*, the recognized standard for Oregon state government.

2. Terms and 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 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
information owner	person with the authority for specified information and has the responsibility for establishing the controls for its generation, collection, processing, dissemination and 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
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 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

3. Authority

Number	Policy title
ORS 182.122	Information Systems Security in Executive Department
ORS 291.038	Agency planning, acquisition, installation, use of Information and telecommunications
ORS 646A.600	Oregon Consumer Identity Theft Protection Act
ORS 676.110 – 676.440	Health Professions Generally, Occupations and professions
OAR 125-800-0005 through 0020	Department of Administrative Services, State Information Security rules <u>Administrative Rule</u>

Policy Number	Policy Title	Effective Date
107-004-050	<u>Information Asset Classification (pdf)</u>	1/31/2008
107-004-051	<u>Controlling Portable & Removable Storage Devices (pdf)</u>	7/30/2007
107-004-052	<u>Information Security (pdf)</u>	7/30/2007
107-004-053	<u>Employee Security (pdf)</u>	7/30/2007
107-004-100	<u>Transporting Information Assets (pdf)</u>	1/31/2008
107-004-110	<u>Acceptable Use of State Information Assets (pdf)</u>	10/16/2007
107-004-120	<u>Information Security Incident Response (pdf)</u>	11/10/2008
107-001-010	<u>Business Continuity Plan Statewide Policy (pdf)</u>	7/27/2010

4. Roles and Responsibilities

Executive Director	<p>Responsible for information security in the agency, for reducing risk exposure, and for ensuring the agency's activities do not introduce undue risk to the enterprise. The Executive Director is also responsible for ensuring compliance with state enterprise security policies, standards, security initiatives and with state and federal regulations.</p> <p>Responsible for identifying information assets and assessing their risk. The Executive Director handles the day-to-day security operations of the agency and is the Incident Response Point of Contact. The Executive Director communicates with the State's Incident Response Team and coordinates agency actions in response to an information security incident.</p> <p>Responsible for creating and maintaining the Information Security Plan, Policy and Procedures and obtaining management and state approvals for implementation. Ensures security policy training is conducted for employees, the policy is received and understood, and enforces the policy when required.</p>
Administrative Staff	Responsible in assisting the Executive Director in developing and implementing the Information Security Plan.
IT Consultant	Responsible for identifying security risks for all Board computerized systems and ensuring appropriate electronic and manual controls are in place to protect the information those systems contain.
Information Owner	Responsible for creating initial information classification, approving decisions regarding controls and access privileges, performing periodic reclassification, and ensuring regular reviews for value and updates to manage changes to risk.
User	Responsible for complying with the provisions of policies, procedures and practices.

5. Security Program

Information security is a business issue. The objective is to identify, assess and take steps to avoid or mitigate risk to agency information assets. Governance is an essential component for the long-term strategy and direction of an organization with respect to the security policies and risk management program. Governance requires executive management involvement, approval, and ongoing support. It also requires an organizational structure that provides an appropriate venue to inform and advise executive, business and information technology management on security issues and acceptable risk levels. Under the Oregon Mortuary and Cemetery Board (Board), the ultimate responsibility for managing information security lies with the Executive Director. The Executive Director is responsible for the day-to-day information security risk assessment and processes of the agency. The Information Technology Consultant is the technical expert on information security risk issues involving all Board IT systems. This position reports directly to the Executive Director. Creating, maintaining, training, implementing and enforcing the Board's Security Policy is the responsibility of the Executive Director.

In order to implement and properly maintain a robust information security function, the Oregon Mortuary and Cemetery Board recognizes the importance of:

- Understanding Board's information security requirements and the need to establish policy and objectives for information security;
- Implementing and operating controls to manage Board's information security risks in the context of overall business risks;
- Ensuring all users of agency information assets are aware of their responsibilities in protecting those assets;
- Monitoring and reviewing the performance and effectiveness of information security policies and controls;
- Communicating results of such audits to the DAS Enterprise Security Office; and
- Continuing improvements based on assessment, measurement, and changes that affect risk.

The goal of this security plan is to identify, classify, manage, transport and secure information assets based on their confidentiality, sensitivity, value and availability requirements. It will also identify how employees will receive policy and security awareness training.

Mortuary & Cemetery Board

Information Security Plan & Risk Management Policies

OMCBUsers:Admin:Information Systems:Security Plan 2012:2012 Security Plan Risk Management Policies for OMCB.docx

6. Security Components

Risk Management

Risk Management refers to the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level. Risk management is critical for each Agency to successfully implement and maintain an acceptable level of risk. Risk assessments will identify, quantify, and prioritize risks against agency criteria for risk acceptance and objectives. The results will guide and determine appropriate agency action and priorities for managing information security risks and for implementing controls needed to protect against those risks.

Risk management will include the following steps:

1. Identify the risks
 - a. Identify agency assets and the associated information owners
 - b. Identify the threats to those assets
 - c. Identify the vulnerabilities that might be exploited by the threats
 - d. Identify the impacts that losses of confidentiality, integrity and availability may have on the assets
2. Analyze and evaluate the risks
 - a. Assess the business impacts on the agency that might result from security failures, taking into account the consequences of a loss of confidentiality, integrity or availability of those assets
 - b. Assess the realistic likelihood of security failures occurring in the light of prevailing threats and vulnerabilities, and impacts associated with these assets, and the controls currently implemented
 - c. Estimate the level of risks
 - d. Determine whether the risks are acceptable
3. Identify and evaluate options for the treatment of risk
 - a. Apply appropriate controls
 - b. Accept the risks
 - c. Avoid the risks
 - d. Transfer the associated business risks to other parties
4. Select control objectives and controls for the treatment of risks

It is recognized that no set of controls will achieve complete security. Additional management action will be implemented to monitor, evaluate, and improve the efficiency and effectiveness of security controls to support agency goals and objectives.

