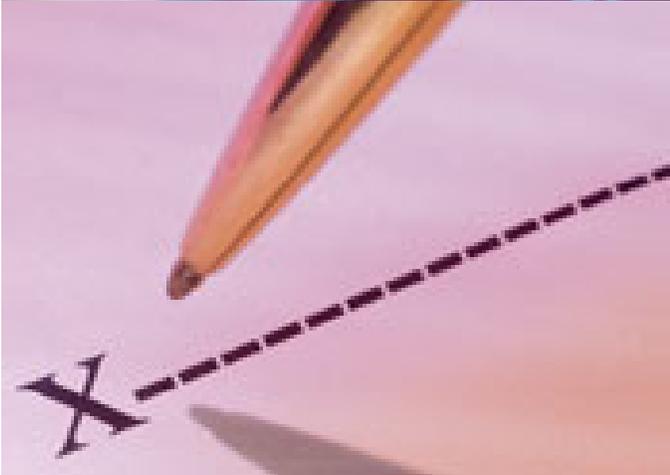


INFORMATION SECURITY PLAN



Information Security Plan for the State of Oregon

September 2009

Enterprise Security Office

(503) 378-6557
security.office@state.or.us
<http://oregon.gov/das/EISPD/ESO>

DAS
DEPARTMENT OF
ADMINISTRATIVE
SERVICES
ENTERPRISE INFORMATION
STRATEGY AND POLICY DIVISION

TABLE of CONTENTS

I.	Executive Summary	3
II.	Roles and Responsibilities	7
III.	Security Management Framework ISO 27001 (SMF).....	9
	SMF 1.0 ISO 27001 Overview	9
IV.	Security Governance and Compliance ISO 27002 (SGC).....	13
	SGC 1.0 Security Organization ISO 27002 Domain Overview	13
	SGC 1.0 Security Organization ISO 27002 Domain Deliverables:	14
	SGC 2.0 Security Policy ISO 27002 Domain	14
	SGC 2.0 Security Policy ISO 27002 Deliverables:	15
	SGC 3.0 Compliance ISO 27002 Domain Overview	15
	SGC 3.0 Compliance ISO 27002 Domain Deliverables:	16
V.	Security Infrastructure and Environment ISO 27002 (SIE).....	16
	SIE 4.0 Human Resources ISO 27002 Domain Overview	16
	SIE 4.0 Human Resources ISO 27002 Deliverables:	16
	SIE 5.0 Asset Management ISO 27002 Domain Overview	17
	SIE 5.0 Asset Management ISO 27002 Domain Deliverables:	17
	ESO Information asset handling procedures documented in the Enterprise.....	17
	SIE 6.0 Physical and Environmental Security ISO 27002 Domain Overview	18
	SIE 6.0 Physical and Environmental Security ISO 27002 Domain Deliverables:	18
VI.	Tactical Security Operations (TSO).....	18
	TSO 7.0 Access Control ISO 27002 Domain Overview	18
	TSO 7.0 Access Control ISO 27002 Domain Deliverables:	19
	TSO 8.0 Incident Management ISO 27002 Domain Overview	19
	TSO 8.0 Information Security Incident Management (ISO 27002) Deliverables:	19
	TSO 9.0 Communications and Operations Management ISO 27002 Domain Overview	19
	TSO 9.0 Communications and Operations Management ISO 27002 Domain Deliverables:	20
	TSO 10.0 Business Continuity Management ISO 27002 Domain Overview	21
	TSO 10.0 Business Continuity Management ISO 27002 Domain Deliverables:	21
	TSO 11.0 Information System Acquisition, Development and Maintenance ISO 27002 Domain Overview	21
	TSO11.0 Information System Acquisition, Development and Maintenance ISO 27002 Deliverables:	23
VII.	Implementation of Plan (IP).....	24
	Implementation Overview	24
	Implementation Deliverables: to be developed upon approval of plan:	24
VIII.	Approval	24
IX.	Appendix A: Applicable Statutes and Policies	25
X.	Appendix B: Terms and Definitions	26
XI.	Appendix C – Roles and Responsibilities.....	27
XII.	Appendix D – Statewide Policies Summary	31

I. Executive Summary

The Department of Administrative Services (DAS) has the responsibility for and authority over state agency information systems and the information stored on those systems under the authority of Oregon Revised Statute (ORS) 182.122¹(Statute). DAS is fulfilling its authority by adopting a comprehensive approach to information security based on the International Organization for Standardization (ISO) 27001, which covers the framework for establishing security management and 27002:2005 addressing technical standards. This resulting State Information Security Plan is the foundation for information security in the State of Oregon Executive Branch agencies.

In this State Information Security Plan, DAS has defined policies, standards, and processes for state agencies with respect to information security. Fundamental components of information security are addressed including roles and responsibilities. Executive department agencies are required to meet or exceed this State Information Security Plan. Agencies also may develop and adopt information security plans that are more stringent than the minimum requirements identified in this State Information Security Plan.

Information is an asset that, like other important business assets, is essential to an organization's business and consequently needs to be suitably protected. Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or by using electronic means, shown on film, or spoken in conversation. In whatever form the information takes, or means by which it is shared or stored, it should always be appropriately secured.

Information systems is defined in Statute and “means computers, hardware, software, storage media, networks, operational procedures and processes used in the collection, processing, storage, sharing or distribution of information within, or with any access beyond ordinary public access to, the state's shared computing and network infrastructure.”

In order to fully implement this plan, each agency must determine what information assets they are responsible for and on which information systems those assets are stored. The agency must identify the risks posed to these information systems, and mitigate them by following the Enterprise Information Security Standards.

To secure information systems security agencies must follow these steps:

- 1) Identification of all information assets and assessing the risk associated with the information asset as required by statewide Information Security policy # 107-004-052.
- 2) Proper classification and labeling of all information provided as required by statewide Information Asset Classification policy # 107-004-050.
- 3) Conduct an annual risk assessment in accordance with OAR 125-700-0010 and in accordance with ISO 27001.

¹ Oregon Revised Statute 182.122 – Information systems security in executive department; rules, <http://www.leg.state.or.us/ors/182.html>

- 4) And, as required by Statute, apply the Enterprise Information Security Standards to mitigate risks. The standards as established set a consistent implementation of security infrastructure and a uniform mechanism for information handling. The standards identify minimum criteria and techniques associated with protecting and securely providing access to the State's information resources. Agencies may elect to exceed the minimum-security standards to meet security requirements of their organization.

The Enterprise Information Security Standards is an appendix to this State Information Security Plan and the standards within it have been compiled using industry resources including the International Organization for Standardization (ISO) 27001 and 27002:2005, National Institute of Standards and Technology (NIST) recommended standards, SANS Institute recommended standards, and Burton Group recommended best practices.

The Enterprise Information Security Standards document provides detailed technical controls, standards, processes and best practices to the following ISO 27002 domains

- a) Access Control
- b) Information Systems Acquisition, Development, and Maintenance
- c) Incident Management
- d) Communications and Operations Management

Information security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities. 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, implemented, monitored, reviewed and improved on an ongoing basis, to ensure security and business objectives of the organization are met. This should be done in conjunction with other business management processes.

Information systems security as defined in statute² represents only a subset of information security as a whole. This State Information Security Plan addresses a comprehensive approach to information security based on the International Organization for Standardization (ISO) 27001 and 27002:2005 standards. The ISO/IEC 27002:2005 *Information technology – Security techniques – Code of practice for information security management*, ISO/IEC 27002:2005 is the standard used by the Enterprise Security Office for structuring this plan. It consists of eleven domains which the ESO has divided into three topic areas. This plan covers all eleven domains.

