



INFORMATION SECURITY PLAN

July 2009

Bret West, Administrator, Operations Division (DAS Chief Information Officer)
(503) 378-2349, ext. 287

Mel Lester, Operations Division Security (DAS Information Security Officer)
(503) 378-2349, ext. 389

TABLE OF CONTENTS

Introduction	1
Terms and Definitions	3
Authority	4
Roles and Responsibilities	4
Security Program Governance	5
Security Components	5
Risk Management	5
Vulnerability Assessments	6
Security Policy	7
Organization of Information Security	8
Asset Management	9
Human Resources Security	9
Physical and Environmental Security	10
Communications and Operations Management	10
Access Control	11
Acquisition, Development and Maintenance of Information Systems	11
Management of Information Security Incidents	12
Management of Business Continuity	12
Compliance	12
Implementation	13

Introduction

Information is an essential business asset that organizations must protect along with other important business assets. Information can exist in many forms — print, notes on paper, films, or data stored electronically. People share information via mail or electronic means, and in conversation. Whatever form information takes, whatever means people use to share it, an organization should always secure information appropriately.

Information security is the protection of information from a wide range of threats. It helps to ensure business continuity, minimize business risk, and maximize return-on-investment and business opportunities. An organization achieves information security by implementing suitable controls, such as the following examples:

- Policies, processes and procedures
- Organizational structures
- Software and hardware functions

Best practice suggests that an organization should set specific security and business objectives in conjunction with other management processes. The organization then implements appropriate information security controls and periodically monitors and improves the controls to meet its security and business objectives.

In order to implement and properly maintain a robust information security function, DAS recognizes the importance of:

- Understanding DAS' information security requirements and the need to establish policy and objectives for information security;

- Implementing and operating controls to manage DAS' 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; and
- Continual improvement based on assessment, measurement, and changes that affect risk.

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

The Department of Administrative Services (DAS) created this plan based on the provisions of ORS 182.122 and Oregon Administrative Rules 125-800-005 through 125-800-0020.

Terms and Definitions

Asset: Anything of value to the agency.

Business continuity: The ability of an organization to continue critical functions during and after a disruption of its regular operations.

Client agencies: State agencies that contract with the Department of Administrative Services (DAS) for services.

Controls: The means of managing risk, which includes policies, procedures, guidelines, practices or organizational structures. Controls may be administrative, technical, management, or legal in nature.

Disaster recovery: Planning for and preparing to restore an information technology infrastructure, to minimize loss and ensure continuity of the agency's critical business functions in the event of a disaster or unplanned event.

Impact: The magnitude of the potential loss or seriousness of an incident.

Incident: A single event or a series of unwanted or unexpected events that cause harm or threaten information assets, and which requires non-routine preventive or corrective action.

Information asset: All written and electronic assets created by an information owner.

Information security: Measures taken to preserve the confidentiality, integrity and availability of information; ensures that information is authentic, reliable, and from an accountable source.

Information security event: An abnormal, observable and measurable occurrence that involves an information asset.

Information systems: Computers, hardware, software, storage media, networks; the procedures and processes used to collect, process, store, share or distribute information (beyond ordinary public access) within the state's shared computing and network infrastructure.

Policy: A document that clearly defines an intended course of action.

Risk: The possibility of an event that will adversely impact business objectives. Risk is measured in terms of potential impact and the likelihood that a threat exists and that someone could exploit an associated vulnerability.

Risk assessment: A process to identify, analyze, and manage potential risks.

Risk evaluation: A process to compare estimated risk against certain risk-criteria to determine the level of the risk.

Risk management: A process to identify, assess, manage, and control potential events or situations to provide reasonable assurance that the agency can achieve its objectives.

Threat: A potential cause of an unwanted incident that may result in harm to a system or the agency.

Vulnerability: Weakness of an asset or group of assets that one or more threats could exploit.

Authority

This plan relies on the following statewide and internal (DAS) policies related to information security.