The Executive Director will develop the Security Plan and Policy.

The Executive Director will work with the Information Technology Consultant in creating a plan, policy and procedures that identifies the risks, classifies those risks and creates control to mitigate risks.

Security Policy

The objective of information security policy is to provide management direction and support for information security in accordance with each OMCB's business requirements and governing laws and regulations. Information security policies will be approved by management, and communicated to all employees and relevant external parties. These policies will set out OMCB's approach to managing information security and will align with relevant statewide policies.

Information security policies will be reviewed annually or when significant changes occur to ensure their continuing suitability, adequacy, and effectiveness. Reviews will include assessing opportunities for improvement of information security policies and approach to managing information security in response to changes to environment, new threats and risks, business circumstances, legal and policy implications, and technical environment.

The Security Policy and Procedures will identify and classify information security risks, how the OMCB will manage those risks, how information will be transported, and how Agency employees will learn and carry out the policies and procedures.

Organization of Information Security

The mission of the Oregon Mortuary and Cemetery Board is to protect the public health, safety and welfare by fairly and efficiently performing its licensing, inspection and enforcement duties; by promoting professional behavior and standards in all facets of the Oregon death care industry; and, by maintaining constructive relationships with licensees, those they serve and others with an interest in the Board's activities. To ensure it meets this mission, the Board has a number of goals and strategies that require the collection and use of sensitive information. The information includes such things as home addresses and phone numbers, social security numbers, certified copies of birth certificates, background checks, police reports, investigation reports, disciplinary actions, credit card transactions, etc.

Information security will be managed within the Board. The Executive Director will approve information security policies, assign information owners and record the specifics in Information Security Procedure A, and coordinate and review the implementation of security across the agency. Information security will be coordinated across different parts of the agency with relevant roles and job functions. Information security responsibilities will be clearly defined in the Information Security Procedures (A-D) and will be communicated during new employee orientation, training sessions and in position descriptions. Security of Board's information assets and information technology that are accessed, processed, communicated to, or managed by external parties will be maintained by placing security language in contracts, creating tracking systems and performing audits.

The Executive Director will ensure Information Security Policies and Procedures conform to agency business requirements and will create the policies and procedures based on agency business needs and the technical expertise of the Information Technology Consultant.

Asset Management

The objective of asset management is to achieve and maintain appropriate protection of the Board assets. All agency assets will be identified and inventoried by interviewing agency employees. Owners of information assets will be identified by determining who has the most control over the information. They will be assigned this responsibility in Policy and will recommend the risk classification of the assets and maintain the appropriate controls. To ensure information receives an appropriate level of protection, information will be classified to indicate the sensitivity and expected degree of protection for handling. The Board will use four different levels of information asset classification. How information is assigned a level will be based on the value, sensitivity, criticalness and legal implications of the information. The technical expert (Information Technology Consultant) and the Executive Director will review the risk-level recommendations and edit as needed. Final recommendations will be presented to the Executive Director who will review, edit and approve or deny them.

The assets and their classifications will be reviewed by the Information Technology Consultant and the Executive Director at least annually. Information Security will be the motivating force behind how sensitive information assets will be identified, documented, implemented, protected and enforced. The Executive Director will review the Board's use of secure mailing and shuttle services; e-mail and internet usage; performing checks on doors and cabinets to ensure they are securely locked at the appropriate times; researching training opportunities; requiring information security training at least annually and maintaining attendance records; ensuring employees comply with the agency's Training Procedures ISP-B; making information security part of each employee's annual performance evaluation; and keeping records of all audits and inspections. The Executive Director may request biannual security audits from the Enterprise Security Office once they identify contractors for state agency use.

Human Resources Security

All employees, volunteers, contractors, and third party users of the Board information and information assets will understand their responsibilities and will be deemed suitable for the roles they are considered for to reduce the risk of theft, fraud or misuse. Security responsibilities will be addressed prior to employment in job descriptions and any associated terms and conditions of employment. Where appropriate, all candidates for employment, volunteer work, contractors, and third party users will be adequately screened, especially for roles that require access to sensitive information. Management is responsible to ensure security is applied through an individual's employment with the Board.

The Board will perform such security background checks on potential employees as allowed by law. The requirement for these checks as well as the requirement to abide by Board's policies and procedures will be included in all position descriptions. Employees will read, and acknowledge understanding the agency's Information Security Policies and Procedures. Employees will be rated on their adherence to the policies and procedures in their annual performance evaluation. Employees and, where relevant, volunteers, contractors and third party users will receive appropriate awareness training and regular updates on policies and procedures as relevant for their job function. Procedures will be implemented to ensure that all equipment and access right are removed and that exit procedures are completed by employees, volunteers, contractors or third parties who no longer work for the Board.

The Executive Director will ensure the policies and procedures are reviewed at least annually and when security and/or information asset changes occur. The Executive Director will also ensure all employees receive timely and appropriate training on the policies and procedures.

Physical and Environmental Security

The objective of physical and environmental security is to prevent unauthorized physical access, damage, theft, compromise and interference to the OMCB's information and facilities. Areas housing critical or sensitive information or information assets will be secured with appropriate security barriers and entry controls. They will be physically protected from the elements, unauthorized access, damage and interference. Secure areas will be protected by appropriate security entry controls to ensure that only authorized personnel are allowed access. Security Procedures will be applied to off-site equipment. Sensitive data and licensed software will be removed or securely overwritten on storage media prior to disposal.