² ORS 182.122



Figure 1

The relationship between this State Information Security Plan and corresponding agency information security plans, the initiatives identified in the Enterprise Information Security Strategic Plan, Enterprise Information Security Standards, and the ISO 27001 and 27002 domains comprises the Enterprise Security Architecture as illustrated below in Figure #2:

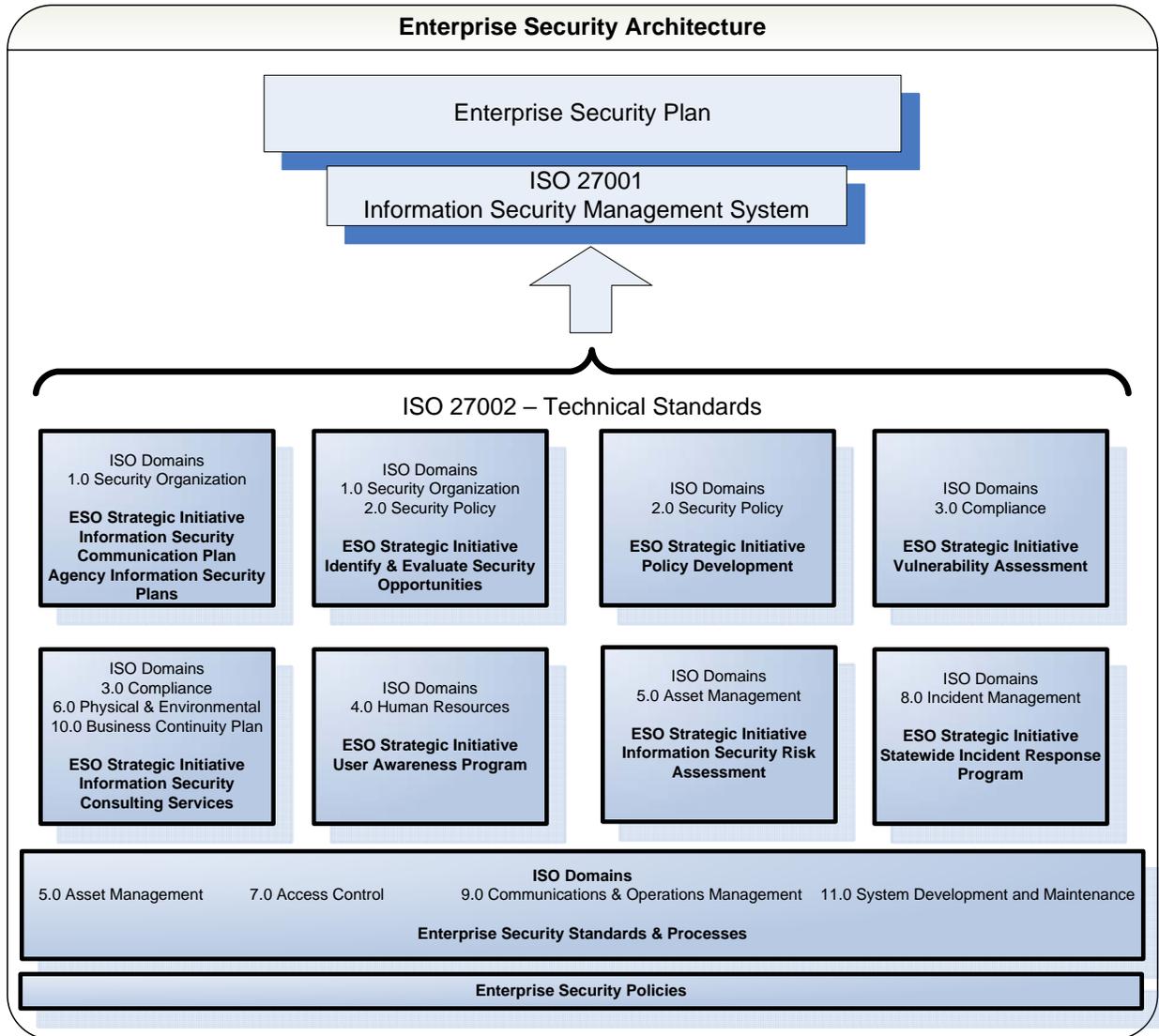


Figure 2

II. Roles and Responsibilities

The roles and responsibilities below are compiled from existing statewide policy, statute and rule. See Appendix A for a matrix of statewide program and agency responsibilities as mandated in Statute and related Oregon Administrative Rules.

DAS Director	Has the authority and responsibility for information systems security under Statute. That authority is carried out through subordinate staff.
DAS	Takes necessary actions to protect the availability, integrity, or confidentiality of state's information systems or the information stored in information systems. In collaboration with state agencies, directs information security planning. In collaboration with state agencies, develops, recommends, implements and maintains administrative rules, policies, architecture, standards, guidelines, processes, and best practices related to information security. Working collaboratively with state agencies, conducts information security assessments and testing. Creates and maintains a state incident response capability. Provides communications practices and tools to form and maintain an information security community of practice. Identifies tracks, analyzes, adjusts, and reports information security performance measurement and management to the Legislature and state executive management.
Enterprise Security Office (ESO)	As designated by DAS, leads statewide information security planning and policy development. Conducts security risk and compliance assessments using staff or third party contractors. Responsible to develop, coordinate and maintain the State Incident Response capability. Maintains a forensic analysis capability ³ . Develops information security awareness and training tools. Tracks information security issues and analyzes trends. Identifies and measures information security performance measures. Conducts training, convenes workgroups, conducts workshops, and leads forums to facilitate agency information security activities. ⁴
State Data Center (SDC)	Responsible for information system security for the state shared computing and network infrastructure. Conducts self-assessments or third party assessments of systems under its control. Monitors state network traffic. Advises agencies and the ESO of issues identified through monitoring. Mitigates threats and works with agencies and the ESO to address vulnerabilities. Develops and maintains architecture for state operated data center and state network. SDC develops data center and state network security

³ ORS 182.122

⁴ OAR 125-800-0020

Agencies

standards. Participates on the State Incident Response Team as needed.⁵

Responsible to protect all information assets in accordance with statewide information security plan, standards and policies⁶.

Responsible for information system security for agency-owned computing and network infrastructure⁷. Develops and maintains information security plans, policies, and procedures based on enterprise direction⁸. Conducts self-assessments or third party assessments of information security risks within its organization including information and data systems under its control. Conducts compliance reviews through self-assessment or through use of third party contractors. Reports incidents to the ESO as required by policy⁹. Provides assessment and audit results to the ESO.

Implements remedial action in response to identified vulnerabilities. Agencies are responsible for compliance with DAS information security policies, architecture, and standards and any applicable state and federal information security regulations (e.g. HIPAA, IRS, PCI DSS, etc).

⁵ ORS 182.122

⁶ Information Asset Classification Policy #107-004-050

⁷ Acceptable Use of State Information Assets Policy #107-004-110

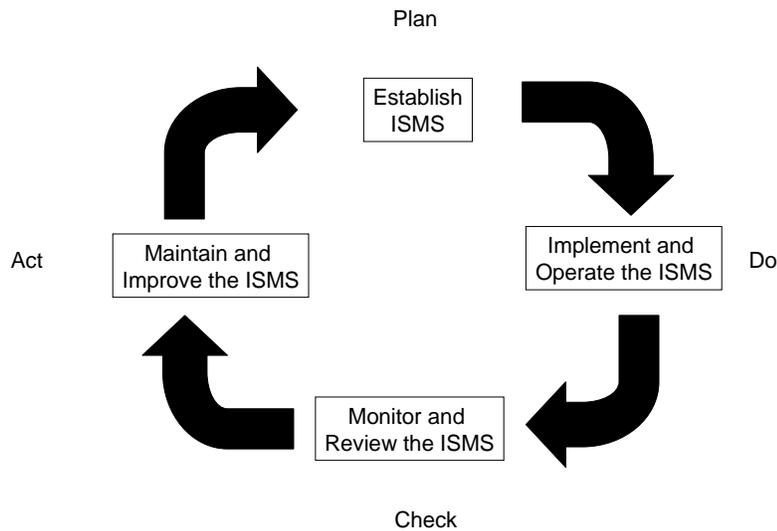
⁸ Information Security Policy #107-004-052

⁹ Information Security Incident Response Policy #107-004-120

III. Security Management Framework ISO 27001 (SMF)

SRA 1.0 ISO 27001 Overview

ISO 27001 specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving a documented Information Security Management System (ISMS). An ISMS ensures the selection of adequate and appropriate security controls to protect information assets. The foundation for determining what controls are appropriate is a comprehensive security risk assessment conducted as required based on changes within the organization.