Statewide policies:

Policy Number	Policy Title	Effective Date
107-004-050	Information Asset Classification	1/31/08
107-004-051	Controlling Portable and Removable Storage Devices	7/30/07
107-004-052	Information Security	7/30/07
107-004-053	Employee Security	7/30/07
107-004-100	Transporting Information Assets	1/31/08
107-004-110	Acceptable Use of State Information Assets	10/16/07
107-004-120	Information Security Incident Response	11/10/08

DAS internal policies:

Policy Number	Policy Title	Effective Date
107-01-010	Acceptable Use of DAS Information Assets	8/14/08
107-01-070	Approval For Purchase of LAN/Desktop Products or Services	10/22/01
107-01-080	Information Technology Security	6/22/00
107-01-130	Archive and Records Management	11/20/05
107-01-140	Passwords	4/04/07
107-01-180	Information Asset Classification and Transportation	5/28/08
107-01-190	Information Security Incident Response	11/18/08

Roles and Responsibilities

DAS Director: Responsible for information security in the agency; responsible to reduce risk-exposure and to ensure that the agency's activities do not introduce undue risk to state government as a whole. Ensures that the agency complies with statewide security policies, standards, and initiatives, and state and federal regulations.

DAS Chief Information Officer (DAS CIO): Establishes and implements the overall DAS information security plan. This person is also responsible for convening the DAS Incident Response Team (DASIRT) when an incident occurs. The DAS CIO also serves as the administrator of the agency's Operations Division, and as a permanent chairperson of the DAS IT Management Council.

DAS Enterprise Security Office (ESO): Leads statewide information security planning and policy development. Conducts risk and compliance assessments using staff or third party contractors. Coordinates the State Incident Response Team (SIRT). Maintains a forensic analysis capability¹. Develops awareness and training tools for information security. Tracks issues and analyzes trends. Identifies and measures performance measures for information security. Conducts training and

¹ ORS 182.122

workshops, convenes workgroups, and leads forums to support the security-related activities of all state agencies.²

DAS IT Management Council: Provides the strategic direction for DAS information technology and security. Council membership includes at least one representative from every DAS division; several division administrators serve on the council, as does the DAS Chief Audit Executive. The council meets monthly.

DAS Information Security Officer (DAS ISO): Implements information security efforts within DAS. The DAS ISO serves as the point of contact for the State Incident Response Team (SIRT) and is responsible to communicate with SIRT within 24 hours of an incident and coordinate the agency's actions with SIRT in response to an incident that involves information security.

DAS Records Officer: Responsible to coordinate DAS' records management program.

DAS Division Records Coordinator: Appointed by each division administrator to work with the DAS Records Officer and staff within his or her division to identify records (including electronic records) and ensure compliance with retention schedules and other state regulations.

Information Owner: A person or group of people who must establish the necessary controls to generate, collect, process, disseminate and dispose of specified information.

State Data Center (SDC): Responsible for the security of the state's shared computing and network infrastructure. The SDC will occasionally direct a third party to perform audits but does not guarantee that an assessment will occur on any application. Assessments do not necessarily look at the entire system, but only the underlying infrastructure for a specific application. Monitors state network traffic and 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 and network-security standards for a state-operated data center and state network. Participates on the State Incident Response Team as needed.

User: A person with authority to access state information or systems including the state network; responsible to comply with policies, procedures and practices.

Security Program Governance

Governance is an essential component for the long-term strategy and direction of an organization's security policies and risk management program. Governance requires the approval and involvement of executive management, and ongoing support. It also requires an organizational structure³ that provides an appropriate venue to inform and advise executive, business and information technology management on security issues and acceptable risk levels.

The DAS ISO annually assesses each DAS division for the Security Components outlined in this plan and compiles a series of composite reports that contain metrics and recommendations for review by the DAS CIO and DAS IT Management Council. Once approved by the DAS IT Management Council, the DAS Director reviews the reports. After the DAS Director accepts a report, the DAS CIO forwards a copy of the composite report to the ESO.

