

EXHIBIT F: SWRCB IT SECURITY POLICIES

OPM-01 - ACCEPTABLE USE POLICY

1. Acceptable Use Policy

1.1 Introduction and Overview

Information assets owned by State Water Resources Control Board (SWRCB) including, but not limited to, SWRCB data and information, collaboration platforms, laptops, cell phones, and removable storage devices are strategic assets intended for official business use and are entrusted to state personnel in the performance of their job-related duties.

Inappropriate use of SWRCB information assets could negatively affect the confidentiality, integrity, or availability of information, information systems, or other information assets of the SWRCB and/or the State of California. Consequently, it is important for all users to access and use information assets in a responsible, ethical, and legal manner that safeguards SWRCB data and information.

Additionally, the appropriate use of information assets benefits the State and SWRCB by strengthening the protection of the SWRCB and its personnel and business partners from illegal or potentially damaging activities.

1.2 Objectives

This policy defines and establishes the requirements for the appropriate use and safeguarding of SWRCB's information assets.

2. Ownership of Information

Data and information in hard copy format that are electronically created, sent, received, processed, or stored on information assets owned, leased, administered, or otherwise under the custody and control of SWRCB are the property of the State. Any information or resources (including e-mail, messages, and files) not specifically identified as the property of other parties, and that is transmitted, processed, or stored on SWRCB's and/or a business partner's IT facilities is the property of SWRCB.

Individual access and use of SWRCB information assets are neither personal nor private. As such, SWRCB and Regional Water Quality Control Boards (Water Boards) management reserves the right to monitor and/or log all employee use of SWRCB information assets with or without prior notice.

3. Scope and Applicability

The scope of this policy extends to all information assets owned or operated by SWRCB and to all personnel authorized to use these assets.

4. Policy Directives

4.1 Users must not use SWRCB information assets to engage in or solicit the performance of any activity that violates laws, regulations, rules, policies, standards, and/or other applicable requirements issued by the federal government, the State of California, and the SWRCB.

4.2 Users must not use SWRCB information assets for personal enjoyment, private gain or advantage, personal gain, political activity, unsolicited advertising, unauthorized fundraising, or an outside endeavor not related to state business.

4.3 Users must use and protect SWRCB information assets in accordance with this policy and applicable information security and privacy policies.

4.4 Users must not engage in any activity that attempts to circumvent or alter the function of SWRCB's security controls (e.g., spoofing email, anonymous proxies).

4.5 Users must not share their work-related account(s), passwords, Personal Identification Numbers (PIN), security questions/answers, security tokens (e.g., smartcard, key fob), or similar information or devices used for authentication and authorization purposes.

4.6 Users must not use SWRCB information assets to send or arrange to send emails and/or intentionally access sites that contain pornographic, racist, or offensive material.

4.7 Users must not use SWRCB information assets to send or arrange to send email chain letters, unauthorized mass mailings, or malicious code.

Internet, Email, and Collaboration Platform Usage

4.8 Users will understand, acknowledge, and adhere to State Water Resources Control Board's Internet, Email, and Collaboration Platform Standards document.

Social Media

4.9 Users responsible for maintaining official SWRCB media accounts must comply with the requirements listed in the State of California's Social Media Standard (SIMM 66B) as well as the

guidelines listed in the Social Media Guidelines for State Water Resources Control Board and Regional Water Quality Control Boards' Internet Presence document.

5. Minimal and Incidental Use

Government Code Section 8314 and the relevant provisions of the Memorandums of Understanding (MOUs) permits the minimal and incidental personal use of State-owned and operated IT resources (e.g., SWRCB computers, telephones, and other approved information assets). As applied at SWRCB, this means:

5.1 Minimal and incidental personal use of state IT assets, including electronic mail, Internet access, fax machines, printers, and copiers is restricted to users that are approved by SWRCB. It does not extend to family members or associates of approved users.