Agencies shall establish and define the scope of their ISMS. Agencies will ensure their Information Security Policy includes the following:

- 1) Objectives, direction and principles regarding information security
- 2) Includes business, legal, or regulatory requirements applicable to the agency, and contractual security obligations
- 3) Aligns with the agency's strategic risk management policy and direction
- 4) Establishes criteria for evaluating risk

These elements are fundamental elements of an agency's Information Security Plan. Agencies are required to submit their Information Security Plan for review and approval to the Enterprise Security Office. As part of the ISMS agencies will periodically review and update their Information Security Plan.

Agencies shall define their risk assessment approach which includes:

1. A methodology
2. Identification of the acceptable levels of risk
3. Criteria for accepting risk

The State Data Center (SDC) will develop an ISMS, including policies and procedures, in consultation with agency customers to ensure agency assets located at the SDC, as well as the state network, are appropriately assessed, monitored and protected.

Agency management must demonstrate its commitment to an ISMS through:

- establishing an ISMS objectives, plan, and policy
- establishing roles and responsibilities for information security
- communicating the importance of complying with information security policy and objectives
- practicing continuous improvement
- providing sufficient resources
- conducting security risk assessments
- deciding the criteria for accepting risks and the acceptable levels of risk
- conducting internal reviews/audits of ISMS to ensure it is effectively implemented and maintained
- conducting management reviews of ISMS on a regular basis; at least annually
- taking preventative actions based on reviews, audits, assessments, and significantly changed risks/threats
- updating and improving the ISMS as required

Security Risk Assessment:

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

It is recognized no set of controls will achieve complete security and the cost of added information security controls must be commensurate with the sensitivity or value of the information being protected. It is also recognized that each Agency Director is responsible for accepting or transferring risk in accordance with the business and security requirements of the agency. Any deviation needs to be documented, approved by Agency Director and kept on file at the agency.

Each agency is required in to conduct an annual risk assessment. This risk assessment must include information systems security and consider the following elements based on International Organization for Standardization ISO 27001:

- 1) Identify the risks¹⁰
 - a) Identify assets and the associated information owners
 - b) Identify the threats to those assets

¹⁰ Information Security Policy #107-004-052

- 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 risks¹¹
- a) Assess the business impacts 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 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 risk¹²
- 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 risks¹³

After identifying the risks agencies must apply the appropriate controls to their information and information systems security. Controls, standards, and procedures for protecting information and information systems based on the ISO 27001 (Annex A – Control Objectives and Controls) and ISO 27002 standards are identified and described in the rest of this plan and in the Enterprise Information Security Standards document.

¹¹ Ibid

¹² Ibid

¹³ Ibid

Measurement & Monitoring:

Agencies must measure the effectiveness of the controls and implement a training and awareness program. Controls and procedures must be monitored and reviewed on an ongoing basis to detect errors, identify attempted and successful security breaches/incidents, and determine whether the actions taken to resolve a breach were effective.

Documentation:

It is important to document management decisions, ensure that actions are traceable to management decisions and policies, and that the recorded results are reproducible¹⁴. These documents must be protected, controlled, updated, stored, and disposed of in accordance with written policies/procedures¹⁵.

Resources:

DAS, through the ESO, contributes to the process of identifying risks and vulnerabilities through two different programs:

- 1) The ESO engages a third party contractor to conduct annual Information Security Business Risk Assessment (ISBRA) to evaluate selected agency's controls and maturity across the eleven ISO 27002 domains. The ESO in conjunction with the third party contractor then provides individualized reports to each agency and a summation of all agencies trends in an Enterprise level report. ESO will continue this process and as resources and tools become available add additional agencies each year.
- 2) Information system vulnerability assessments conducted in accordance with the criteria outlined in the Enterprise Vulnerability Assessment Plan.

SMF 1.0 ISO 27001 Deliverables:

Deliverable #	Title	Owner	Compliance date/frequency
SMF 1.1	Agency Annual Risk Assessment- per OAR125-700-0010	Agency	TBD
SMF 1.2	Agency Information Systems Security Risk Assessments per Statute	Agency	TBD
SMF 1.3	Agency Information Security Management System, (ISMS)Framework	Agency	TBD
SMF 1.4	Enterprise Information Security Business Risk Assessment (ISBRA)	ESO	Annually

Additional related deliverables appear in section SGC 3.0 of this plan.

¹⁴ ISO 27001 – 4.3.1

¹⁵ ISO 27001 – 4.3.2 and 4.3.3

IV. Security Governance and Compliance ISO 27002 (SGC)

SGC 1.0 Security Organization ISO 27002 Domain Overview

Information security is a business issue. The purpose of an information security program 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 a venue to inform and advise executive, business and information technology management on security issues and acceptable risk levels.

Agencies must define and document an information security governance structure tailored to the individual agencies business needs. At a minimum, each agency must identify an information security point-of-contact and should identify a representative to the Information Security Council.

At the statewide level, policy development and statewide information security initiatives are developed collaboratively with agencies. While responsibility for statewide information security has been assigned to DAS by statute and rule, several governance bodies exist to provide advice, guidance, and subject matter expertise in the identification, development, and management of governing policies, guidelines, tools, and initiatives. These governance groups are:

Enterprise Information Security Advisory Board – The Enterprise Information Security Advisory Board (EISAB) is chartered to provide recommendations to the DAS Director and to support enterprise-wide information security through collaborative efforts to ensure the confidentiality, integrity and availability of the state’s information assets. This effort includes the protection and enhancement to the security of state information assets. It is the role of the EISAB, as the embodiment of leaders in state government, to evaluate the feasibility of enterprise information security initiatives and strategies, and make informed recommendations to the DAS Director and agency peers.¹⁶

Information Security Council – The Information Security Council (ISC) is chartered to support information security through collaborative efforts to ensure the confidentiality, integrity and availability of the state’s information assets. The ISC is the avenue for agencies to participate and assist in the development of strong enterprise security and to provide input for security initiatives to meet agency business needs. These efforts include, but are not limited to, identification and development of enterprise strategies, policies and initiatives that protect and enhance the security of state information assets. It is the role of the ISC, as the embodiment of information security subject matter expertise in state government, to validate the feasibility of enterprise information security initiatives and strategies and make informed, clearly defined and prioritized recommendations to the ESO.¹⁷

¹⁶ Enterprise Security Advisory Board Charter, approved 4/13/2007.

¹⁷ Enterprise Information Security Council Charter, adopted 9/11/2008.

Chief Information Officer Council – The Chief Information Officer Council (CIO Council) is comprised of state and local government chief information officers and information technology leaders. The CIO Council provides a forum for all agencies to collaborate in the management of information resources across state government. The CIO Council advises the State Chief Information Officer and state business leaders on strategic information resource management (IRM) planning, statewide IRM policies, statewide technical architecture and standards, and planning implementation of statewide information technology initiatives.¹⁸

Agency Heads – The heads of executive branch agencies convene bi-monthly to review information about statewide initiatives and align agency strategies.

Small Agency Heads - The heads of small executive branch agencies convene quarterly to review information about statewide initiatives and align agency strategies.

Administrative Business Services Directors – The DAS Director’s Office has chartered this group to provide leadership and feedback on enterprise business management opportunities to:

- 1) Provide better efficiency and customer service to state government
- 2) Share information
- 3) Identify and provide training and development opportunities
- 4) Review, discuss and develop work products around the state’s business services

Department of Justice – Representatives from the Department of Justice review enterprise policies and other documents for legal sufficiency.

DAS Executive Staff – The DAS Executive Staff consists of division directors and Director’s Office staff. This group sets the mission, vision, strategies and goals for the department. The department implements policy and financial decisions made by the governor and the Legislature, and sets and monitors standards of accountability. DAS supports state agencies by providing strong and stable management infrastructure.¹⁹

SGC 1.0 Security Organization ISO 27002 Domain Deliverables:

Deliverable #	Title	Owner	Compliance date/frequency
SGC 1.1	EIS Advisory Board Charter	EISAB	Updated as needed.
SGC 1.2	Information Security Council Charter	Agency	Updated as needed.

SGC 2.0 Security Policy ISO 27002 Domain

The development of a Security Policy affirms the direction and support required for information security within an agency. The security policy reinforces management’s fundamental belief of how staff will conduct business with their constituents. The security policy will be in accordance

¹⁸ Chief Information Officer Council overview, http://oregon.gov/DAS/EISPD/cioc_index.shtml#Overview.