Security Components

Risk Management

Strong risk management is critical for DAS to successfully implement and maintain a secure environment.

² OAR 125-800-0020

³ Appendix A DAS Organization Chart, http://oregon.gov/DAS/docs/DAS_Org_Chart.pdf

The Safety and Risk Unit of DAS' State Services Division provides leadership to DAS and state agencies regarding risk management. The Safety and Risk Unit (SRU) works with executives and managers, safety advisors and risk coordinators to help state agencies establish effective safety and risk management systems. These systems are designed to:

- Identify risks
- Analyze risks
- Mitigate risk exposures (through the development of loss control programs)

Each division of DAS will perform annual risk assessments to identify, assess, and prioritize risks against certain risk-criteria. The results will help the division determine the appropriate priorities, actions and controls to manage the risks.

No set of controls will achieve complete security. The cost of added information security controls must correspond to the sensitivity or value of the information protected.

The following outline describes the assessment-process, which the division's records coordinator(s) will oversee in coordination with the DAS Records Officer, the appropriate DAS Risk Coordinator (if any) and the DAS Information Security Officer:

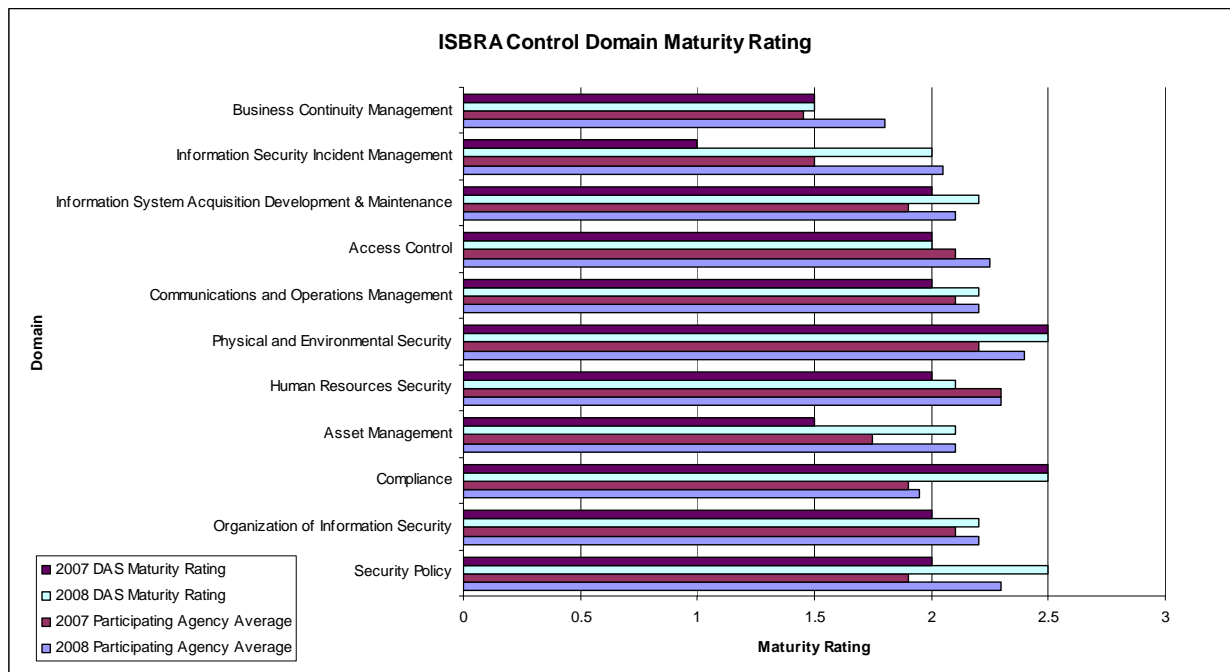
1. Identify the risks.
 - a. Identify the division's information assets and the associated information owners.
 - b. Identify threats to those assets.
 - c. Identify vulnerabilities that the identified threats might exploit.
 - d. Identify the impacts of a loss of confidentiality, integrity or availability of the assets.
2. Analyze and evaluate the risks.
 - a. Assess the business impacts that might result from security failures; consider the consequences of a loss of confidentiality, integrity or availability of the assets.
 - b. Assess the realistic likelihood that security failures might occur in light of prevailing threats and vulnerabilities, the impacts associated with the assets, and the controls currently in place.
 - c. Estimate the level of risks.
 - d. Determine whether the division considers the risks acceptable.
3. Select a risk management strategy.
 - a. Apply appropriate controls to mitigate the risks.
 - b. Accept the risks.
 - c. Avoid the risks.
 - d. Transfer the associated business risks to other parties.
4. Document the objectives and controls in place to mitigate or treat the risks.