5.2 Minimal and incidental use must not result in direct costs to SWRCB, cause legal action against SWRCB, or reflect negatively upon the mission or values of SWRCB.

5.3 Minimal and incidental use must not interfere with the normal performance of an employee's work duties.

5.4 Questions related to minimal and incidental use questions and issues will be addressed by using the guidelines of the Acceptable Use Policy. Management at Water Boards will work collaboratively with the Human Resources Branch Chief, Labor Relations office, and Information Security Officer (ISO) to resolve issues related to minimal and incidental use.

6. Roles and Responsibilities

WaterBoards Executive Director

6.1 The Executive Director owns this Acceptable Use Policy and is responsible for ensuring that all users of SWRCB information assets are aware of this policy and acknowledge their individual responsibilities.

6.2 The Executive Director is responsible for ensuring that this policy will be reviewed, updated accordingly, and approved by appropriate parties on an annual basis.

6.3 The Executive Director is responsible for the periodic auditing and assessment of compliance with this policy.

WaterBoards Management

6.4 Management shall be committed to ensuring compliance with this and other applicable organizational policies.

WaterBoards Users

6.5 Users must use and protect SWRCB information assets in accordance with this policy and applicable information security and privacy policies.

6.6 Users must not use SWRCB information assets to engage in or solicit the performance of any activity that violates laws, regulations, rules, policies, standards, and/or other applicable requirements issued by the federal government, the State of California, and the SWRCB.

6.7 Users of SWRCB information assets must not engage in any activity that attempts to circumvent SWRCB's security controls (e.g., spoofing email, anonymous proxies, or unauthorized encryption), or other activities that may degrade the performance of information resources or may deprive an authorized user access to SWRCB assets.

6.8 Users must not use SWRCB information assets for personal enjoyment, private gain or advantage, personal benefit, political activity, unsolicited advertising, unauthorized fundraising, or an outside endeavor not related to state business.

6.9 Users must not connect or otherwise attach personal or unauthorized devices or equipment to the SWRCB network infrastructure.

6.10 Users must not share their work-related account(s), passwords, Personal Identification Numbers (PIN), security questions/answers, security tokens (e.g., smartcard, key fob), or other information or devices used for identification, authentication and/or authorization purposes.

6.11 Users must report any security concerns pertaining to SWRCB information asset security of which they become aware to the ISO, designee, or appropriate security staff. Security concerns in information asset security include unexpected software or system behavior, which could result in unintentional disclosure of information or exposure to security threats.

6.12 Users must report any suspected or actual activities and/or events indicating misuse or violation of this Acceptable Use Policy to the ISO, designee, or appropriate security staff.

6.13 All Water Boards personnel are required to acknowledge they have read and understood this policy and applicable information security and privacy policies. The acknowledgment via an

Acceptable Use Acknowledgment Form will be filed in the employee's official personnel record.

7. Enforcement

7.1 Violation of the provisions described in this policy may result in possible corrective action or internal discipline as appropriate pursuant to Government Code Section 19572. Criminal or civil action may also be initiated in appropriate circumstances, including violation of State or Federal laws.

7.2 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, Privacy Officer/Program Coordinator, and ISO to identify all security and privacy requirements applicable to their programs and ensure implementation of the requisite controls.

7.3 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.

8. Auditing

SWRCB has the right to audit any activities related to the use of State information assets as written in the security banner presented before login.

9. Reporting

Violations of this policy must be reported to the Information Security Office.

10. Security Variance Process

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 a security variance as defined in the SWRCB Security Variance policy.

11. Authority

This policy complies with the State of California Government Code Section 11549.3.

12. State Administrative Manual (SAM) and Statewide Information Management Manual (SIMM) References

SAM References	
5305.3	Information Security Roles and Responsibilities
5320.4	Personnel Security
4989.3	Agency Roles and Responsibilities

SIMM References	
5360-B	Remote Access Agreement
5300-A	State-Defined Security Parameters for NIST SP 800-53 Controls
66B	Social Media Standard

13. Definitions of Key Terms

Please refer to the SWRCB Information Technology Glossary for terms and definitions used in this policy.