¹⁹ “DAS Pocket Facts,” http://oregon.gov/DAS/docs/pocket_facts.pdf.

with each agency’s business requirements and will consider all relevant laws and regulations. The governance groups listed in section SGC 1.0 Security Organization play key roles in statewide information security policy development and approval. The process of developing a statewide information security policy is a collaborative process but authority for final approval and adoption of each policy belongs to the DAS Director.

SGC 2.0 Security Policy ISO 27002 Deliverables:

Deliverable #	Title	Owner	Compliance date/frequency
SGC 2.1	Enterprise information security policy and review process link to Policy Approval Process	DAS	Updated as needed.
SGC 2.2	Enterprise Information Security Policy Architecture	ESO	Updated as needed.
SGC 2.3	Internal Agency Security Policies & Governance Processes	Agency	

SGC 3.0 Compliance ISO 27002 Domain Overview

To avoid any breaches of law, statutory, regulatory or contractual obligations, and of any security requirements²⁰ it is necessary to monitor and maintain compliance with statutory and regulatory requirements.

The design, operation, use, and management of information and information assets are subject to statutory, regulatory, and contractual security requirements. Legal requirements include, but are not limited to: state or federal statute, statewide and agency policy, regulations, contractual agreements, intellectual property rights, copyrights, and protection and privacy of personal information.

Agencies must identify the legal, statutory, contractual and policy requirements with which their information security controls must comply. Agencies must comply with the requirements and controls identified in this State Information Security Plan and the associated Enterprise Information Security Standards. ESO will survey agencies on their progress for implementing requirements of the State Information Security Plan and develop a scorecard to monitor implementation progress.

DAS, through the ESO, will conduct vulnerability assessments at the enterprise and agency level. Any agency may be the subject of a DAS conducted assessment.

Agencies shall conduct audits/assessments of information security including implementation of information security policies, plans, processes, procedures, and systems. Agencies shall document the results in their annual audit plans.

Agencies may elect to hire a third party to conduct information security audits and assessments using statewide contracts per Statute.

²⁰ ISO 27002:2005 Compliance with legal requirements. p. 100

As per Statute, agencies are responsible for sharing the results of information security audits and risk assessments with the ESO. The ESO collects the results of information security audits and risk assessments for the purpose of aggregating the results and identifying common themes or areas for improvement across multiple agencies. This process including reporting procedures, exclusions, and the level of information required to be reported is documented in the Enterprise Information Security Vulnerability Assessment plan.

SGC 3.0 Compliance ISO 27002 Domain Deliverables:

Deliverable #	Title	Owner	Compliance date/frequency
SGC 3.1	Information Security Audits within Agency	Agency	TBD
SGC 3.2	Enterprise Information Security Vulnerability Report	ESO	TBD
SGC 3.3	Enterprise Vulnerability Assessment Plan	ESO	Annual review
SGC 3.4	Vulnerability Assessments	ESO	6 per biennium

V. Security Infrastructure and Environment ISO 27002 (SIE)

SIE 4.0 Human Resources ISO 27002 Domain Overview

To ensure employees, contractors, and all users, including business partners, understand their security responsibilities and are suitable for the roles they are considered for, human resources security must be a part of each agency’s hiring and review process. As identified in the Employee Security policy #107-004-053, agencies must protect information assets and reduce the risk of human error and misuse of enterprise information and equipment. Agencies must also provide information security awareness training for all staff that have access to the agency’s information assets.

DAS, through the ESO, makes available to all state agencies generic information security training materials²¹. These materials include security awareness training modules and supporting materials such as brochures, whitepapers, and posters. At a minimum, the generic information security materials cover topics included in statewide policies, areas required by statute or rule, or information covered in recognized best practices such as the National Institute of Standards and Technology (NIST) 800-16 “Security Basics and Literacy” standard for federal employees.

SIE 4.0 Human Resources ISO 27002 Deliverables:

Deliverable #	Title	Owner	Compliance date/frequency
SIE 4.1	Statewide Employee Security Policy	ESO	Annual review
SIE 4.2	Agency Employee Security	Agency	TBD

²¹ OAR 125-800-020 Information Security

	Policies		
SIE 4.3	Process for Access Control to Information Assets within Agency	Agency	TBD
SIE 4.4	Generic Information Security Training Materials	ESO	As needed by Agencies
SIE 4.5	Agency Information Security Awareness Training	Agency	TBD

SIE 5.0 Asset Management ISO 27002 Domain Overview

As defined in the Statewide Information Asset Classification Policy²², information is any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics. The Oregon State Legislature has identified information as “a strategic asset of the state which must be managed as a valuable state resource²³.”

DAS is responsible for developing and implementing statewide policy for asset classification and establishing standards to protect information assets.

DAS owns many enterprise-level information assets and is responsible for identifying specific positions as the designated information owner for these assets through its information asset classification policy and plan. These DAS information assets include, but are not limited to: human resource/personnel information, statewide financial information, information related to state owned and leased facilities, statewide procurement information, and information associated with the state shared computing and network infrastructure. These information assets will be classified in accordance with the DAS Information Asset Classification Policy 107-004-050. Information asset classification levels and required handling procedures will be communicated to agencies by December 31, 2009 for all Level 4 “Critical” information and by June 30, 2010 for information Levels 1-3.

SIE 5.0 Asset Management ISO 27002 Domain Deliverables:

Deliverable #	Title	Owner	Compliance date/frequency
SIE 5.1	DAS classification of enterprise level information assets	DAS Division Level Authority	TBD
SIE 5.2	Agency classification of agency information assets and assignment of information owners per Information Asset Classification Policy # 107-004-050	Agency	TBD
SIE 5.3	ESO Information asset handling standards documented in the Enterprise Information Security Standards	ESO	TBD
SIE 5.4	Agency compliance with the	Agency	TBD

²² Information Asset Classification Policy #107-004-050

²³ ORS 291-037 Legislative findings on information resources

	Transporting Information Assets Policy #107-005-100		
--	--	--	--

SIE 6.0 Physical and Environmental Security ISO 27002 Domain Overview

Agencies shall provide for physical and environmental controls to all facilities to mitigate unauthorized physical access, damage, theft compromise or interference to their collection, use, storage and disposal of business information. In accordance with the standards identified in this plan and the Information Asset Classification Policy #107-004-050, information assets must be secured with appropriate security and access controls, and protected from unauthorized access, damage and interference consistent with the classification level assigned to the asset.

Agencies must carefully evaluate facilities that house agency information and information technology equipment to identify suitable controls to protect information from environmental threats, physical intrusion and other threats.

Agencies must coordinate with the DAS Facilities division to implement appropriate controls on access to buildings owned or managed by the state through mechanical and electronic locks. Accommodations will be made for high security access areas with escalated access restrictions. Agencies must follow DAS policy guidelines and processes for building security access control.²⁴

SIE 6.0 Physical and Environmental Security ISO 27002 Domain Deliverables:

Deliverable #	Title	Owner	Compliance date/frequency
SIE 6.1	DAS Building Security Access Controls Policy # 125-6-215	DAS/Agencies	
SIE 6.2	Evaluation of Agency facilities for security	Agency	As changes occur to facilities.

VI. Tactical Security Operations (TSO)

TSO 7.0 Access Control ISO 27002 Domain Overview

Access to information, information systems, information processing facilities, and business processes is based on business and security requirements and the need to know.

Per policy #107-004-050: Information Asset Classification, agencies are responsible to control access to information assets by employees. Agencies also are responsible (Employee Security Policy #107-004-053) for educating users on their responsibilities for maintaining effective access controls.

²⁴ Building Security Access Controls policy #125-6-125, effective July 1, 2003, <http://oregon.gov/DAS/FAC/docs/1256215.pdf>.

Access to state resources is not only required by state employees but also by agency business partners and citizens. For agencies to effectively maintain a secure infrastructure agencies must utilize the same minimum access control requirements for agency business partners and citizens utilizing state resources. The Enterprise Information Security Standards attached to this plan provides the minimum required standards for implementing access control at executive branch agencies.