Each division's administrator (or designee) will review the division's risk assessment. Once approved, the records coordinator will send the assessment to the DAS ISO, who will compile the assessments of all divisions for evaluation by the DAS CIO and DAS IT Management Council, and finally the DAS Director. Once accepted by the DAS Director, the DAS CIO forwards the risk assessment to the ESO.

Vulnerability Assessments

In addition to the risk-assessment process described above, ORS 182.122 requires DAS to conduct vulnerability assessments through self-assessment, third-party contractor, or (as resources permit) through the ESO. The assessments will verify the level of DAS' security of information systems. DAS is one of several agencies included in the ESO's annual Information Security Business Risk Assessment (ISBRA), which assesses DAS' maturity in the 11 security domains identified in ISO 27002. DAS will continue to participate in ISBRA and provide assessment and audit results to the ESO.

The results of the 2007 ISBRA establish the baseline for DAS' maturity in information security. The department's goal is to continually improve its results.



Maturity Rating	Maturity Phase	Maturity Description
1	Initial	Undefined tasks
2	Managed	Defined tasks, depends on individual projects
3	Defined	Organization standards defined and tailored for individual projects
4	Quantitatively Managed	Process performance measured quantitatively
5	Optimizing	Change process to achieve quantitative process improvement objectives

Security Policy

Information security policies provide direction to DAS employees and managers, consistent with the department's business requirements, governing laws and regulations. The policies establish DAS' approach to managing information security and align with relevant statewide policies (ORS 182.122 requires DAS to develop and implement policies and procedures based on statewide policies). The DAS Director must approve all information security policies, which the DAS CIO will publish and share with all employees and relevant external parties.

The DAS ISO will review the department's information security policies bi-annually — or more frequently if significant changes occur — to ensure their continued suitability, adequacy and effectiveness. The DAS IT Management Council actively participates in policy-development. The council may suggest new policies or revise existing policy-language, and approves all security-related policies before review by other stakeholders or the DAS Executive Team. The council continually assesses opportunities to improve DAS' information security policies and the department's management of security in response to new threats or risks, business circumstances, legal or policy implications, and the technical environment.

DAS uses the following process to develop information security policies:

1. The DAS CIO identifies the need for a security policy.
2. DAS IT Management Council considers and discusses an initial draft of the policy. If needed, the council forms a subcommittee to refine the draft.
3. Subcommittee works on revisions and develops a final recommendation.
4. The full council discusses the evolving policy and develops a final draft.
5. The DAS CIO presents the council's recommendation to the DAS Executive Team.
6. Once approved, the DAS Director signs the final policy.
7. The DAS CIO posts the policy on the DAS Web site and communicates any new requirements to all DAS employees.
8. In some cases, supervisors must obtain employees' signatures to verify they have read and understand the policies.