The staff of OMCB will use the appropriate level of protection for the assigned level of risk for all their information assets. When the highest level of protection is required, the information will be protected by a double set of physical protections (for example in a locked file cabinet in a locked room), encryption and password control. Physical and environmental factors will be considered when protecting sensitive information.

Communications and Operations Management

Responsibilities and procedures for the management and operation of all IT Equipment will be established. As a matter of policy, segregation of duties will be implemented, where appropriate, to reduce the risk of negligent or deliberate system or information misuse. Precautions will be used to prevent and detect the introduction of malicious code and unauthorized mobile code to protect the integrity of software and information. To prevent unauthorized disclosure, modification, removal or destruction of information assets, and interruption to business activities, media will be controlled and physically protected. Procedures for handling and storing information will be established and communicated to protect information from unauthorized disclosure or misuse. Exchange of sensitive information and software with other agencies and organizations will be based on a formal exchange process. Media containing information will be protected against unauthorized access, misuse or corruption during transportation beyond OMCB's physical boundaries.

The highest protection level on information that needs to be transported will be done by ensuring appropriate transport procedures in place. This includes the use of reliable carriers and incorporating security language into their contracts; ensuring employees who carry sensitive information follow transport requirements; packaging will protect the contents; labeling is clear on both the inside and outside of the package; maintaining a chain of custody; and using other risk management techniques such as locking storage containers, encryptions and tamper evident packaging.

When employees, volunteers or contractors use portable and removable storage devices, they will only be given access to the sensitive information they need to do their jobs. The information owner will develop procedures that will monitor the location and the information stored on the device. Supervisors will ensure that users receive all appropriate Policies and Procedures. To detect unauthorized access to agency information and information systems, systems will be monitored and information security events will be recorded and reported. The OMCB will employ various monitoring techniques to comply with applicable statewide policies which are referenced and included in the Security Policy.

When sensitive information or equipment containing this information is no longer needed, appropriate disposal procedures will be followed. Those procedures include permanently destroying information that has reached the appropriate retention timeframe, and physically destroying disks, drives, Compact Disks, etc.

The Executive Director is responsible for arranging for or directly providing training and monitoring all employees and volunteers in the policies and procedures of information security. Contractors will be required to comply with our information security policies and procedures by placing the condition in their contracts and supplying them with copies of the policies and procedures.

Access Control

Access to information, information systems, information processing facilities, and business processes will be controlled on the basis of business and security requirements. Formal procedures will be developed and implemented to control access rights to information, information systems, and services to prevent unauthorized access. Users will be made aware of their responsibilities for maintaining effective access controls, particularly regarding the use of passwords. Users will be made aware of their responsibilities to ensure unattended equipment has appropriate protection. A clear-desk policy for papers and removable storage devices and a clear-screen policy will be implemented, especially in work areas accessible by the public. Steps will be taken to restrict access to operating systems to authorized users. Protection will be required commensurate with the risks when using mobile computing and teleworking facilities.

The Board will ensure password and encryption policies are addressed in its procedures. The Information Technology Consultant will be responsible for ensuring the appropriate controls are programmed. The Executive Director will ensure those controls meet business requirements and will provide secondary oversight. All employees will receive training on the use of passwords, when systems are to be locked or timed out, how the different levels of information security determines how the information is handled, and when and how information will be transported and disposed of.

Information Systems Acquisition, Development and Maintenance

All staff will comply with policies and procedures to ensure the security of information systems. Encryption will be used, where appropriate, to protect sensitive information at rest and in transit. Access to system files and program source code will be controlled and information technology projects and support activities conducted in a secure manner. Technical vulnerability management will be implemented with measurements taken to confirm effectiveness.

The Executive Director will develop systems that focus on the appropriate level of security for the lifetime of the system. Contracts will be developed and implemented with security issues addressed. Appropriate sensitive information sharing will be reviewed and approved by the Executive Director. Vulnerabilities will be assessed and penetration tests will be run. Encryption procedures will be implemented. The transport of sensitive information will follow policies and procedures.

Information Security Incident Management

Information security incidents and weaknesses associated with information systems will be communicated in a manner allowing timely corrective action to be taken. Formal incident reporting and escalation procedures will be established and communicated to all users. Responsibilities and procedures will be established to handle information security incidents and vulnerabilities once they have been reported.

It is the objective of the Executive Director to safeguard all sensitive information. In the event the safeguards fail, the Agency Director will report information security breaches as follows:

- The employee immediately notifies the Director of the incident;
- The Director immediately notifies the Board Chair and IT consultant;
- The Director is the designated IT point of contact for the Statewide Incident Response Team (SIRT) and will notify them as described in the Incident Response Plan;

- All supervising staff will respond in accordance with the Policies and Procedures to the Incident Response Plan.
- The Executive Director is the designated point of contact for the Department of Administrative Services, Director's Office and will notify DAS based on the seriousness of the situation.

Business Continuity Management

The objective of business continuity management is to counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption. The Board has in place a business continuity plan (BCP) that addresses management's process to minimize the impact of these interruptions. The BCP is reviewed biannually to ensure processes continue to meet business requirements. It is frequently updated whenever an employee leaves, a new employee is hired, or when business contacts change. Emergency response drills are conducted at least annually using different scenarios – earthquake, flood, bomb scare, etc. The BCP includes instructions on how to secure the office and the information assets it contains; how and who to notify in case of emergencies; how contact will occur if lines of communication are severed; where employees will assemble; who is responsible for specific tasks (like recovery of electronic systems and databases, mail management, customer communications, etc.) and who the backup is; and how employees will be informed and trained on BCP.

