



Department of General Services

Information Security and Privacy and Division and Office Business Planning

12.11.08



MEMORANDUM

Date: December 11, 2008

To: Executive Team
Management Team

From: Department of General Services
Information Security Office

Subject: Information Security and Privacy Integration with Division Business Planning

The purpose of this document is to provide departmental Information Security and Privacy objectives for inclusion in Division Business Plans. This includes tasks that establish consistent enterprise implementation of Information Security and Privacy. Current Federal and State requirements and DGS policy reinforce the Divisions role and responsibilities in safeguarding DGS assets (including personal information) collected, used, maintained, and/or held in custodianship for the administration of state programs and services.

Protection of DGS assets and personal information is essential to accomplishing the DGS mission. Failure to protect DGS information and technology can jeopardize the confidentiality, integrity and availability of resources to implement Department and Division strategic and business plans. Managing Security and Privacy risks protects business processes, technology and people and maintains the public and customer trust in DGS.

While ultimate responsibility rests with the Director, every employee plays a role in the protection of DGS assets. The ISO provides security and privacy oversight for compliance and is available for consultation to assist Divisions with policy implementation in transitioning DGS to a "Security Aware" organization. The attached documents provide direction and outline tasks for the enterprise implementation of the DGS Information Security and Privacy programs.

The DGS enterprise Information Security and Privacy program implementation requires integration by both Division/Office and Technical Management to manage DGS security risks. Following is recommended language for Division Business Plan objectives related to Information Security:

Division/Office Information Security Objective

- (1) Specify and monitor the integrity and security of information assets and the use of those assets within their areas of program responsibility, and
- (2) Ensure that program staff and other users of the information are informed of and carry out information security and privacy responsibilities.

Technical Information Security Objective

- (1) Implement the necessary technical means to preserve the security, privacy, and integrity of the DGS's information assets and manage the risks associated with those assets, and
- (2) Act as a custodian of information per SAM Section 5320.3.

The ISO is developing and updating polices associated with the attached summary of tasks that align with the objectives. The ISO will provide draft policies for review within the second quarter of 2009 and communicate progress to Executive and Management teams. Contact the ISO if you have any questions at 376-3940 or DGSInfoSec@dgs.ca.gov.

State Administrative Manual Management Memorandum 08-11 Issued November 6, 2008

State Administrative Manual (SAM) and law, including but not limited to SAM Sections 5100 and 5300 through 5399, and the California Information Practices Act (IPA) of 1977 (Civil Code sections 1798 et seq.), require all state agencies to establish:

- Ongoing data inventory and classification procedures for all records held by the DGS. (SAM section 5320.5 and Chapter 1600).
- Administrative, technical, and physical safeguards to appropriately ensure the security (confidentiality, integrity, and availability) of those records and to protect against anticipated threats or hazards that could result in any injury. (SAM sections 5310 and 5325, and Civil Code section 1798.21).
- Rules of conduct for any person involved in the design, development, operation, use, disclosure, maintenance, and destruction of records containing personal information. (Management Memo 06-12, SAM sections 5310 and 5325, and Civil Code section 1798.20).
- Ongoing training and instruction to any persons involved in the design, development, operation, use, disclosure, maintenance, and destruction of records containing personal information about the rules and consequences of noncompliance. (SAM section 5325 and Civil Code section 1798.20).
- Encryption of portable computing devices and media that store, transport, or access confidential, personal and sensitive information and systems. (SAM section 5345.2)
- For ITSD and Division contracted 3rd Party IT services or procurement: Use of the American National Standards Institute (ANSI) management information standards and the Federal Information Processing Standards (FIPS) in their information management planning and operations. (SAM section 5100). The ANSI standards are national consensus standards that provide guidance on a variety of issues central to the public and industrial sectors. Under the Information Technology Management Reform Act (Public Law 104-106), the Secretary of Commerce approves standards and guidelines that are developed by the National Institute of Standards and Technology (NIST) for Federal computer systems. These standards and guidelines are issued by NIST as FIPS for use government-wide. NIST develops FIPS when there are compelling Federal government requirements such as for security and interoperability and there are no acceptable industry standards or solutions.
- Notification to the ISO when a security breach involving their personal information has occurred. The DGS (ISO and impacted Division) is required to notify individuals affected by the unauthorized disclosure. (SAM section 5350.3 and Civil Code section 1798.29)
- Annual Agency Risk Management and Privacy Program Certification acknowledging the extent to which DGS meets security and privacy requirements submitted to Office of Information Security and Privacy Protection. (SAM sections 5300.3, 5315.1, 5320 through 5320.4, and 5360.1). Government Code section 11549.3 charges the Office of Information Security and Privacy Protection (OISPP) with responsibility for the creation, updating, and publishing of information security and privacy policies, standards, and procedures directing state agencies to effectively manage security and risk for information and information technology.