The DAS CIO uses several vehicles to communicate with DAS employees about new policies and other security-related information. Messages on information security appear in the monthly DAS internal newsletter. Security is an agenda item at regularly scheduled meetings of all DAS supervisors. E-mails to all staff go out periodically when issues surface and when the ESO sends out newsletters. In addition, a link to all policies appears on the DAS home page.

Organization of Information Security

The DAS Operations Division maintains the responsibility to implement the requirements of statewide policies and to establish internal policies for DAS that ensure the security of the department's information assets.

The Operations Division Administrator serves as DAS' Chief Information Officer. The DAS Information Security Officer reports to the DAS CIO. These two positions work with staff from across the agency on information security issues. Refer to the Roles and Responsibilities section above for additional information on these positions and other roles related to information security.

The DAS information security program uses the following principles as the foundation for all actions:

- Take a proactive approach to information security.
- Ensure compliance with state and federal regulations.
- Align information security practices with business practices and priorities.
- Identify trends and proactively address risks that impact information security.
- Act consistently and integrate industry best practices.
- Demonstrate sound fiscal management while achieving high results.
- Maintain trust, credibility, and integrity of the agency.

Several security goals exist to meet statewide requirements and DAS' operational security objectives. The purpose is to protect the confidentiality, integrity, and availability of the department's information assets.

1. Promote information security governance and accountability through these actions:
 - a. Establish a robust DAS IT Management Council — a council comprised of influential and knowledgeable DAS executives who meet frequently and regularly.
 - b. Develop policies to guide information security.
 - c. Continually monitor for new threats, risks, best practices and tools.
 - d. Analyze information security incidents to identify trends and specific actions necessary to mitigate risk.
2. Maintain an information security plan to guide and support the implementation of DAS security policies and practices; the plan should also heighten awareness of security issues.

3. Manage risk by requiring information security assessments on business risk, vulnerability and compliance.
4. Provide guidance and support during and after information security incidents to allow the resumption of business operations and ensure data integrity.

Asset Management

The objective of asset management is to achieve and maintain appropriate protection of DAS' assets. The department identifies the owners of information assets via the actions of each division's records coordinators. According to policy 107-01-130, Archive and Records Management⁴, the records coordinators must inventory all information assets within their divisions and coordinate the records-management program for those assets. The coordinators also prepare a "Special Schedule" for the public records in the custody of the agency. See OAR 166-030-0026.

The Special Schedule applies to all records regardless of physical form, which may include the following examples (not an exhaustive list): Paper, microfilm, microfiche, audio and video recordings, electronic mail, photographs, optical or digital disks, CD-ROM and other recording media, databases.

DAS will ensure an appropriate level of protection for its information assets. According to policy 107-004-052, Asset Classification, the information owners will use certain criteria to classify the assets, and the resulting classifications will appear in the Special Schedule for public records in the agency's custody. The DAS Records Officer will maintain a current copy of each division's Special Schedule.

As in most organizations, the CIO and ISO do not own most of the department's data. The DAS policy on asset classification and transportation places the responsibility to assess risk and take appropriate actions to mitigate risk with data owners throughout the agency.

This plan is subject to the limitations and conditions of the Oregon Public Records Law, which defines information that is open or exempt from public disclosure.

The following statute and policies guide DAS on the acceptable use, identification and documentation of information and information assets:

- ORS 192.4
- Statewide policy 107-004-050, Information Asset Classification
- Statewide policy 107-004-100, Transporting Information Assets
- DAS policy 107-01-180, Information Asset Classification and Transportation⁵.

Human Resources Security

All employees, volunteers, contractors, and third-party users of DAS information and information assets will receive instructions about their responsibilities. DAS will determine and apply suitable roles for users to reduce the risk of theft, fraud or misuse.

DAS will address security responsibilities prior to employment, via position descriptions and associated terms and conditions of employment. Where appropriate, candidates for employment, volunteer work, contractors, and third-party users will receive adequate screening, especially for roles that require access to sensitive information. Additionally, management will apply security principles and processes throughout an employee's employment.