Compliance

The design, operation, use, and management of information and information assets are subject to statutory, regulatory, and contractual security requirements. Compliance with legal requirements is necessary to avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements. Legal requirements include, but are not limited to: the Board Statute (ORS chapter 692), Oregon Administrative Rules (OAR chapter 830), criminal laws, Oregon Administrative Procedures Act, other state statutes, statewide and agency policy, regulations, contractual agreements, intellectual property rights, copyrights, and protection and privacy of personal information. Both statewide and agency policies used to support this plan are listed on page 2.

Controls will be established to maximize the effectiveness of security of information assets and protection of the audit process for the Board. Controls can range from documenting who has keys to secure storage areas to tracking when passwords are changed. Controls will safeguard operational systems and audit tools used to protect the integrity of information and prevent misuse.

To prevent misuse and ensure the Board's policies and procedures are current and applicable, they will be randomly reviewed by the Executive Director. The Executive Director will conduct compliance audits as follows: biennial review of policies and procedures with all employees, quarterly random interviews with information owners to ensure all assets have been identified and procedures are in place to protect the information. Monthly spot checks will be done to ensure doors, cabinets and computers follow the appropriate protection levels for the information that is being used. Reviews of information technology contracts will ensure information security requirements are addressed. Adding the requirement for contractors to abide by the Board's Security Policy will be placed in all contracts when they are created or renewed. Regular testing and monitoring of the use of passwords will be performed.

Periodic audits of the personal use of the Board's computer system will be performed to ensure compliance with the Acceptable Use policy. Annual review of physical inventories and destruction log sheets will ensure compliance with procedures on the appropriate storage and disposal of IT assets. Records of all audits will be maintained by the Executive Director and reported to the DAS Enterprise Security Office in January of each year.

The Board will also consider use of the new contracts being developed by the Enterprise Security Office for IT security audits.

7. Implementation

The Board is responsible for the security of all our information assets in whatever format they take. That includes the Local Area Network, agency-owned systems, specialized applications, desktop and laptop computers, paper files, etc. The Board is committed to identifying our information assets, assigning a risk classification to them, and protecting them from their creation to disposal. To meet this goal, the Board has created this plan. The Plan will give direction and support for its Information Security Policy and Procedures. The Policy and Procedures have been developed in conjunction with the Plan. They will lay out the specific requirements and processes needed to implement the Plan. The Executive Director will train employees, volunteers and contractors on the Policy and Procedures within one month of implementation and monitor

Mortuary & Cemetery Board

Information Security Plan & Risk Management Policies

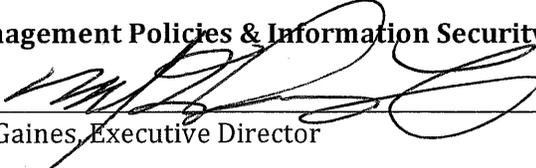
OMCBUsers:Admin:Information Systems:Security Plan 2012:2012 Security Plan Risk Management Policies for OMCB.docx

compliance by active management oversight, performing random audits and reviewing reports. The Executive Director will formally evaluate each employee's execution of the Policy and Procedures by including Information Security as a performance measure on their annual appraisal. The Executive Director will respond to breaches of security quickly and efficiently, and the Board will keep information security to the forefront of all business practices.

The Information Security Plan, Policies and Procedures are living documents. The very nature of information assets and systems subject them to constant change. We expect the documents to change just as frequently. Whenever changes occur, The Executive Director will update whatever documents are affected. Changes can come from all levels – top management because of law, business or policy changes all the way to the line employee because of a shuttle route change. This Plan, as well as the Policies and Procedures, will become an integral part of everyday Oregon Mortuary and Cemetery Board operations.

8. Approval

Risk Management Policies & Information Security Plan for Oregon Mortuary & Cemetery Board

By:  _____ Date 17 Jan 2013
Michelle Gaines, Executive Director

Policy No. 2012 – 01 Information Security

Approval date January 1, 2012

Objective: To establish an information security program that complies with state polices and other federal and state regulations

Reference: DAS Information Security policy (107-004-052)

Policy

It is the policy of the state of Oregon to ensure the confidentiality, integrity, and availability of information assets entrusted to the state by its citizens by securing those assets from unauthorized access, modification, destruction, or disclosure and to ensure their physical security.

This policy applies to all employees and individuals working for third parties that have an authorized business relationship with the agency who have been granted access to agency information independent of its form. This policy is modeled after and complies with the DAS Information Security policy (107-004-052).

Each Agency Director for each Board is responsible to ensure all employees and individuals working for third parties understand and adhere to this policy. The security of the agency's information assets is everyone's responsibility. Access to information must be strictly controlled using the least-privilege principle, and information must be used only for business purposes. Executive management is committed to this policy.

The OMCB has established an Information Security Program that complies with the DAS security policy framework, state policies, applicable regulations, and relevant industry best practices. The Executive Director will clearly state organization-wide objectives, identify and assign responsibilities, develop and implement security policies and practices, and provide a framework for monitoring and enforcement.

Information security policies will be reviewed annually to accommodate organizational changes and the evolving information security environment.

Roles and responsibilities:

The Executive Director is accountable for all levels of responsibility when using agency information assets held by the individual Agency and each Director is responsible to:

- establish an information security program and plan to govern the integrity of information assets
- authorize access to assets and comply with legal requirements for information confidentiality

The Executive Director will act as the Agency Information Officer and Information Security Officer and is responsible for prioritizing information security efforts, reviewing and recommending security policies, promoting organizational security efforts and recommending strategic direction. The following are included:

- strategic planning and implementation of information technologies
- aligning information technologies with statewide technical architecture and standards
- managing information technology resources
- creating and managing a reliable, secure network
- convening the Information Security Incident Response Team (SIRT) when an incident occurs and evaluating information security incidents and response
- coordinating agency's actions with SIRT in response to incidents involving information security

The Executive Director shall:

- acquire, develop, and maintain production applications to process agency information
- designate data classification levels for systems and data elements
- define system service level requirements
- define access privileges and approve access requests,
- monitor compliance
- investigate information security incidents, and
- establish procedures to resolve information security policy violations.