OPM-02 - IDENTIFICATION AND AUTHENTICATION POLICY

1. Identification and Authentication Policy

1.1 Introduction and Overview

Information assets owned by State Water Resources Control Board (SWRCB) are intended to be accessed by authorized entities and used exclusively for SWRCB's business purposes.

Consequently, it is imperative that all entities that request access to SWRCB's information assets are uniquely identified prior to being granted access.

1.2 Objectives

The objective for this policy is to establish SWRCB's requirements to control access to information assets by uniquely identifying the person or entity requesting access before access is granted.

2. Scope and Applicability

The scope of this policy extends to all State and Agency information assets owned and operated by SWRCB, information assets managed by third parties on behalf of SWRCB, and all information assets that process or store SWRCB information in support of SWRCB's services and mission. This policy applies to all SWRCB and Regional Water Quality Control Boards (Water Boards) personnel and processes acting on behalf of Water Boards personnel. This policy governs physical and logical access. Logical access includes local access and network, including remote access.

3. Policy Directives

SWRCB will ensure that a SWRCB Identity and Access Management (IAM) strategy is developed, clearly defined, documented, and implemented.

The SWRCB IAM strategy must include the following:

- 3.1 Requirements to meet all state and federal requirements.
- 3.2 The unique identification of all authorized personnel or processes acting on behalf of SWRCB that access SWRCB information assets prior to being granted access.
- 3.3 The use of appropriate credentials for the identification of non-State personnel.
- 3.4 Implement methods that enable non-repudiation of access requests to all information assets and protect related audit log data for a minimum of 6 months.
- 3.5 Implementation of a suitable IAM infrastructure supporting SWRCB's requirements.
- 3.6 Implementation of safeguards to protect the confidentiality, integrity, and availability of the supporting IAM infrastructure.
- 3.7 Definition and implementation of authentication mechanisms based on the type and method of access and the inherent risks associated with each access use case.

- 3.8 Control and management of access by administrative and privileged users, including the ability to immediately revoke access when necessary.
- 3.9 Requirement to implement application level identification and authentication in addition to platform level access to provide additional security, as appropriate by owners of information assets.
- 3.10 Definition, documentation, and implementation of audit and security activity and event logging requirements for privileged use.
- 3.11 Identification, development and implementation of supporting identity and access management processes and procedures.

4. Roles and Responsibilities

Information Security Officer

- 4.1 The Information Security Officer (ISO) owns this policy and is responsible for ensuring that all users of SWRCB information assets are aware of this policy and acknowledge their individual responsibilities.
- 4.2 ISO is responsible for ensuring that this policy will be reviewed, updated accordingly, and approved by appropriate parties every three (3) years.
- 4.3 ISO is responsible for the annual auditing and assessment of compliance with this policy.

WaterBoards Management

- 4.4 SWRCB Management shall be committed to ensuring compliance with this and other applicable organizational policies.

WaterBoards Owners of Information Assets and/or Program Management

- 4.5 Owners of information assets will ensure that this policy is implemented and will review the policy's implementation annually.
- 4.6 Owners of information assets will ensure that identification and authentication technologies and process controls commensurate with the sensitivity or criticality of the asset are implemented for assets under their purview.

WaterBoards Information Asset Custodians

- 4.7 Information asset custodians will assist owners of information assets in selecting identification

and authentication technologies and process controls commensurate with the sensitivity or criticality of the asset.

4.8 Information asset custodians will implement identification and authentication technologies and process controls as defined by owners of information assets.

4.9 Information asset custodians will maintain the identification and authentication infrastructure and supporting processes and procedures.

4.10 Information asset custodians will maintain identification and authentication records as defined by owners of information assets for a minimum of six (6) months, or as defined by SWRCB.