All employees and, where relevant, volunteers, contractors and third-party users will receive appropriate awareness training before DAS management requests access to information or information

⁴ Appendix B, DAS Information Security Policy 107-01-130, Archive and Records Management, <http://oregon.gov/DAS/OP/docs/pdf/10701130.pdf>

⁵ Appendix C, DAS Information Security Policy 107-01-180, Information Asset Classification and Transportation, <http://oregon.gov/DAS/OP/docs/policy/internal/107-01-180.pdf>

assets in DAS' custody. The request should specifically state that the employee, volunteer, contractor or third party has successfully completed training required to access the specific asset in addition to any general awareness training required by DAS. Annually, DAS employees must successfully complete one or more online training modules (prepared by ESO). Employees must also be familiar with relevant policies and procedures for their job function.

When an employee, volunteer, contractor, or third party exits DAS, management will oversee the return of all equipment and removal of all access rights.

Refer to the following policies for DAS' objectives and initiatives relating to human resources security: statewide policy 107-001-110, Acceptable Use of State Information Assets; DAS policy 107-01-010, Acceptable Use of DAS Information Assets⁶.

Physical and Environmental Security

The objective of physical and environmental security is to prevent unauthorized physical access, damage, theft, compromise, and interference to DAS' information and facilities. In locations that house critical or sensitive information or assets, the department will utilize appropriate security barriers and entry controls to provide physical protection from unauthorized access, damage or interference. These controls will ensure that only authorized personnel gain access. The department will use key cards with photo IDs where appropriate.

The Operations and Maintenance section of the DAS Facilities Division provides the following building security services:

- Electronic locks on building doors which lock and unlock as directed by Agency Key Coordinators
- Levels of access assigned to key cards as directed by Agency Key Coordinators
- Master keying system (mechanical locks) to control access to all locked areas
- Database of all keys and key cards issued to employees, contractors, etc.
- Design, installation and maintenance of additional security equipment (CCTV, alarms, intercoms), as requested
- Security for off-site equipment, as requested

Before disposing of equipment that contains storage media, DAS will ensure removal of all sensitive data and licensed software, or ensure secure overwriting of such data. Refer to the statewide e-waste policy, 107-009-0050, Sustainable Acquisition and Disposal of Electronic Equipment.

Communications and Operations Management

DAS will establish appropriate policies and procedures to manage and operate all information-processing facilities. Where appropriate, DAS will segregate duties to reduce the risk of negligent or deliberate misuse of systems or information.

The department will take precautions to prevent and detect the introduction of malicious code and unauthorized mobile code. These actions will protect the integrity of software and information.

To prevent interruptions to business activities, and unauthorized disclosure, modification, removal or destruction of information assets, DAS will control and physically protect all media.

DAS will protect information from unauthorized disclosure or misuse by establishing and communicating procedures to handle and store information. Exchanging sensitive information or

⁶ Appendix D, DAS Information Security Policy 107-01-010, Acceptable Use of DAS Information Assets, <http://oregon.gov/DAS/OP/docs/policy/internal/107-01-010.pdf>

software with other agencies and organizations must involve a documented exchange-agreement that references the information classification level and any specific procedures.

During transport beyond DAS' physical boundaries, DAS will protect media that contains information against unauthorized access, misuse or corruption.

To detect unauthorized access to agency information and information systems, DAS will monitor systems and record information security events. To comply with statewide policies related to acceptable use, DAS will use monitoring techniques.

Refer to the following policies for additional information: statewide policy 107-004-100, Transporting Information Assets; DAS policy 107-01-180, Information Asset Classification and Transportation.

Access Control

Business and security requirements will guide the control of access to information, information systems, information-processing facilities and business processes. To prevent unauthorized access, DAS will develop and implement formal procedures to control access rights to information and systems, and restrict access to operating systems to only authorized users.