TSO 7.0 Access Control ISO 27002 Domain Deliverables:

Deliverable #	Title	Owner	Compliance date/frequency
TSO 7.1	Enterprise Information Security Standards	ESO	Update as needed
TSO 7.2	Agency compliance with the Access Control standards identified in the Enterprise Information Security Standards	Agency	TBD
TSO 7.3	Agency compliance with policy #107-004-053 and minimum access controls for business partners and citizens in accordance with the policy	Agency	TBD

TSO 8.0 Incident Management ISO 27002 Domain Overview

As per Statute and the Information Security Incident Response policy #107-004-120, information security incidents will be communicated in a manner allowing timely corrective action to be taken. Although Statute only requires reporting of information systems security incidents, the Information Security Incident Response policy covers incidents including information in all its forms.

Information security incident management at the state of Oregon will be implemented by agencies as identified in the Information Security Incident Response Policy #107-004-120.

TSO 8.0 Information Security Incident Management (ISO 27002) Deliverables:

Deliverable #	Title	Owner	Compliance date/frequency
TSO 8.1	Statewide Information Security Incident Response Policy	ESO	June 30, 2009
TSO 8.2	Agency compliance with the Information Security Incident Response policy	Agency	June 30, 2009

TSO 9.0 Communications and Operations Management ISO 27002 Domain Overview

Agencies are responsible for the establishment of responsibilities and procedures to ensure secure operations of information processing facilities.

At the State of Oregon, the majority of information processing occurs in the State Data Center (SDC). However, there are agencies that use small computer rooms, third party data centers or

locally host servers not supported by the SDC. These agencies also have specific responsibilities under this plan and Statute to protect those information systems.

DAS, through the SDC²⁵, maintains responsibility for developing and implementing procedures for the management and operation of the State Data Center and the state’s network infrastructure. The SDC must enforce segregation of duties and periodically review duties to reduce the risk of negligent or deliberate system or information misuse. The SDC is responsible to monitor, prevent and detect the introduction of malicious code, protect the integrity of information systems, and set operational standards. To prevent unauthorized disclosure, modification, removal or destruction of information assets, and interruption to business activities, systems must be controlled and protected in accordance with established policies²⁶ and compliance with the Enterprise Information Security Standards. .

Agencies operating their own independent or satellite data centers or computer rooms must implement and document procedures for monitoring their information systems and Local Area Networks (LANs). Clear procedures for information systems security and management are fundamental to securing information and systems. These procedures must be identified and documented in their agency information security plans. DAS has the authority²⁷ to conduct a vulnerability assessment within any of these facilities and any vulnerability assessment would include review of established procedures. Agencies are required to meet or exceed the standards identified in the Enterprise Information Security Standards.

Agencies that elect to use a third party hosting facility must ensure that their host follows clear procedures for information systems security and management. These procedures must be identified and documented in their agency information security plans. Third party providers must meet or exceed the standards identified in the Enterprise Information Security Standards.

As per Statute, information systems must be monitored and information security events recorded to detect unauthorized access to information and information systems. Agencies are responsible for employing monitoring techniques to comply with applicable statewide policies related to acceptable use for agency-managed networks and systems. DAS through the SDC monitors and records events specific to the State Data Center and the state’s network infrastructure. Agencies with their own data centers or computer rooms must monitor and record events specific to their information systems and LANs.

TSO 9.0 Communications and Operations Management ISO 27002 Domain Deliverables:

Deliverable #	Title	Owner	Compliance date/frequency
TSO 9.1	Enterprise Information Security Standards	ESO	TBD
TSO 9.2	SDC compliance with Enterprise	SDC	TBD

²⁵ ORS 182.122 establishes DAS responsibility for and authority over information systems security in the executive department

²⁶ Transporting Information Assets Policy #107-005-100, Controlling Portable and Removable Storage Devices Policy # 107-004-051.

²⁷ ORS 182.122 establishes DAS responsibility for conducting vulnerability assessments

	Information Security Standards		
TSO 9.3	Agency compliance with Enterprise Information Security Standards	Agency	TBD

TSO 10.0 Business Continuity Management ISO 27002 Domain Overview

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, agencies must plan for business continuity management. At the state, business continuity management is necessary to ensure critical services are quickly restored to the public following any potential service disruption.

The state has adopted the business continuity plan (BCP) as the approach to identifying critical business activities and planning alternative ways to maintain and provide services in the event of a disaster or service disruption. Developing a BCP involves identifying the agency’s critical business functions and then determining the critical processes, information systems, key staff, and essential records connected to those critical functions. A plan is then developed that describes how the critical business functions would be quickly restored using a combination of preventative and recovery controls.

An agency’s BCP must address Disaster Recovery (DR). The recovery of critical information systems identified within the BCP is fundamental to restoring business operations. DR should be tested and closely reviewed for thoroughness and timeliness. If business outcomes are not achieved agency must update and retest DR plan.

TSO 10.0 Business Continuity Management ISO 27002 Domain Deliverables:

Deliverable #	Title	Owner	Compliance date/frequency
TSO 10.1	Agency BCP per policy # 107-001-010	Agency	June 30, 2009
TSO 10.2	Agency BCP testing	Agency	May, 2010
TSO 10.3	Agency DR testing	Agency	May, 2010
TSO 10.4	SDC DR testing	SDC	May, 2010

TSO 11.0 Information System Acquisition, Development and Maintenance ISO 27002 Domain Overview

Security is an integral part of all information systems throughout their life-cycle. The design and implementation of information systems supporting the business process is crucial for security. Security requirements must be identified and incorporated into information systems whether they are off-the-shelf products or custom developed applications. Furthermore, information systems including operating systems, infrastructure, business applications, off-the-shelf applications and custom developed applications must be maintained to prevent the introduction of security issues or vulnerabilities.

DAS is responsible for developing information security policies, standards and architectures to enforce information security standards for the state’s computing network and infrastructure. DAS will lead enterprise-level efforts, and assist agency efforts. The Enterprise Information Security

Standards provides a framework for integrating security requirements into acquisition, development and maintenance of information systems.

DAS has defined several policies to strengthen information systems security and several affect aspects of acquisition, development, maintenance and disposal of information systems. One example, the Transporting Information Assets Policy #107-004-100, states, “encryption or similar levels of security should be employed, where appropriate, to protect information at rest and in transit.” System files and program source code are examples of information assets that require such protection.

Agencies are responsible for the security of their systems, applications, and information. Agencies must implement procedures ensuring system development and procurement processes include steps to enforce information security standards in the acquisition, development, maintenance and decommission of agency-owned systems.

Acquisition and Development

Agencies involved in the purchase of applications or the custom development or adaption of applications to support their business processes must implement procedures ensuring system development includes steps to identify and incorporate security requirements into applications. Agencies will identify a system owner(s) who has responsibility for the overall system. The system owner will be a business representative and represent the business needs of the system.

Agencies must follow specific standards for applications, regardless of whether they are purchased or custom developed are identified in the Enterprise Information Security Standards section on Information Systems Acquisition, Development and Maintenance: System Development Lifecycle. Agencies are required to seek approval from the State CIO in advance of purchase, and/or report on information technology investments in accordance with the procedures described in the Information Technology Investment Review/Approval interim policy (http://www.das.state.or.us/DAS/EISPD/ITIP/docs/ITIRPOLICYv11_Final_040104.doc) Agencies are required to comply with the management procedures and a quality assurance framework for the development, review, improvement, integration, security, and use of information resources as defined in statewide policy #107-004-030 Technology Investment Strategy Development And Quality Assurance Reviews.

Maintenance of Information Systems

Information systems require ongoing maintenance to remain both operational and secure. Hardware can require firmware updates while software requires routine patching for security vulnerabilities and upgrades. Agencies must maintain the hardware and software for which they are responsible. Vendor supplied software used in operational systems should be maintained at a level supported by the supplier.

Agencies must follow specific standards for maintenance and support of information systems as identified in the Enterprise Information Security Standards. Elements include:

- Workstation and Desktop Management
- Patch Management
- Information Systems Development Lifecycle

Disposal of Information and Information Systems

Agencies must ensure complete removal and absolute destruction of all data, information, operating system software, firmware or non-writeable read-only media, and formatting in compliance with approved sanitization methods provided for in Department of Defense (DOD) Directive DOD 522022-M in accordance with Sustainable Acquisition and Disposal of Electronic Equipment (E-waste/Recovery Policy 107-009-0050)

Agencies that dispose of equipment through the DAS Surplus Property program will receive documentation that all sensitive, proprietary and licensed data is irretrievably removed from storage devices and that all hard drives are reformatted to DOD standards.