WaterBoards Users

4.11 Users must report any incidents of possible misuse or violation of this policy to the ISO, designee, or appropriate security staff.

4.12 All Water Boards personnel are required to acknowledge they have read and understood this policy and applicable SWRCB information security and privacy policies.

5. Enforcement

5.1 Violation of the provisions described in this policy may result in possible corrective action or internal discipline as appropriate pursuant to Government Code Section 19572. Criminal or civil action may also be initiated in appropriate circumstances, including violation of State or Federal laws.

5.2 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, Privacy Officer/Program Coordinator, and ISO to identify all security and privacy requirements applicable to their programs and ensure implementation of the requisite controls.

5.3 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

SWRCB has the right to audit any activities related to the use of State information assets.

7. Reporting

Violations of this policy must be reported to the Information Security Office.

8. Security Variance Process

If compliance is not feasible or is technically impossible, or if deviation from this policy is necessary to support a business function, the respective manager must formally request a security variation as defined in the SWRCB Security Variance policy.

9. Authority

This policy complies with the State of California Government Code Section 11549.3.

10. State Administrative Manual (SAM) and Statewide Information Management Manual (SIMM) Reference

SAM References	
5335	Information Security Monitoring
5340	Information Security Incident Management
5360	Identity and Access Management

SIMM References	
5300-A	State-Defined Security Parameters for NIST SP 800-53 Controls
5340-A	Incident Reporting and Response Instructions
5360-A	Telework and Remote Access Security Standard

11. Definitions of Key Terms

Please refer to the SWRCB Information Technology Glossary for terms and definitions used in this

policy.

OPM-03 - ENDPOINT SECURITY POLICY

1. Endpoint Security Policy

1.1 Introduction and Overview

State Water Resources Control Board (SWRCB) information assets are often used to conduct business functions internally and with other state and non-state entities, persons, and devices on the internet. Devices used for such SWRCB business purposes comprise servers, network devices, and end user devices including mobile computers, tablets and smart devices that connect to networks. Smart devices are rapidly evolving to “things”i. Collectively such devices are “endpoints” or “endpoint devices.” Some SWRCB information assets are more prone to loss or theft, due to their size, mobility, and/or location of use.

The ubiquitous nature of modern telecommunications networks now extends organizational network environment boundaries and corresponding information security risks to endpoint devices.

SWRCB needs to ensure that SWRCB endpoints are suitably protected to prevent unauthorized access to and the protection of data and information that may reside on the endpoints.

1.2 Objectives

Objectives for this policy are to define the requirements to protect SWRCB endpoints that may routinely interact with unknown or untrusted devices on the Internet, or that are more susceptible to loss or theft.

2. Scope and Applicability

The scope of this policy extends to all state and agency information assets owned or operated by SWRCB.

This policy applies to all SWRCB and Regional Water Quality Control Boards (Water Boards) personnel and to all personnel authorized to use SWRCB assets.

3. Policy Directives

SWRCB will:

- 3.1 Ensure that only SWRCB authorized endpoints are permitted to access or connect to SWRCB resources.
- 3.2 Ensure that all SWRCB endpoints are identified, and endpoint asset inventories are documented and continually updated.
- 3.3 Ensure that risks to individual SWRCB endpoint device types and the data they access, process, and/or store are assessed.
- 3.4 Ensure that appropriate endpoint protection controls are selected to manage risks to each endpoint type.
- 3.5 Ensure endpoint security technical controls satisfy requirements listed in State Information Management Manual (SIMM) 5300-A State-Defined Security Parameters for NIST SP 800-53 Controls and SIMM 5335-A Endpoint Protection Standard.
- 3.6 Ensure that endpoint protection controls include people (asset users), processes and technology controls.
- 3.7 Ensure that endpoint protection controls are continuously monitored.
- 3.8 Ensure that endpoint protection controls are implemented, maintained, and reviewed at least annually.