Employees, contractors, vendors, and business partners are responsible for:

- complying with all information security policies
- using information only for agency business purposes, and
- maintaining the confidentiality, integrity, and availability of the information

Compliance:

All employees, contractors, vendors, and business partners are responsible for understanding and complying with information security policies.

Violation of this policy or associated policies, standards, guidelines, or procedures can result in limitation, suspension, or revocation of system privileges and can lead to other disciplinary action up to and including dismissal for employees or termination of contracts for contractors, vendors, or business partners. Violations can also result in civil and/or criminal prosecution.

Individuals have the responsibility to report suspected policy violations to the Executive Director. All reports of alleged policy violations will be investigated

Policy No. 2012 - 02 Systems Access and Termination Policy

Approval date January 1, 2012

Objective: To establish policy on setup and deactivation of access to OMCB systems, and other third-party systems accessed by OMCB staff.

Policy

This policy outlines agency management's responsibility and the process for establishing and terminating system access for Board employees, contractors, and others that require access in support of agency business needs. The objective of this policy is to promote a high level of information security by providing access to system resources only while performing agency business.

Responsibilities. The Executive Director is responsible for granting and terminating system access for individuals under their control (employees, temporaries, and contractors). System access includes both internal systems and systems provided by external business partners. The Executive Director shall keep employee files to establish, modify, or terminate all systems access for an employee, temporary employee, or contractor. Managers are required to complete this form and send it to the

Establishment/Modification of Access. The Executive Director will grant employee and contractor access based on the principle of "least privilege." This ensures individuals receive the minimum level of access to information systems necessary to perform their duties. Directors are responsible for authorizing access to staff under their control. The Director shall submit appropriate requests to the PSOB Building Manager for access to any assigned work areas of the Portland State Office Building.

Termination of Access. It is essential that the Executive Director terminate access to agency systems in a timely manner to protect the information, systems, and resources. The Executive Director is required to terminate access immediately upon termination of the employee or contractor. Responsibilities for terminating access are for all employees, contractors or anyone needing access. The Director is responsible for processing the termination, in accordance with DAS HR. The Director shall submit appropriate requests to the PSOB Building Manager to termination of access rights to work areas in the Portland State Office Building.

Dated: Jan. 1, 2012

No. 2012 - 02 Physical Security - Facility Access Controls

Approval date January 1, 2012

Objective: To establish policy on setup and deactivation of access to OMCB systems.

Policy

This policy applies to all individuals who work within agency facilities in the Portland State Office Building. It is the responsibility of all Agency staff to ensure visitors are properly monitored and escorted in compliance with this policy.

Facility access - employees and authorized contractors

All agency facilities have controlled access environments with the exception of public areas identified in this policy. Only authorized personnel with official business are allowed entry into designated work areas. Individuals should not be in agency facilities more than 30 minutes before and/or after their scheduled appointment without Director's approval.

All employees and some contractors will need to be issued access cards for access. The access card allows entry into designated areas and a photo identification badge provides a visual means to identify employees and contract staff. In some cases, employees may also need a physical key to access their work area.

Employees and contractors are provided photo identification badges for ease of identification within the facilities. Employee photo identification badges have the employees name printed on them. The Photo identification badges are to be worn at all times while within the facilities and displayed above the waist in plain sight.

Board employees and contractors are NOT authorized to enter other areas of the Portland State Office not controlled by the OMCB or otherwise designated as a public area. Staff and contractors must have authorization to access any such areas to be granted by the controlling Agency.

Facility access - visitors

There is a designated public area, on the ground floor of the State Office building which can be used and on the 4th floor hallways which includes restrooms, and the kitchen. The Conference room 445 is not a public area, except when approved meetings allow for public access. The public areas can be accessed by the public unescorted during posted business hours from 8 a.m. to 5 p.m. Monday through Friday. Visitors may also attend OMCB events in other areas when scheduled outside of normal business hours, without an escort.

The office spaces at the State Office Building have public areas that are maintained by their respective property owners and fall outside the scope of this policy. To go beyond the public areas in agency facilities, visitors are required to be escorted by an authorized employee or contractor. The employee is responsible that Visitors are not left alone.

Management of physical keys, access cards, and photo identification badges

Photo identification badges and keys are issued by the Portland State Office Building Manager. It is each employee's responsibility to provide appropriate protection of his or her physical key, access card with photo identification badge to prevent unauthorized use. Badges should not be worn or displayed when off premises.

The Executive Director shall authorize the issuance of physical keys, access cards with photo identification badges for their employees by using the appropriate request forms. The Director or authorized Manager will pick up access cards for their employees from the PSOB Building Manager. Active access cards will not be sent through the interoffice mail system. Employees or contractors authorized to be issued a physical key can obtain the key from

Mortuary & Cemetery Board

Information Security Plan & Risk Management Policies

OMCBUsers:Admin:Information Systems:Security Plan 2012:2012 Security Plan Risk Management Policies for OMCB.docx

the OMCB's Director. The Portland State Office Building Manager maintains an inventory of keys issued and returned. The physical key is the responsibility of the employee or contractor issued the key and must not be given to any other person.