Information Security and Privacy Division Business Plan Integration

The following are particularly important requirements within the existing legal and policy framework that all Divisions should incorporate into their business plans and implement to safeguard DGS information assets including but not limited to personal information. These are areas that the ISO will create or update current policy, standards, guidelines, and procedures to comply with SAM:

1. Access Rules and Controls. Divisions must ensure that their access control practices support the principle of "least privilege" and appropriate segregation of duties. Least privilege refers to the granting of employee access to personal information or systems based on a legitimate business need to access the information in the performance of their job duties. Divisions and Programs must also implement controls to detect and deter misuse, unauthorized access, or access that exceeds the limits of an employee's authorized access. For example, an employee may, by virtue of his or her job-related duties, have access to all records in a particular database or system, including records that may be held by the department or program about those personally known to him or her (e.g., friends, family members, neighbors, etc.). However, that employee should not access those records unless specifically assigned a job-related duty in support of the processing or handling of such records. And when appropriate communicate it to the supervisor and be excused from processing or handling those records. Divisions and programs must also employ, to the extent practical, technical controls to automate compliance with these requirements. (SAM sections 5100, 5335.1, 5335.2, 5340, and 20050).
2. Employee Training. **Before** permitting access to DGS information and information systems, Divisions must train all employees (including managers and contracted staff) about their privacy and security responsibilities. Supervisors must also be trained about their role and responsibilities for providing day-to-day instruction, training and supervision of staff regarding their obligation to safeguard DGS assets and personal information. Thereafter, Divisions must train employees at least once annually to ensure employees continue to understand their responsibilities. Additional or advanced training should also be provided commensurate with increased responsibilities or changes in duties. Both initial and refresher training must cover acceptable rules of behavior and the consequences when rules are not followed. For Divisions implementing telecommuting or telework, and other authorized remote access programs, training must include the rules of such programs. (SAM section 5325 and Civil Code section 1798.20).
3. Signed Acknowledgements. Divisions must ensure that all individuals with authorized access to DGS information assets and personal information sign an acknowledgement at least once each year to demonstrate both their receipt of the rules and requisite training, as well as their understanding of the consequences for failure to follow the rules. (SAM section 5325).
4. Written Agreements with Third Parties. Divisions must ensure that when DGS assets are accessed or connected to by third parties, it is either specifically permitted or required by law and that a written agreement is executed between the parties. The written agreement is to identify the applicable Federal and state laws, as well as all departmental policies, standards, procedures, and security controls that must be implemented and followed by the third party to adequately protect the information. The agreement must also require the third party, and any of its sub-contractors with whom they are authorized to share the data or system access, to access or share only the minimum resources necessary, to securely store, transport, return or destroy the personal information upon expiration of the contract, and to provide immediate notification to the Division or DGS ISO, and to individuals when appropriate, whenever there is a breach of personal information. (SAM sections 5310 and 5320.3, and Civil Code section 1798.19).

Information Security and Privacy Division Business Plan Integration

5. Encryption. Divisions must encrypt all confidential, personal, or sensitive data when storing, transporting or processing on mobile devices or media whenever that type of information is authorized for use on such devices or media, using only NIST certified cryptographic modules (FIPS 140-2 validated products). (SAM sections 5100 and 5345.2)
6. Review and Reduce Current Personal Information Holdings. Divisions must review current holdings of all records containing personal information and ensure to the maximum extent practical, such holdings are reduced to the minimum necessary for the proper performance of a documented agency function. (Civil Code section 1798.14).
7. Review Current Forms and Other Methods of Personal Information Collection. Divisions must review all current forms, paper, and any other methods (e.g., online or telephony) used to collect personal information, for appropriate Privacy Notice to ensure the specific authority or authorization to collect such information exists, and appropriate notice is included on or with any such forms. (Civil Code section 1798.17).
8. Eliminate Unnecessary Collection and Use. When in the course of such reviews, the collection of personal information is no longer necessary for an authorized business purpose, agencies shall ensure that its collection is discontinued, and that the forms or any other methods used to collect this information are properly retired, revised, or replaced. (Civil Code section 1798.14).
9. Alternative to Use of Social Security Numbers. Recently enacted privacy laws prohibit the use of Social Security numbers as personal identifiers in state systems, or specifically require truncation when they must be used. All DGS Divisions should participate in government-wide efforts to explore alternatives to the use of Social Security numbers as a personal identifier for both recipients of state programs and services, and state employees. (Civil Code sections 1798.14 and 1798.85).
10. Risk Assessment. Divisions must ensure that their risk management practices and ongoing assessments and reviews include evaluations of the adequacy of administrative and technical controls implemented. This includes information or access contractors and other custodians. Additionally, contingency plans must be developed, implemented, and tested to ensure availability and continuity of operations. Consult with the Information Security Office and Information Technology Services Division for security requirements and technical controls. This includes changes to existing or new business processes or technology solutions. (SAM sections 5305 to 5305.2).
11. Incident Management. While Civil Code section 1798.29 focuses on computerized data elements, the current state policy requires notification when a breach of an individual's personal information involves these same "notice-triggering" data elements or otherwise exposes individuals to substantial risk of harm, regardless of the data medium. (SAM section 5350.3). Prompt investigation of incidents involving the improper dissemination of information, or the loss, damage, or misuse of information assets. Incident management includes the formulation and adoption of an incident management plan that provides for the timely assembly of appropriate staff and their response to, reporting on, and recovery from a variety of incidents. (SAM sections 5350 and 8643).

Information Security and Privacy Division Business Plan Integration

12. Monitoring and Compliance. In addition to internal administrative and technical monitoring tools, internal accounting and administrative controls provide reasonable assurances that Information Security and Privacy measures adopted by DGS and its Divisions are followed. This includes annual reporting to the State OISPP demonstrating DGS's compliance with law and policy. Furthermore, in accordance with the California Financial Integrity and State Manager's Accountability Act (FISMA) to ensure requirements are fully complied with the DGS Audits Office must conduct an internal review and report on the adequacy of its internal controls (SAM section 20060).