4. Roles and Responsibilities

WaterBoards Executive Director

- 4.1 The Executive Director owns this policy and is responsible for ensuring that all users of SWRCB information assets are aware of this policy and acknowledge their individual responsibilities.
- 4.2 The Executive Director is responsible for ensuring that this policy will be reviewed, updated accordingly, and approved by appropriate parties on an annual basis.
- 4.3 The Executive Director is responsible for the annual auditing and assessment of compliance with this policy.

WaterBoards Owners of Information Assets and/or Program Management

- 4.4 Owners of information assets must ensure that endpoint protection controls are defined, documented, and implemented, and that implementation is reviewed annually.
- 4.5 Owners of information assets must ensure that endpoint protection technologies and controls are maintained and updated per vendor recommendations and align with SIMM 5300-A State-Defined Security Parameters for NIST SP 800-53 Controls and 5335-A Endpoint Protection Standards.
- 4.6 Owners of information assets must ensure endpoint protection controls commensurate with the sensitivity or criticality are implemented for assets under their purview.

WaterBoards Information Asset Custodians

- 4.7 Asset custodians must advise owners of information assets of suitable endpoint protection options.
- 4.8 Asset custodians must implement endpoint protection controls as defined by owners of information assets.
- 4.9 Asset custodians must maintain and update endpoint protection technologies as recommended by vendors and as defined by owners of information assets.
- 4.10 Asset custodians must maintain records of endpoint protection controls and decisions as defined by owners of information assets.

Information Security Officer

- 4.11 The Information Security Officer (ISO) must assist owners of information assets and information asset custodians with the identification and selection of endpoint protection controls.
- 4.12 The ISO must ensure that endpoint protection controls meet SWRCB requirements for security and privacy.

WaterBoards Users

- 4.13 All Water Boards users are required to read and acknowledge they have read and understood this policy and applicable SWRCB information security and privacy policies.
- 4.14 Each Water Boards user will be issued one computer (desktop PC or laptop/notebook) to

conduct official Water Boards business. Any variance to this must be approved by the CIO or designee.

5. Enforcement

5.1 Violation of the provisions described in this policy may result in possible corrective action or internal discipline as appropriate pursuant to Government Code Section 19572. Criminal or civil action may also be initiated in appropriate circumstances, including violation of State or Federal laws.

5.2 As set forth in Government Code section 11549.3, SWRCB 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 the OIS, SWRCB 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.

5.3 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 SWRCB has the right to audit any activities related to the use of State information assets.

7. Reporting

7.1 Violations of this policy must be reported to the Information Security Office.

8. Security Variance Process

If compliance is not feasible or is technically impossible, or if deviation from this policy is necessary to support a business function, the respective manager must formally request a security variation as defined in the SWRCB Security Variance policy.

9. Authority

This policy complies with the State of California Government Code Section 11549.3.

10. State Administrative Manual (SAM) and Statewide Information Management Manual (SIMM) Reference

SAM References	
5305.5	Information Asset Management
5335	Endpoint Defense
5335.1	Malicious Code Protection

SIMM References	
5300-A	State-Defined Security Parameters for NIST SP 800-53 Controls
5355-A	Endpoint Protection Standard

11. Definition of Terms

Please refer to the SWRCB Information Technology Glossary for terms and definitions used in this policy.

OPM-08 - SECURITY AND PRIVACY AWARENESS POLICY

1. Security and Privacy Awareness Training Policy

1.1 Introduction and Overview

A well-trained workforce, aware of information privacy and security risk, plays a crucial role in protecting organizations against a variety of information security threats. Consequently, a formal privacy and security awareness and training program is a key component of the State Water Resources Control Board's (SWRCB) information security program.

1.2 Objectives

Objectives for this policy are to establish the requirement of a formal and effective SWRCB privacy

and security awareness and training program for all SWRCB and Regional Water Quality Control Boards (Water Boards) personnel.