Agencies may return e-waste to a manufacturer or vendor with a current state price agreement that contains Buy-Back or Take Back provisions in accordance with Sustainable Acquisition and Disposal of Electronic Equipment (E-waste/Recovery Policy 107-009-0050).

Physical Security in the Disposal of Information and Information Systems

DAS issues policies and guidelines for the proper disposal of electronic equipment. In support of the Governor's Executive Order 06-02²⁸ on sustainability, DAS has adopted²⁹ the Electronic Products and Acquisition Technology (EPEAT) standards for the acquisition and disposal of electronic equipment. Statewide policy requires complete removal and absolute destruction of all data, information, operating system software, firmware or non-writeable read-only media, and formatting in compliance with approved sanitization methods provided for in Department of Defense Directive DOD 522022-M. The DAS Surplus Property disposal program provides documentation that sensitive, proprietary and licensed data is irretrievably removed from storage devices and that all hard drives are reformatted to DDS standards for agencies that utilize this service.

TSO 11.0 Information System Acquisition, Development and Maintenance ISO 27002 Deliverables:

Deliverable #	Title	Owner	Compliance date/frequency
TSO11.1	Statewide Information Security Policies	ESO	TBD
TSO11.2	Enterprise Information Security Standards	ESO	Update as needed
TSO11.3	Agency compliance with Enterprise Information Security Standards	Agency	TBD
TSO11.4	Review of IRR compliance with Enterprise Information Security Standards	DAS EISPD	As needed
TSO11.5	Agency compliance with Sustainable Acquisition and Disposal of Electronic Equipment (E-waste/Recovery Policy)	DAS/Agencies	TBD

²⁸ Executive Order 06-02, "Sustainability for the 21st Century, <http://governor.oregon.gov/Gov/pdf/eo0602.pdf>

²⁹ Statewide Sustainable Acquisition and Disposal of Electronic Equipment (E-Waste/Recovery Policy) #107-009-0050, effective January 1, 2007, <http://oregon.gov/DAS/OP/docs/policy/state/107-009-0050.pdf>

VII. Implementation of Plan (IP)

Implementation Overview

All plans must be implemented if success is to be achieved. These are the steps that the ESO will put into place to ensure that the Information Security Plan will be successfully implemented and maintained.

1. EISAB review and recommends approval of the Information Security Plan.
2. Communication to Agencies regarding their participation requirements.
3. Map to existing ESO Initiatives for identification of metrics and deliverables to be tracked and reported
4. Enterprise Information Security Plan Implementation Schedule to be developed upon acceptance
5. Monitor, update, and track progress per schedule.

As with every plan there are exceptions regarding who will and will not be considered as a stakeholder or impacted by the implemented solutions. With this in mind DAS ESO directs agencies to the policy titled "Exceptions to Policies" #107-001-0020. ESO cannot grant any exceptions to policy, ORS or OAR that agencies must be in compliance with.

Implementation Deliverables: to be developed upon approval of plan:

Deliverable #	Title	Owner	Compliance date/frequency
IP 1.1	EISAB recommends approval of the Information Security Plan	ESO	September 28, 2009
IP 1.2	Communications Plan	ESO	November 2009
IP 1.3	Implementation Schedule	ESO	December 2009
IP 1.4	Implementation Metrics	ESO/Agencies	May, 2010
IP 1.5	Implementation Reporting	ESO	June 2010

VIII. Approval

By: _____
Scott Harra, Director, DAS

Date

By: _____
Dugan Petty, State Chief Information Officer, DAS

Date

By: _____
Theresa Masse, State Chief Information Security Officer, DAS

Date

IX. Appendix A: Applicable Statutes and Policies

Governing statewide statutes and rules:

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

State information security policies:

Policy Number	Policy Title	Effective Date
107-001-010	Statewide Business Continuity Planning	3/17/2006
107-004-050	Information Asset Classification	1/31/2008
107-004-051	Controlling Portable and Removable Storage Devices	7/30/2007
107-004-052	Information Security	7/30/2007
107-004-053	Employee Security	7/30/2007
107-004-100	Transporting Information Assets	1/31/2008
107-004-110	Acceptable Use of State Information Assets	10/16/2007

107-004-120	Information Security Incident Response	11/10/2008
-------------	--	------------

X. Appendix B: Terms and Definitions

The terms and definitions in this plan are derived from the statewide information security policies.

asset	anything that has value to the agency ³⁰
business continuity	ability of an organization to ensure continuity of service and support for its customers and to maintain its viability before, after, and during an event
control	means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal nature
disaster recovery	advance planning and preparations necessary to restore information technology infrastructure, minimize loss and ensure continuity of the critical business functions of an organization in the event of a disaster or unplanned event
information custodian	An individual, organizational unit (e.g. IT, Operations, Systems, Network) or entity (e.g. Office for Technology) acting on behalf of the information owner
information owner	An individual or group of individuals that has responsibility for making classification and control decisions regarding use of information.
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 systems	computers, hardware, software, storage media, networks, operational procedures and processes used in the collection, processing, storage, sharing or distribution of information within, or with any access beyond ordinary public access to, the state's shared computing and network infrastructure
policy	overall intention and direction as formally expressed by management
risk	the likelihood of a threat agent taking advantage of a vulnerability and the resulting business impact. A risk is the lost potential or probability that a threat will exploit the vulnerability.

³⁰ Information Asset Classification Policy #107-004-050

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.
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.

XI. Appendix C – Roles and Responsibilities

Oregon Revised Statute 182.122

	Enterprise Security Office	State Data Center	Agency
Information Systems Security			
<i>Plans, standards, policies, procedures³¹</i>	Develop enterprise information security plans, standards, and policies.	Information systems security for state network and systems under SDC control. Develop plans, standards, policies, and procedures.	Adopt and implement standards, policies and procedures.
<i>Review/verify security of information systems³²</i>	Conduct security assessments using ESO staff or third party.	Conduct self assessments or third party assessments of systems security under SDC control.	Conduct self assessments, third party assessments, or assessments using ESO staff.
<i>Monitor network traffic³³</i>		Monitor state network traffic.	Agencies with their own LANs – monitor network traffic.
<i>Identify and react to threats³⁴</i>	Work with SDC and agencies to address vulnerabilities.	Mitigate threats, work with agencies and ESO to address vulnerabilities.	Agencies must mitigate threats to their information systems, work with ESO to address vulnerabilities.
<i>Conduct vulnerability assessments³⁵</i>	Conduct security assessments using ESO staff or third parties.	Conduct self assessments or third party assessments of systems security under SDC control.	Conduct self assessments, third party assessments, or assessments using ESO staff.
Incident Response			

³¹ ISO 27002 domains: Security policy, organization of information security, policies touch all other domains

³² ISO 27002 domains: Risk management , compliance

³³ ISO 27002 domain: Operations and communications management

³⁴ ISO 27002 domains: Security policy, incident response management

³⁵ ISO 27002 domains: Risk management, compliance

<i>Policies</i> ³⁶	Develop enterprise level policies.		Develop agency policies.
<i>Respond to events</i> ³⁷	Respond through SIRT or at the request of SDC or agency.	Respond for state network and systems under SDC control and at the request of ESO or agency.	Respond if capable, or request SDC or ESO assistance.
<i>Alert appropriate parties</i> ³⁸	Through SIRT.	Advise ESO and agencies of issues identified through monitoring.	Advise ESO of incidents.
<i>Implement forensic techniques</i> ³⁹	Trained staff, procedures, and forensics lab.		Develop capability or request ESO assistance.
<i>Evaluate event; lessons learned</i> ⁴⁰	Document through SIRT or ESO working with agency.	Document work in conjunction with ESO and agency.	Work in conjunction with ESO and SDC.
	Enterprise Security Office	State Data Center	Agency
<i>Communicate; track trends</i> ⁴¹	Track/trend incidents and communicate to agencies, executive management and legislatures.		
<i>Remedial Action</i> ⁴²	Work with agencies and provide recommendations; review agency follow-up actions.	Implement remedial action and report back to the ESO.	Implement remedial action and report back to the ESO.
Agencies			
<i>Security of computers, hardware, software, storage media, networks, operations procedures and processes outside the control of the SDC.</i> ⁴³			Agencies are responsible for information security and security of their systems, applications, desktops, LANs, etc.
<i>Follow enterprise policies, standards, and procedures</i> ¹⁶		Subject to DAS agency policies.	Develop and implement policies, procedures based on enterprise policies.
<i>Report results of any assessments,</i>		Provide assessment and audit results to the ESO.	Provide assessment and audit results to the ESO.

