Information Security Policy (ISP) **INCIDENT RESPONSE AND BREACH NOTIFICATION POLICY**	**Issued by (Policy Owner): Andrew Sturmfels, Administration Deputy Director**
Effective Date: 1-15-19	**Signature:**
Supersedes: None	**Last Reviewed: 01/12/2021**

1. Incident Response and Breach Notification Policy

1.1. Introduction and Overview

The Department of General Services (DGS) is required by federal and state laws to promptly investigate and report incidents and breaches involving loss, damage, misuse of information assets, or unauthorized disclosure of sensitive departmental and personal information. The implementation of this policy is detailed in the DGS Information Security and Privacy Incident Response Plan.

1.2. Objectives

The objective of this policy is to meet federal and state regulatory requirements for response to security and privacy incidents and breaches, and establish roles and responsibilities for effective implementation as outlined in the DGS Information Security and Privacy Incident Response Plan.

2. Scope and Applicability

2.1. The scope of this policy extends to all state and agency information assets owned or maintained by DGS, as well as state information assets managed by third parties on behalf of DGS. This policy applies to all DGS personnel and business associates of DGS through Business Associate Agreements, Memoranda of Understanding, or other contractual agreements.

3. Policy Directives

DGS shall:

3.1. Require personnel to report all known or suspected incidents to the information security office immediately by following the incident reporting process. See Section 7 of this policy.

3.2. Promptly investigate incidents involving loss, theft, damage, misuse of information assets, or improper dissemination of information. *(SAM 5340 Information Security Incident Management)*

3.3. Report information security incidents consistent with security reporting requirements. *(SAM 5340 Information Security Incident Management)*

3.4. Manage information security incidents to determine the cause, scope, and impact to stop unauthorized activity, limit loss and damage, and prevent reoccurrence. *(SAM 5340 Information Security Incident Management)*

Information Security Policy (ISP) **INCIDENT RESPONSE AND BREACH NOTIFICATION POLICY**	**Issued by (Policy Owner): Andrew Sturmfels, Administration Deputy Director**
Effective Date: January 15th, 2019	**Last Reviewed: 01/12/2021**
Supersedes: None	

3.5. Develop, disseminate, and maintain a formal, documented DGS Information Security and Privacy Incident Response Plan according to the specification outlined in SAM 5340. This plan must include documented procedures and associated incident response controls including, but not limited to:

3.5.1. Reporting suspected and actual security incidents to the DGS Information Security Office as required by SIMM 5340-A and other applicable laws and regulations;

3.5.2. Managing security incident case assignments and the security investigation process in a timely and effective manner;

3.5.3. Managing security incidents involving a breach of personal information in accordance with the criteria and procedures set forth in SIMM 5340-C;

3.5.4. Mobilizing emergency and third-party investigation and response processes as necessary;

3.5.5. Consulting with system owners to help quarantine incidents and limit damage;

3.5.6. Consulting with appropriate DGS personnel if there is a violation of the Acceptable Use Policy;

3.5.7. Communicating with law enforcement when actual or suspected criminal activity is involved.

3.6. Implement incident handling for information security and privacy incidents that includes preparation, detection and analysis, containment, eradication, recovery and lessons learned. *(SAM 5340.3 Incident Handling)*

3.7. Report its action plan through the Plan of Action and Milestone (POAM) process. *(SAM 5340.3 Incident Handling)*

3.8. Investigate and mitigate breaches that compromise the security or privacy of patients' health information, personally identifiable information and/or personal information by:

3.8.1. Collecting and preserving evidence;

3.8.2. Documenting corrective actions;

3.8.3. Notifying affected individuals

3.8.4. Providing reports to appropriate oversight entities.

3.9. Provide incident response training to information system users consistent with assigned roles and responsibilities. Incident response training shall include the identification and reporting of suspicious activities. *(SAM 5340.1 Incident Response Training)*

3.10. Conduct annual incident response testing that assesses the effects on DGS operations, assets, and personnel. Incident response testing shall include the use of checklists, walk-through or tabletop exercises, and simulations to prepare personnel and mitigate the impacts of actual incidents. *(SAM 5340.2 Incident Response Testing)*

Information Security Policy (ISP) **INCIDENT RESPONSE AND BREACH NOTIFICATION POLICY**	**Issued by (Policy Owner): Andrew Sturmfels, Administration Deputy Director**
Effective Date: January 15th, 2019	**Last Reviewed: 01/12/2021**
Supersedes: None	

4. Roles and Responsibilities

4.1. The Deputy Director of Administration owns this policy and is responsible for ensuring that all personnel with access to state information assets are aware of this policy.

4.2. The DGS Information Security Officer (ISO) is responsible for:

4.2.1. Ensuring that DGS has a formally documented and operational DGS Information Security and Privacy Incident Response Plan.

4.2.2. Ensuring that the DGS Information Security and Privacy Incident Response Plan, and the procedures within it, describe the necessary roles and responsibilities and activities to enable security incident handlers to effectively prepare for, detect, analyze, contain, eradicate and recover from security incidents.