Users will receive instruction about their responsibility to maintain effective access controls, particularly the use of passwords. Management will ensure that users understand their responsibility to appropriately protect unattended equipment. A "clear desk" policy for papers and removable storage devices, and a "clear screen" policy will help limit unauthorized access, especially in work areas accessible by the public. Users must protect mobile computing devices and telework areas in proportion to identified risks.

Refer to the following policies for additional information: statewide policy 107-004-052, Information Security; DAS policy 107-01-140, Passwords.

Acquisition, Development and Maintenance of Information Systems

DAS will establish appropriate policies and procedures to ensure the security of information systems when it acquires or develops systems and during system-maintenance processes. Use of encryption (where available and appropriate) will help to protect sensitive information at rest and in transit. DAS will control access to system files and program source-code and conduct technology projects and support activities in a secure manner. In addition, the department will implement technical vulnerability-management tools and use available measures to confirm their effectiveness.

ORS 182.122 requires state agencies to secure information systems, applications, desktops, local area networks, etc. DAS has assigned this responsibility to the security sections of its Technology Support Center and Security Program (Operations Division). DAS will implement internal policies and procedures to ensure that system development include steps at proper junctures to enforce security standards. The standards will apply to all phases (lifecycles) of systems: acquisition, development, maintenance and decommissioning.

The SDC holds explicit authority for the security of the state network and systems within its control. The center will implement policies, procedures, standards and architecture that enforces information security standards for the state's computing network and infrastructure.

DAS also will use industry standards and plans for the entire life of each information system, which includes initiation, concept development, planning, requirements analysis, design, development, integration and testing, implementation, operations and maintenance, and disposition.* These stages closely tie to the stages of project management as outlined in the Project Management Book of

Knowledge, the state of Oregon's designated approach to project management. *System Development Life Cycle (SDLC)

At each stage in the SDLC, DAS will include information security analysis and address information security concerns. Identifying risk during the SDLC will occur, in part, through a program of assessments that includes vulnerability assessments and penetration tests of state and agency-owned systems. Various entities may conduct these assessments — DAS Operations staff, ESO staff, or qualified third parties. Assessments and tests must use clearly documented methods that align with the National Institute of Standards. DAS must share the results with the ESO.

Management of Information Security Incidents

DAS will communicate about information security incidents in a timely manner so that the appropriate people can take suitable corrective action. The department will maintain and follow its established procedures for incident reports and escalation measures — information that all employees have received. A detailed incident-response policy and plan outline the responsibilities and procedures that staff will follow to handle information security incidents.

DAS will report all information security incidents and remedial actions to the ESO.

Refer to the following resources for additional information: DAS policy 107-01-190, Information Security Incident Response⁷; and DAS Information Security Incident Response Plan⁸.

Management of Business Continuity

The definition of business continuity is the 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 that disrupts normal business operations. DAS has established a management process for business continuity to minimize the impact on the department and to recover from loss of information assets (to an acceptable level). This will occur through a combination of preventive and recovery controls that address the information security requirements of the agency.

Business continuity planning (BCP) and disaster recovery are essential parts of risk management. The DAS executive team provides leadership throughout the department for BCP development, testing and maintenance. The department completed its first phase of planning on June 30, 2009, and the executive team reports and discusses its progress related to BCP on a monthly basis.

Compliance

The design, operation, use, and management of information and information assets are subject to various security requirements in statutes, regulations and contracts. Compliance with legal requirements is necessary to avoid breaches of any of the department's obligations. Legal requirements include, but are not limited to: state statute, statewide and agency policy, regulations, contracts, intellectual property rights, copyrights, and protection and privacy of personal information. See the Authority section of this plan for a list of relevant statewide and DAS policies.