New employees and contractors are scheduled by the Building Manager to have their photos taken when a request is received to have an access card established. Photo identification badges are issued during this appointment.

For a new Agency Director, another authorized staff member or Board chair shall aid in obtaining required pass and keys.

Deactivation of access cards and return of physical keys

Directors are responsible to ensure the timely return of physical keys and deactivation of an access card when an individual leaves employment or when access requires immediate restrictions. The Director can request terminating or restricting access of an employee or contractor by contacting the PSOB Building manager.

Lost or damaged physical keys and access cards

In the event of a lost or damaged access card, the employee or Director must contact the PSOB Building manager and request immediate deactivation of the lost or damaged card to minimize the potential for unauthorized access into agency facilities. The must submit a request for issuing a new access card.

In the event of a lost or damaged physical key, the employee or contractor must contact the Director who then contacts the PSOB Building manager.

Lost photo identification badges

Employees will contact their Director who will contact the PSOB Manager to request a replacement photo identification badge. Directors will pick up badges and give to the employee. The Agency Director will verify the picture on the photo matches the employee receiving the badge.

Request for changes to photo identification badge

The Executive Director can request changes to the information on the photo identification badge when an employee changes his or her name by sending. Employees should turn in old badges to their managers for destruction

Forgotten access cards

Employees who forget their access cards must gain access by calling an authorized employee each time to access the suite.

Access times

Access times are based on the agency's operational hours, employee work schedule, and the employees' business needs to access the facilities. The access times listed below allow entry into all general work areas within the facilities. Agency Directors shall indicate the times that most closely cover the work hours of the employees as outlined

There are three access levels. Agency Directors will determine the appropriate level of access for employees or contactors:

Level 1: Mon - Fri 7 to 7

Level 2: Mon - Sun 7 to 7

Level 3: 24/7

E-mail approval from the Director to allow access into restricted areas is acceptable. General access areas, such as elevator access, are restricted by hours of operation of the Portland State Office Building which are from 8 - 5 Monday - Friday except for holidays and furlough days.

Mortuary & Cemetery Board

Information Security Plan & Risk Management Policies

OMCBUsers:Admin:Information Systems:Security Plan 2012:2012 Security Plan Risk Management Policies for OMCB.docx

Reports

The Portland State office Building manager keeps a list of all employees or contractors who were issued keys. The Agency Directors shall provide the level of access for keys. Agency Director must notify the Building manager as soon as reasonable if the employee or contractor no longer needs a key. Agency Directors are responsible for returning physical keys to the Portland State office Buildings Facilities Services manager as soon as reasonable.

Training and orientation

New employees receive instruction on the agency badge systems during their initial employee orientation. Training is conducted by the Executive Director and provides guidance on the use and display of access photo identification badges. Continued education is conducted through internal communications or publications and during regularly scheduled staff meetings within the agency.

Challenging access

Employees and contractors are responsible for helping ensure only authorized persons enter agency facilities beyond the designated public area. Individuals are encouraged to challenge an unrecognized person not displaying an appropriate photo identification badge or a visitor without an authorized escort outside the designated public area. It is not necessary to challenge visitors in the designated public area during posted business hours. Individuals not comfortable challenging someone should contact management immediately.

Door security

Individuals are responsible to ensure all those coming through secure doors have the required badge at entry. Doors must be properly closed and latched to avoid unauthorized access into the agency's facilities. This includes doors leading to restricted areas from designated public areas at all times, as well as external public doors. These doors are not allowed to be propped open while unattended

Policy 2012 - 03 Systems Development Life Cycle Policy

Executive Summary

This document provides an overview of the IT System Development and Life Cycle process for the OMCB and other HRLB agencies in the Portland State Office Building, a core system which helps manage a wide variety of activity to the licensee Data Base and conduct projects or automate Agency activities with information technology. The Data Base is not limited to technical activity but actually begins with customer needs and evolves through processes and user requirements to develop a solution or support process.

A more detailed explanation of procedures is outlined in an Agency Policy and Procedures manual and/or Desk Manuals. The primary objective of implementing a standardized policy is to provide coordinated excellent service to support the activity of customers and users of all the HRLBs who share IT Systems.

IT support and Contract:

Any IT Support for OMCB will be provided under the direct guidance of Grant A. Moyle, who is contracted as OMCB's primary Systems IT contractor. Mr. Moyle will be the primary/lead contact for all issues. Mr. Moyle will perform all remote work on the Agency's systems, unless notified and agreed to by the Agency, in advance.

The Contractor will provide on-going database development and support (based on Microsoft Visual FoxPro and Microsoft CRM), network and e-mail support services (based on Windows Small Business Server/Microsoft Exchange), and desktop support (Windows 2000 Professional) for the Agency.

DATABASE SERVICES:

Maintain and update the Visual FoxPro Licensing & Investigation Database used by the Agency
Design new database reports, formats and procedures as required by the Agency
Create merge functions for advanced mail merge and integration with other applications, including a searchable, Web-based directory of licensees
Provide database export capabilities to meet the requirements of the Oregon Department of Justice, Oregon Department of Revenue, etc. per Oregon Revised Statutes
Train staff in the application of new features of the database, as needed
Develop and Implement a secure, web based renewal system

WORKSTATION SERVICES:

Install, configure, maintain, and troubleshoot Windows XP Professional workstations and related application software; provide upgrade support for future needs
Install, configure, maintain, and troubleshoot workstation and application connectivity with printers, local area network (LAN) and wide area network (WAN) resources
Recommend hardware and software upgrades, as necessary
Ongoing support using SharePoint and other State tools for www.oregon.gov website management and interact on behalf of the Board with DAS, EDS, IRMD and other EGov resources within the state