³⁶ ISO 27002 domains: Security policy, incident response management

³⁷ Ibid

³⁸ Ibid

³⁹ Ibid

⁴⁰ Ibid

⁴¹ ISO 27002 domain: Risk management

⁴² ISO 27002 domain: Incident management

⁴³ State Information Security Plan page 1 Agency plans and ISO domain: Security policy

<i>evaluations, or audits.</i> ⁴⁴			
--	--	--	--

Oregon Administrative Rule 125-800-005 through 125-800-0020

	Enterprise Security Office	State Data Center	Agency
State Information Security			
<i>Protect shared computing and network infrastructure</i>		Information systems security for state network and systems under SDC control. Monitor state network traffic. Mitigate threats, work with agencies and the ESO to address vulnerabilities.	Protect agency systems, applications, desktops, LANs, etc.
<i>Leadership</i>	Direct and coordinate all enterprise information security activities.	Develop and implement SDC information security activities based on enterprise direction	Develop and implement agency information security activities based on enterprise direction.
<i>Policies and architecture</i>	Develop enterprise level policies and architecture.	Develop technical policies and architecture for SDC controlled systems.	Develop agency policies and technical procedures based on enterprise direction related to agency controlled information systems.
<i>Conduct vulnerability assessments</i>	Conduct security assessments using ESO staff or third party.	Conduct self assessments or third party assessment of the state network and systems under SDC control.	Conduct security assessments using ESO staff, third parties, or self assessments.
<i>Manage information systems</i>	Develop enterprise policies and provide consultation on systems management.	Develop enterprise systems and management standards for SDC.	Develop and implement agency policies and procedures based on enterprise policies.
<i>Awareness and training</i>	Develop information security awareness and training tools.	Technical security training for SDC controlled systems.	Technical security training for agency IS staff and information security training for all staff handling information assets.
<i>Reporting</i>	Track/trend information security.	Report remediation progress to the ESO.	Report remediation progress to the ESO.
<i>Performance management</i>	Identify and measure information security performance measures.	Develop and implement process to measure performance related to agency security plan,	Develop and implement process to measure performance related to agency security plan,

⁴⁴ ISO 27002 domain: Compliance

		policies, etc.	policies, etc.
<i>Compliance</i>	Conduct compliance reviews using ESO staff or third party.	Conduct compliance reviews of SDC controlled systems through ESO staff, third party, or through self assessments.	Conduct agency compliance reviews through ESO staff, third party, or through self assessments.
<i>Evaluation</i>	Conduct security assessments using ESO staff or third party.	Conduct self assessments or third party assessment of the state network and systems under SDC control.	Conduct security assessments using ESO staff, third parties, or self assessments.
<i>Collaboration</i>	Collaborate with agencies on development of policies, standards and in conducting assessments.	Work with other governmental jurisdictions within Oregon for appropriate cost sharing.	
	Enterprise Security Office	State Data Center	Agency
Agency			
<i>Information security</i>			Chief executive is responsible for agency's information security. Develop and implement policies and procedures based on enterprise policies. Designate an agency security liaison. Develop and implement information security activities based on enterprise direction.
<i>Plans and standards</i>	Develop requirements for agency security plans. Review and approve agency security plans.		Develop a security plan based on the enterprise standards. Submit security plan to ESO for certification and revise security plans to meet certification requirements.
Security Assessments			
<i>Conduct vulnerability assessments</i>	Conduct security assessments using ESO staff or third party.	Conduct self assessments or third party assessment of the state network and systems under SDC control.	Conduct security assessments using ESO staff, third parties, or self assessments.
<i>Identify and react to threats</i>	Follow up on agency mitigation efforts.	Mitigate threats, work with agencies and ESO to address vulnerabilities.	Mitigate threats, work with SDC and ESO to address vulnerabilities.
<i>Report results of any</i>	Collect and aggregate	Provide assessment and	Provide assessment and

<i>assessments, evaluations, or audits</i>	assessment and audit results. Report aggregate results and trends to Director and agencies.	audit results to the ESO.	audit results to the ESO.
--	---	---------------------------	---------------------------

	Enterprise Security Office	State Data Center	Agency
Incident Response			
<i>Policies</i>	Develop enterprise level policies.	Develop data center procedures for systems under SDC control.	Develop agency policies and procedures.
<i>Respond to events</i>	Respond through SIRT or at the request of SDC or agency.	Respond for state network and systems under SDC control and at the request of ESO or agency.	Respond if capable or request SDC or ESO assistance.
	Enterprise Security Office	State Data Center	Agency
<i>Alert appropriate parties</i>	Through SIRT.	Advise ESO and agencies of issues identified through monitoring.	Advise ESO of incidents.
<i>Implement forensic techniques</i>	Trained staff, procedures, and forensic lab.	Utilize DAS agency capability or request ESO assistance	Develop capability or request ESO assistance.
<i>Evaluate event, lessons learned</i>	Document through SIRT or ESO working with agency.	Document work in conjunction with ESO and agency.	Work in conjunction with ESO and SDC.
<i>Communication, track trends</i>	Track, identify trends of incidents and communicate to agencies.		
<i>Remedial actions</i>	Work with agencies and provide recommendations; review agency follow-up actions.	Identify and take appropriate remedial action and report back to the ESO.	Identify and take appropriate remedial action and report back to the ESO.

XII. Appendix D – Statewide Policies Summary

		Agency Actions Required by Policy
--	--	--

Policy No.	Subject	Agency Policy	Agency Procedures / Processes	Agency Plan	Information Classification	Designate Information Owner	Apply Information Protection	Assess Risk	Monitoring / Tracking/ Reporting	Testing	Training
107-004-110	Acceptable Use of State Information Assets	✓	✓						✓		
107-001-010	Business Continuity Planning		✓	✓				✓		✓	✓
107-004-051	Controlling Portable and Removable Storage Devices	✓	✓				✓		✓		
107-004-053	Employee Security	✓	✓								✓
107-004-050	Information Asset Classification			✓	✓	✓	✓	✓	✓		
107-004-052	Information Security	✓	✓	✓			✓	✓			✓
107-004-100	Transporting Information Assets			✓	✓		✓	✓	✓		
107-004-120	Information Security Incident Response		✓	✓					✓		

Policy No.	Subject	Effective Date	Compliance
107-004-110	Acceptable Use of State Information Assets	10/16/2007	
<p>Purpose: To inform authorized users of state agency information assets of the appropriate and acceptable use of information, computers, and devices.</p> <p>Requirements: Any use of information, computer systems and devices will comply with the policy. Agencies will put in place policies, procedures and practices that enable compliance, deter misuse, and detect policy violations. Users of state information assets are responsible for complying with the provisions of the policy and agency-promulgated supporting procedures and practices. Agencies will monitor use of information systems and assets. Agencies will, at a minimum, monitor on a random basis and for compliance. Monitoring systems or processes will be used to create usage reports and resulting reports will be reviewed by agency management for compliance. <i>See policy for specific restrictions and areas of discretionary use.</i></p> <p> <input checked="" type="checkbox"/> Agency Policy <input checked="" type="checkbox"/> Agency Procedures/Processes <input type="checkbox"/> Agency Plan <input type="checkbox"/> Information Classification <input type="checkbox"/> Designated Information Owner <input type="checkbox"/> Application of Information Protection <input type="checkbox"/> Risk Assessment <input checked="" type="checkbox"/> Monitoring </p>			

Policy No.	Subject	Effective Date	Compliance
107-001-010	Business Continuity Planning	3/17/2006	
<p>Purpose: Establishes guidelines requiring all agencies to develop, implement, test, and maintain Business Continuity Plans.</p> <p>Requirements: Agency director is responsible for plan development and designate a Business Continuity Planning Sponsor</p>			

Continuity Planning Coordinator.