4.2.3. Ensuring that security incident response management is integrated across DGS, and with other state and DGS contingency and emergency management plans, teams and advisory resources.

4.2.4. Ensuring that all DGS personnel receive incident response awareness training and education in accordance with the individual's functional role within DGS.

4.2.5. Ensuring that DGS incident response capabilities are exercised and documented annually to test incident response effectiveness, derive lessons learned, and continuously improve capabilities.

4.2.6. Ensuring that all security incidents and DGS responses are monitored and documented and that all activities and decisions related to responses to security incidents are recorded.

4.2.7. Ensuring that the DGS Information Security and Privacy Incident Response Plan, including procedures and supporting documentation, are updated annually.

4.2.8. Auditing and assessing compliance with this policy annually.

4.3. Personnel are responsible for participating in and providing assistance with incident response activities as directed by the Incident Commander of the Information Security Incident Response Team.

Information Security Policy (ISP) **INCIDENT RESPONSE AND BREACH NOTIFICATION POLICY**	**Issued by (Policy Owner): Andrew Sturmfels, Administration Deputy Director**
Effective Date: January 15th, 2019	**Last Reviewed: 01/12/2021**
Supersedes: None	

5. Enforcement

5.1. Violation of this policy may result in adverse employment action that may include termination, dismissal, loss of access privileges to state information assets, and civil and/or criminal prosecution.

5.2. Violation of this policy by third parties may also result in the termination of contracts and agreements made with DGS and civil and/or criminal prosecution.

5.3. As set forth in Government Code section 11549.3, state entities shall comply with the information security and privacy policies, standards and procedures issued by the California Office of Information Security (OIS). In addition to compliance with the information security and privacy policies, standards, procedures, and filing requirements issued by OIS, state entities shall ensure compliance with all security and privacy laws, regulations, rules, and standards specific to and governing the administration of their programs. Program administrators shall work with their general counsel, ISO, and Privacy Program Officer/Coordinator to identify all security and privacy requirements applicable to their programs and ensure implementation of the requisite controls.

5.4. The consequences of state entity negligence and non-compliance with state laws and policies may include: Loss of delegated authorities, negative audit findings, monetary penalties and legal actions.

6. Auditing

6.1. DGS has the right to audit any activities related to the use of state information assets.

7. Reporting

7.1. All personnel must report actual or perceived policy violations or security incidents by telephone at (916) 376-3940, or by emailing DGSInfoSec@dgs.ca.gov. For more information about reporting security incidents or policy violations to the DGS ISO, go to " https://cadgs.sharepoint.com/sites/ETS-ISO/SitePages/Security-Incident-Reporting.aspx "

8. Security Exemption Process

8.1 If compliance is not feasible or is technically impossible, if existing policy currently in place already meets these requirements, or if deviation from this policy is necessary to support a business function, the respective manager must formally request an information security variance by submitting an "IT Security Exemption Request" form to the ISO from the ISO Resources site: " https://cadgs.sharepoint.com/sites/ETS-ISO/SitePages/IT-Exemptions.aspx "

Information Security Policy (ISP) **INCIDENT RESPONSE AND BREACH NOTIFICATION POLICY**	**Issued by (Policy Owner): Andrew Sturmfels, Administration Deputy Director**
Effective Date: January 15th, 2019	**Last Reviewed: 01/12/2021**
Supersedes: None	

9. Authority

9.1. This policy complies with Public LAW 104-191 Health Insurance Portability and Accountability Act of 1996 (HIPAA), California Government Code Section 11549.3, California Information Practices Act of 1977 (Civil Code Section 1798 et seq.), State Administrative Manual (SAM) Chapter 5300, Statewide Health Information Policy Manual (SHIPM), Statewide Information Management Manual (SIMM), and National Institute of Standards and Technology (NIST) Special Publication 800-53.

10. DGS References

Reference	Article
ISO-PL1	DGS Information Security and Privacy Incident Response Plan

11. Revision History

Date	Description of Change	Reviewer
12/13/2018	Approved by IT Governance Council	Gary Renslo, CIO
01/15/2019	Approved for Distribution by Administration Deputy Director	Andrew Sturmfels
01/12/2021	Updated hyper-links	Mike Arakji

12. Definitions of Key Terms

12.1. DGS uses SAM 5300 definitions developed by the California Department of Technology for information security and privacy https://cdt.ca.gov/security/technical-definitions/.

12.2. Key Terms specific to this policy:

12.2.1. **Incident Commander** – The individual responsible for the management, documentation, mitigation, and reporting of known or suspected incidents.

12.2.2. **Information Security Incident Response Team (SIRT)** – The collection of personnel, headed by the Incident Commander, who communicate and collaborate to track, investigate, document, and resolve known or suspected incidents. The SIRT is determined by the scope and impact of each incident and may not be a consistent group of individuals. Any individual within the department that is called upon to participate in the SIRT must do so in order to protect the confidentiality, integrity, and availability of state information assets.