DAS maintains personal information of consumers and will notify customers if a security breach of personal information occurs. According to Oregon's Identity Theft Protection Act (ORS 646A.600) customer notices will occur as soon as possible, in one of the following manners:

- Written notification

⁷ Appendix E, DAS Information Security Policy 107-01-190, Information Security Incident Response, <http://oregon.gov/DAS/OP/docs/policy/internal/107-01-190.pdf>

⁸ Appendix F, DAS Information Security Incident Response Plan, http://oregon.gov/DAS/OP/docs/policy/internal/DAS_Incident_Response_Plan.pdf

- Electronic notification, if this is the customary means of communication between you and your customer, or
- Telephone notice, provided that you can directly contact your customer

DAS may delay customer notices if a law enforcement agency determines that the notice will impede a criminal investigation.

If an investigation or consultation with a law enforcement agency (federal, state or local) determines no reasonable likelihood of harm to consumers, or if the personal information included encryption or was unreadable, DAS can forego customer notices.

Substitute notice

If the cost to notify customers would exceed \$250,000, or the number of affected people exceeds 350,000, or if sufficient means are unavailable to contact consumers, DAS may issue a substitute notice by following these two steps:

1. Conspicuous posting of the notice (or a link to the notice) on the DAS Web site
2. Notification to major statewide Oregon television and newspaper media

Notifying credit-reporting agencies

If a security breach affects more than 1,000 consumers, DAS will report to all nationwide credit-reporting agencies, without unreasonable delay, the timing, distribution, and the content of the notice given to affected consumers.

HIPAA requires DAS to implement policies and procedures to address security incidents, and requires creation of a security incident-response team or another reasonable and appropriate response and reporting mechanism. DAS maintains an incident-response plan and an incident-response team, as well as a method to classify security incidents. DAS policy 107-01-190, Information Security Incident Response, addresses these requirements and the DAS Information Security Incident Response plan describes processes and procedures to implement the policy.

DAS will establish controls to maximize the effectiveness of the audit process for information systems. During the audit process, controls will safeguard operational systems and tools to protect the integrity of the information and prevent misuse.

Implementation

The DAS ISO and CIO positions lead information security plan implementation. The recent creation of a dedicated DAS Information Security Officer has positioned the agency for success in the information security arena.

Many of the policies referenced in this plan contain details about various security initiatives. A summary of the initiatives follows.

Education and Training. During 2009-10, the DAS ISO will launch security modules through the iLearnOregon (learning management) system. All current staff will take two modules as described earlier in this plan. New staff will take two mandatory modules within one month of hire.

The DAS CIO will continue to present security-related education to DAS supervisors. The DAS ISO will prepare security-related articles for each edition of the DAS *E-connect* (internal newsletter).

The DAS CIO and ISO will actively share security-related advice to all DAS employees as issues arise. These issues could include such things as new phishing schemes, emerging social engineering activities or newly discovered threats.

Incident Management. The DAS ISO actively responds to incidents and, more importantly, proactively works with staff to prevent incidents before they happen. The ISO will meet with all divisions and work units within DAS during 2009-11 to understand business processes, assess risk, and collaboratively develop strategies to prevent incidents.

Annual Assessments. DAS will continue to take part in the ESO's annual Information Security Business Risk Assessment. DAS will use the results of the annual assessment to monitor progress and set priorities for the agency. These evaluations typically happen in the fall or winter of each year.

The DAS ISO annually assesses each DAS division for the Security Components outlined in this plan and compiles a series of composite reports that contain metrics and recommendations for review by the DAS CIO and DAS IT Management Council. Once approved by the DAS IT Management Council, the DAS Director reviews the reports. After the DAS Director accepts a report, the DAS CIO forwards a copy of the composite reports to the ESO.

Information Asset Classification. Every division will meet the timelines included in DAS policy 107-01-180. The ISO will provide technical assistance to ensure compliance.

Approval

By: 
Scott L. Harra, DAS Director

8/11/09
Date

By: 
Bret West, Operations Division Administrator (DAS CIO)

8/11/09
Date

By: 
Mel Lester, DAS Information Security Officer (DAS ISO)

7/23/2009
Date