SERVER AND NETWORK SERVICES:

Manage, monitor, and maintain Microsoft Exchange Server 2003 and future updates/versions.
Manage, monitor, and maintain Corporate/Enterprise Antivirus Services
Manage, monitor, and maintain local Firewall/VPN services to support remote connectivity.
Consult with staff and provide support for LAN and Internet connectivity

Consult with staff and provide assistance in obtaining support from vendors for warranty services.
Recommend hardware and software upgrades, as necessary
Represent the interest of the Board's to IRMD infrastructures, including E-mail, Local Area Network (LAN), Wide Area Network (WAN) and internet

INFORMATION SECURITY POLICIES:

Discuss and implement Information Security Policies with Agency
Work with Agency staff to ensure protection of sensitive information
Assess and enhance network security, disaster recovery, and business continuity for the Licensing Boards

Part III. Special Considerations.

KEY PERSON:

Contractor acknowledges and agrees that Agency selected Contractor, and is entering into this Contract, because of the special qualifications of Contractor's key people. In particular, Agency through this Contract is engaging the expertise, experience, judgment, and personal attention of Grant A. Moyle ("Key Person"). Contractor's Key Person shall not delegate performance of the management powers and responsibilities he is required to provide under this Contract to another (other) Contractor employee(s) without first obtaining the written consent of Agency. Further, Contractor shall not re-assign or transfer the Key Person to other duties or positions such that the Key Person is no longer available to provide Agency with his expertise, experience, judgment, and personal attention, without first obtaining Agency's prior written consent to such re-assignment or transfer. In the event Contractor requests that Agency approve a re-assignment or transfer of the Key Person, Agency shall have the right to interview, review the qualifications of, and approve or disapprove the proposed replacement(s) for the Key Person. Any approved substitute or replacement for a Key Person shall be deemed a Key Person under this contract.

Oregon Mortuary and Cemetery Board
INFORMATION SECURITY PROCEDURES

TITLE/SUBJECT: Information Asset Identification Tables and Protection Procedures
NUMBER: ISP-A
REFERENCE: Information Security Plan and Policy
APPLICATION: All Board staff and Board members, temporaries, volunteers and contractors
EFFECTIVE DATE: September 2010

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.

Note: The Board classification levels in this Policy Procedure follow the guidelines in the statewide policy.

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 Executive Director or designee of the information asset and the risk level assigned to it.
- 5) The Executive Director 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	Executive Director	No special handling or safeguards required
Lists of licensees	Office Manager	No special handling or safeguards required
Other materials created for public consumption	Executive Director	No special handling or safeguards required
Press releases	Executive Director	No special handling or safeguards required
Public Web pages	Executive Director	No special handling or safeguards required
Public Board disciplinary orders	Executive Director	No special handling or safeguards required
Published annual performance progress reports	Executive Director	No special handling or safeguards required
Published budget documents	Executive Director	No special handling or safeguards required
Published licensing records	Executive Director	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	Executive Director	Not in public view. May be sent electronically or mailed without security controls
Names, addresses & phone numbers of licensees facility or workplace.	Executive Director / Office Manager	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.)	Executive Director / Office Manager	Not in public view. May be sent electronically or mailed without security controls
Published internal audit reports	Executive Director	Not in public view. May be sent electronically or mailed without security controls
Regular outgoing checks	Executive Director / Office 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	Executive Director / Office Manager	Locked cabinet or drawer when not in use
Cash receipts – anything of monetary value including credit card transactions	Executive Director / Office Manager	Locked cabinet or drawer when not in use
Contracts with vendors that handle sensitive information	Executive Director / Office Manager	Contracts must contain security language and stored in a secure location.
Correspondence containing case related information	Executive Director / Compliance Manager / Investigator(s) / AAG	Locked cabinet or drawer when not in use
Court reporter tapes, voice files, transcripts and CDs	Executive Director / Compliance Manager / Investigator(s) / AAG	Tapes must be protected at all times with at least one level of security.
Employee and licensee health related information in formats such as paper, fax, e-mail, FMLA files, CDs sent to consultants, archived documents, etc.	Executive Director / Compliance Manager / Office Manager	<ul style="list-style-type: none"> ○ Locked cabinet, drawer or room when not in use. ○ If mailed, signature tracking process and logging system will be used. ○ No downloading of sensitive information onto personally owned computers or wireless storage devices.
Firewall configurations	Executive Director / Information Technology Consultant	<ul style="list-style-type: none"> ○ 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. ○ Use intrusion detection and prevention systems. ○ Keep records on what is “normal” network traffic.
Incoming mail that contains checks	Executive Director / Compliance Manager / Office Manager / Investigator(s) / Office Assistant	Locked cabinet or drawer when not being processed

Investigations that are in process and the permanent investigation files	Executive Director / Compliance Manager Office Manager / Investigator(s) / AAG	Locked cabinet, drawer or room when not in use
IT business security back-up procedures and tapes	Executive Director / Information Technology Consultant	<ul style="list-style-type: none"> ○ Establish physical access controls to server room. ○ Implement security software updates and patches timely. ○ Subscribe to alert services that report external threats. ○ Ensure all servers are up to date with the appropriate application version and security patches. ○ Scan servers for configuration issues and implement fixes. ○ Routinely change default passwords and adjust security parameters. ○ Establish formal data backup processes and conduct periodic tests.
IT systems access	Executive Director / Information Technology Consultant	<ul style="list-style-type: none"> ○ Level of access is based on the employee's job functions. ○ Monitor user accounts and inactivate if unused after 30 days. ○ Shut down accounts within 24 hours of an employee termination or illegal activities are detected. ○ Monitor software licenses for inactive or pirated copies. ○ Conduct surveillance of internet activities and e-mail usage. ○ Perform random reviews of documents and software contained on agency-issued laptops and PDAs.
Licensing applications and all their inclusions	Executive Director / Compliance Manager / Office Manager / Office Assistant	<ul style="list-style-type: none"> • Locked cabinet or drawer when not in use • In password protected computer systems
Network and system configurations	Executive Director / Information Technology Consultant	<ul style="list-style-type: none"> ○ Document all system and network configurations. ○ Establish and follow a formal configuration/change control process that includes vulnerability identification and patching. ○ Document the responsibilities and show a separation of duties between the system administrator and the security administrator.
Passwords	All Board Staff	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...),

