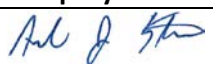


Information Security Policy (ISP) <b>ACCESS CONTROL POLICY</b>	<b>Issued by (Policy Owner): Andrew Sturmfels, Administration Deputy Director</b>
<b>Effective Date:</b> 1-15-19	<b>Signature:</b> 
<b>Supersedes:</b> None	<b>Last Reviewed:</b> N/A

## 1. Access Control Policy

This Access Control Policy documents requirements of personnel for the appropriate control and management of physical and logical access to, and the use of, state information assets.

### 1.1. Introduction and Overview

Access can enable or restrict the ability to do something with a resource. Access control, then, is the selective restriction of these abilities and is comprised of both physical and electronic access.

State information assets owned by the Department of General Services (DGS) are strategic assets intended for official business use, and are entrusted to personnel and business partners in the performance of their job-related duties.

### 1.2. Objectives

Objectives for this Access Control Policy are to:

- 1.2.1. Enable the development and implementation of a DGS identity and access management strategy that comprehensively addresses all access to state information assets;
- 1.2.2. Document requirements for the appropriate control and management of physical and logical access to, and the use of, state information assets;
- 1.2.3. Require the use of appropriate authentication methods based on the type and sensitivity of state information assets being accessed; and,
- 1.2.4. Govern the use of privileged access rights, such as those assigned to Administrator and Privileged Accounts.

## 2. Scope and Applicability

- 2.1 This policy applies to all personnel, all state information assets owned or operated by DGS, and all forms of physical and electronic access to state information assets including using wired, wireless and remote access network connections.

## 3. Policy Directives

- 3.1. DGS executive management adopts a comprehensive identity and access management strategy based on statutory and organizational business requirements, including:
  - 3.1.1. Supporting unique identification, individual user types and groups, job roles and/or access methods;
  - 3.1.2. Limiting access to state information assets and associated facilities to authorized users, processes, or devices, and to authorized activities and transactions;
  - 3.1.3. Defining roles and assigning responsibilities pertaining to access control tools, technologies and processes;

Information Security Policy (ISP) <b>ACCESS CONTROL POLICY</b>	<b>Issued by (Policy Owner): Andrew Sturfels, Administration Deputy Director</b>
<b>Effective Date: January 15<sup>th</sup>, 2019</b>	<b>Last Reviewed: N/A</b>
<b>Supersedes: None</b>	

- 3.1.4. Developing and implementing standards, technologies and processes to support its access control strategy;
- 3.1.5. Formally defining and documenting user account types and groups, and access use cases, commensurate with employment responsibilities within the office;
- 3.2. DGS program management must ensure that access for non-active personnel is deactivated prior to or immediately after separation, as appropriate, by reporting separated personnel to the Enterprise Technology Solutions (ETS) Help Desk. Non-active accounts include those that are issued for temporary use or emergency use.
- 3.3. The information security office must periodically review accounts with elevated privileges and verify that continued privilege account access is required.
- 3.4. DGS programs that are responsible for access to state information assets must ensure access technology and process controls are commensurate with the sensitivity or criticality of information assets under their purview.
- 3.5. DGS programs that are responsible for access to state information assets must authorize all forms of access, including but not limited to remote access. DGS may choose to implement individual user remote access agreements which describe remote user responsibilities.
- 3.6. The information security office must audit and assess user access rights and privileges to ensure alignment with individual job roles and functions on an annual basis.
- 3.7. Personnel must access DGS approved cloud storage services rather than personal cloud storage services while using state information assets.
- 3.8. Personnel must not access or connect any personal storage devices or media, including mobile phones or flash drives, to state information assets.
- 3.9. Personnel must report to their program management and to the information security office any access and privileges beyond what they require to perform their job functions.

#### 4. Roles and Responsibilities

##### **Deputy Director of Administration, Chief Information Officer, and Information Security Officer**

- 4.1. The Deputy Director of Administration Division owns this policy and is responsible for ensuring that all appropriate personnel with access to state information assets are aware of this policy.
- 4.2. The DGS Chief Information Officer (CIO) is responsible for ensuring that appropriate personnel, including executive and program management, as identified within this policy, understand their individual responsibilities.
- 4.3. The DGS Information Security Officer (ISO) is responsible for ensuring that this policy will be reviewed annually, and updated accordingly.
- 4.4. The DGS ISO is responsible for implementing and enforcing remote access agreements between DGS and authorized contractors and business partners.
- 4.5. The DGS ISO is responsible for the periodic auditing and assessment of compliance with this policy.

Information Security Policy (ISP) <b>ACCESS CONTROL POLICY</b>	<b>Issued by (Policy Owner): Andrew Sturmfels, Administration Deputy Director</b>
<b>Effective Date: January 15<sup>th</sup>, 2019</b>	<b>Last Reviewed: N/A</b>
<b>Supersedes: None</b>	

## 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](mailto:DGSInfoSec@dgs.ca.gov). For more information about reporting security incidents or policy violations to the DGS ISO, go to ["http://inside.dgs.ca.gov/iso/Risk/Security\\_Incident\\_Reporting.aspx"](http://inside.dgs.ca.gov/iso/Risk/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: ["http://inside.dgs.ca.gov/iso/Resources.aspx"](http://inside.dgs.ca.gov/iso/Resources.aspx)

## 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.

Information Security Policy (ISP) <b>ACCESS CONTROL POLICY</b>	<b>Issued by (Policy Owner): Andrew Sturfels, Administration Deputy Director</b>
<b>Effective Date: January 15<sup>th</sup>, 2019</b>	<b>Last Reviewed: N/A</b>
<b>Supersedes: None</b>	

## 10.DGS References

Reference	Article
ISP-01	Acceptable Use Policy
AO 16-01	DGS Privacy Policy Statement

## 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 Sturfels

## 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. **Cloud storage services:** A business or website that maintains and manages its customers' data and makes that data accessible over a network, usually the internet.

12.2.2. **DGS executive management:** The Director, Deputy Directors, Office Chiefs, and any other high-level managers responsible for oversight of DGS personnel, business, strategy, and functionality. Executive management are represented in the DGS IT Governance Council.

12.2.3. **DGS program management:** This includes managers and supervisors responsible for direct staff oversight within division and office units under the general direction of executive management.