Agencies will develop, implement, maintain, and test Business Continuity Plans:

- Conduct business impact analysis
- Identify and document all critical business functions
- Complete a disaster recovery plan
- Ensure short-term and long-term review and revision of plans
- Establish awareness and training programs

Participate in statewide business continuity planning efforts.

Agency Policy
 Agency Procedures/Processes
 Agency Plan
 Information Classification

Designated Information Owner
 Application of Information Protection
 Risk Assessment
 Monitor

Policy No.	Subject	Effective Date	Co
107-004-051	Controlling Portable and Removable Storage Devices	7/30/2007	

Purpose: To ensure the confidentiality, integrity, and availability of state information assets stored on portable or removable storage devices.

Requirements: Each agency will physically control and protect portable and removable storage devices, and protect and manage information stored on them.

Agencies will adopt policy and procedures identifying types of approved devices, govern use of personally-owned devices, and methods for tracking the devices.

Agencies will adopt policy and procedures identifying what agency information assets may or may not be stored on portable storage devices and approved methods for securing that information, as needed, appropriate to the information's sensitivity.

Agency Policy
 Agency Procedures/Processes
 Agency Plan
 Information Classification

Designated Information Owner
 Application of Information Protection
 Risk Assessment
 Monitor

Policy No.	Subject	Effective Date	Co
107-004-053	Employee Security	7/30/2007	

Purpose: To protect information assets and reduce the risk of human error and misuse of enterprise information and equipment.

Requirements: Each agency will develop and enforce a policy that:

- Requires pre-employment screening of employees commensurate with the value and risk of the information assets they have access to;
- Establishes accountability and responsibility to all employees having access to the agency's information assets;
- Establishes processes for timely removal of all permissions for employees having access to information assets and their assets at termination or reassignment; and
- Establishes user awareness training for employees.

Agency Policy
 Agency Procedures/Processes
 Agency Plan
 Information Classification

Designated Information Owner
 Application of Information Protection
 Risk Assessment
 Monitor

Policy No.	Subject	Effective Date	Co
107-004-050	Information Asset Classification	1/31/2008	

Purpose: To ensure State of Oregon information assets are identified, properly classified, and protected throughout their lifecycle

Requirements: All state agency information will be classified and managed based on its confidentiality, sensitivity, value and retention requirements.

Each agency will identify and classify its information assets.

Proper levels of protection will be implemented to protect assets relative to the classification.

All information will have an information owner or owners established within the agency's line of business. Information owners include:

- Create an initial information classification, including assigning classification levels to all data;
- Approve decisions regarding controls, access privileges of users, and ongoing decisions regarding information management;
- Ensure the information will be regularly reviewed for value and updated to manage changes to risk due to vulnerabilities, or changes in the environment;
- Perform periodic reclassification based on business impact analysis, changing business priorities and/or new laws, security standards;
- Follow state archive document retention rules regarding proper disposition of all information assets.

Each agency will identify its information assets for the purpose of defining its value, criticality, sensitivity and legal importance.

Agencies will use the classification schema included in the policy to differentiate between various levels of sensitivity and value:

- Level 1 – Published
- Level 2 – Limited
- Level 3 – Restricted
- Level 4 – Critical

Each information asset will have a range of controls, designed to provide the appropriate level of protection of the information based on the value of the information in that classification.

Agencies will properly identify and protect information meeting the definitions, requirements and effective dates outlined in the Consumer Identity Theft Protection Act (Senate Bill 583, 2007 Legislative Session) as they relate to personal information.

Agencies will develop a plan for identifying, classifying and protecting information assets no later than 6/30/2009.

All Level 4 – Critical information assets will be identified and protected no later than 12/31/2009.

Agencies will comply with all other provisions of the policy, including identification, classification and protection of all information assets by 6/30/2010.

<input type="checkbox"/> Agency Policy	<input type="checkbox"/> Agency Procedures/Processes	<input checked="" type="checkbox"/> Agency Plan	<input checked="" type="checkbox"/> Information Classification
<input checked="" type="checkbox"/> Designated Information Owner	<input checked="" type="checkbox"/> Application of Information Protection	<input checked="" type="checkbox"/> Risk Assessment	<input checked="" type="checkbox"/> Monitoring

Policy No.	Subject	Effective Date	Cor
107-004-052	Information Security	7/30/2007	

Purpose: To emphasize the state's commitment to information security and provide direction and support for information security with business requirements and relevant laws and regulations. Names state standard to guide policy development.

Requirements: Each agency will develop and implement information security plans, policies and procedures that protect its information from the time of creation, through useful life and through proper disposal.

Each State Agency Head is responsible for information security in his/her agency, for reducing risk exposure, and for ensuring that all activities do not introduce undue risk to the enterprise. Each State Agency Head also is responsible for ensuring his/her agency's activities with state enterprise security policies, standards, and security initiatives, and with state and federal security regulations.

All agency employees are responsible for protecting the confidentiality, integrity and availability of the agency's information assets.

Each agency will establish a plan to initiate and control the implementation of information security within the agency and manage it with information assets. The plan will include:

- Processes to:
 - Identify agency information assets;
 - Determine information sensitivity;
 - Determine the appropriate levels of protection for that information;
- Applicable state directives and legal and regulatory requirements;
- Identification of roles and responsibilities for information security within the agency;
- Identification of user security awareness and training elements; and,
- Information security policies that govern agency information security activities.

Each agency will ensure that new business needs and risks are reflected in its information security plans and policies.

Agency information security plans, policies, standards and procedures will be reviewed and revised, as needed, by the agency no less than every five years.

Agency Policy
 Agency Procedures/Processes
 Agency Plan
 Information Classification
 Designated Information Owner
 Application of Information Protection
 Risk Assessment
 Monitoring

Policy No.	Subject	Effective Date	Cor
107-004-100	Transporting Information Assets	1/31/2008	

Purpose: To ensure the security of state information assets when in transit.

Requirements: Each agency must use appropriate security controls for transportation of sensitive information assets (physical media, disk, paper) during transit and beyond the physical boundaries of a facility from loss, destruction or unauthorized access.

Each agency that sends, receives or transports confidential or sensitive information to or from another facility or agency/entity must assure that the information is protected appropriately during transit.

The determination of the sensitivity level of an asset is governed by the statewide Information Asset Classification policy, and it is the responsibility of the information owner to identify sensitive information and ensure appropriate protection.

Agency Policy
 Agency Procedures/Processes
 Agency Plan
 Information Classification
 Designated Information Owner
 Application of Information Protection
 Risk Assessment
 Monitoring

Policy No.	Subject	Effective Date	Cor
107-004-120	Information Security Incident Response	11/10/2008	

Purpose: Create effective information security incident response and handling capabilities for state agencies.

Requirements: Each agency will establish capabilities to respond to information security incidents involving information in an electronic, data, paper, or verbal. Agencies may establish this capability by using internal or a combination of internal and external resources.

Agency capabilities at a minimum must include:

- An incident response plan
- Processes and procedures to implement the incident response plan
- A point of contact to interface with the State Incident Response Team (SIRT)

Agency incident response plan must identify:

- Incident response roles and responsibilities
- Resources and procedures for incident:
 - Preparation and planning
 - Monitoring
 - Identification
 - Evaluation
 - Reporting
 - Response
 - Investigation
 - Recovery and remediation
 - Follow-up and lessons learned
 - Internal and external incident communications
- Awareness training for information security incident responsibilities, identification, and reporting
- Training for designated response resources
- Process for testing and updating plan periodically

Each agency must report information security incidents no later than 24 hours after discovery. Agency point of contact will work with the State to establish method of reporting.

<input type="checkbox"/> Agency Policy	<input checked="" type="checkbox"/> Agency Procedures/Processes	<input checked="" type="checkbox"/> Agency Plan	<input type="checkbox"/> Information Classification	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Designated Point of Contact	<input checked="" type="checkbox"/> Application of Information Protection	<input type="checkbox"/> Risk Assessment	<input checked="" type="checkbox"/> Reporting	