		<p>special characters (*, &, \$, etc.) and be at least 8 characters long.</p> <ul style="list-style-type: none"> ○ They may not be dictionary words or a sequence of characters from the keyboard (e.g. qwerty). ○ Passwords may not be reused within two years.
Payroll records	Executive Director / Office Manager	Locked cabinet or drawer when not in use
Personally identifiable information: SSN, home address, etc. of licensees	Executive Director / Office Manager	The information owner must authorize disclosure, transmission or dissemination of this information.
Personnel files and other related human resource information	Executive Director / Compliance Manager / Office Manager	Locked cabinet or drawer when not in use
Police reports and court records	Executive Director / Compliance Manager	Locked cabinet or drawer when not in use
Proprietary business information	Executive Director	Locked cabinet or drawer when not in use
Regulated information covered under the Health Information Portability Act - generally all medical records	Executive Director	Locked cabinet or drawer when not in use
Storage devices such as servers, desktop PCs, laptops, and portable devices.	Executive Director / Information Technology Consultant	<ul style="list-style-type: none"> ○ Always under at least one locked control – servers, laptops and PDA’s in a room protected by a coded locking system. ○ Desktop PCs are in a locked office after hours. ○ Maintain a logging procedure that identifies who has the equipment and what information is on it. ○ Ensure environmental protections are adequate- AC, fire detection, uninterrupted power supplies, etc. ○ Disable unused ports. ○ Know what processes are running and validate new processes against change management processes. ○ Ensure appropriate wireless encryption protocol is enabled prior to the devices being connected to enterprise systems. ○ Install and configure anti-spy software and ensure automatic updates are processed. ○ Routinely check for unauthorized external access capability. ○ Perform frequent scans to detect and

		remove viruses, worms and Trojans.
USB drives containing case information	Executive Director / Board and Committee Members	Locked cabinet or drawer when not in use. When removed from the office, the drives must be both physically and technically protected. The protections would include: <ul style="list-style-type: none"> • Permission from the information owner; • What information is on the drives; • Who is in possession of the drives; • If mailed, signature tracking is required; and • The users have been trained on protecting the drives 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
Investigation and / or inspection documents that are extremely sensitive and could lead to dangerous physical situations (i.e. threats of violence) to staff or others. These are exceptions to those normally found at Level 3.	Executive Director / Compliance Manager / Investigator(s) / Office Manager	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
Mortuary and Cemetery Board
PROCEDURES**

TITLE/SUBJECT: Information Asset Training and Monitoring Procedures
NUMBER: ISP-B
APPLICATION: All Board employees and Board members, temporaries, volunteers and contractors
EFFECTIVE DATE: July 2010

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 that they understand them. The signed document will reside in their personnel or contractor file.
- 3) At time of policy presentation, each person shall take a training class, in person or as an online 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. 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 class again as a refresher.
- 5) The Executive Director 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 Board'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 Mortuary and Cemetery Board
PROCEDURES

TITLE/SUBJECT:	Information Asset Security Incident Procedure
NUMBER:	ISP-C
REFERENCE:	Information Security Plan and Policy
APPLICATION:	All Board staff and Board members, temporaries, volunteers and contractors
EFFECTIVE DATE:	July 2010

PURPOSE: The Board information assets are critical to agency operations. All people who work for or transact business with the Board 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:

- What employees will do to help protect and secure Board 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 is difficult to decipher. A password that is not found in the dictionary and has a combination or numbers, letters and other characters is hard to crack;
- Guard your password carefully. Do not share it with anyone else or post it in a visible area that others can easily see;
- Make sure your data files are stored on the network server and not on your hard drive;
- Take precautions when sending sensitive or proprietary information via e-mail, shuttle and regular mail using the information classification system as a guideline;
- 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;
- Make sure discarded confidential documents are placed face down in shred barrels;
- Lock, log off or shut down your computer prior to leaving for the day;
- Never post confidential or personal information on Web pages; and
- Be aware of unfamiliar people in your work area.

It is the objective of the Board to safeguard all sensitive information. In the event the safeguards fail, the Board will report information security incidents as follows:

- The employee immediately notifies the Executive Director or IT Consultant of the incident;
- The Executive Director is the designated point of contact for the Statewide Incident Response Team. S/he will notify them and inform the rest of the OBNE employees what actions are being taken;
- The Executive Director is the designated point of contact for the Department of Administrative Services, Director's Office. S/he will notify DAS based on the seriousness of the situation and will keep the rest of the Board employees updated.



**Oregon
Mortuary and Cemetery Board
PROCEDURES**

TITLE/SUBJECT: Information Asset Disposal Procedures
NUMBER: ISP-D
REFERENCE: Information Security Plan and Policy Statewide Policy 107-009-0050
APPLICATION: All Board employees and Board members, temporaries, volunteers, contractors
EFFECTIVE DATE: July 2010

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 Statewide 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 disks, tapes, CD's, and USB drives before being reused or disposed of by the Board.