2. Scope and Applicability

The scope of this policy extends to all Water Boards personnel and governs all forms of access to SWRCB information assets.

This policy applies to all Water Boards personnel and to all personnel authorized to use SWRCB assets.

3. Policy Directives

SWRCB will:

- 3.1 Establish a formal SWRCB privacy and security awareness and training program, with clearly defined roles and responsibilities, designed to be delivered to all personnel with access to State information assets.
- 3.2 Provide privacy and security and awareness training to all personnel upon commencement of their employment with Water Boards, and on an annual basis thereafter.
- 3.3 Require role-based privacy and security awareness and training content is delivered commensurate with personnel roles and responsibilities. Retraining will be required if significant changes occur to curriculum or the job role.
- 3.4 Ensure effectiveness of the awareness program through a process of tracking and reporting metrics.
- 3.5 Maintain individual records of all security and privacy training undertaken annually by Water Boards personnel.

4. Roles and Responsibilities

Water Boards Executive Director

- 4.1 The Executive Director owns this policy and is responsible for ensuring that all users of SWRCB information assets are aware of this policy and acknowledge their individual responsibilities.

4.2 The Executive Director is responsible for ensuring that this policy will be reviewed, updated accordingly, and approved by appropriate parties on an annual basis.

4.3 The Executive Director is responsible for the periodic auditing and assessment of compliance with this policy and effectiveness of the program.

Information Security Officer (ISO)

4.4 The ISO must guide and monitor the development and implementation of the SWRCB's security and awareness training program.

Water Boards Users

4.5 Users must participate in all required security and awareness training annually and are required to complete training within thirty (30) days of onboarding.

4.6 Users must complete all required role-based training if assigned based on job function included but not limited to personnel, finance, or information technology.

4.7 All Water Boards personnel are required to read and acknowledge they have read and understood this policy and applicable SWRCB information security and privacy policies. Security and Privacy Awareness training records must be retained for 12 months at minimum.

5. Enforcement

5.1 Violation of the provisions described in this policy may result in possible corrective action or internal discipline as appropriate pursuant to Government Code Section 19572. Criminal or civil action may also be initiated in appropriate circumstances, including violation of State or Federal laws.

5.2 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 OSI, 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, Privacy Officer/Program Coordinator and ISO to identify all security and privacy requirements applicable to their programs and ensure implementation of the requisite controls.

5.3 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

SWRCB has the right to audit any activities related to the use of State information assets.

7. Reporting

The ISO and/or the Training Coordinator will provide SWRCB program management with regular reports on personnel participation in, and the effectiveness of privacy and security and awareness training. Violations of this policy must be reported to the Information Security Office.

8. Security Variance Process

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 a security variance as defined in the SWRCB Security Variance policy.

9. Authority

This policy complies with California Government Code Section 11549.3.

10. State Administrative Manual (SAM) and Statewide Information Management Manual (SIMM) References

SAM References	
5305.3	Information Security Roles and Responsibilities
5320	Training and Awareness for Security and Privacy
5320.1	Security and Privacy Awareness
5320.2	Security and Privacy Training
5320.3	Security and Privacy Training Records
5320.4	Personnel Security

SIMM References	
SIMM 5300-A	State-Defined Security Parameters for NIST SPS 800-53 Controls

11. Definitions of Key Terms

Please refer to the SWRCB Information Technology Glossary for terms and definitions used in this policy.

OPM-09 - ACCESS CONTROL POLICY

1. Access Control Policy

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 logical access.

Information assets owned by the State Water Resources Control Board (SWRCB) are strategic assets intended for official business use and are entrusted to State 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 SWRCB identity and access management strategy that comprehensively addresses all access to SWRCB information assets;
- 1.2.2 Document requirements for the appropriate control and management of physical and logical access to, and the use of, SWRCB information assets;
- 1.2.3 Require the use of appropriate authentication methods based on the type and sensitivity of 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

This policy applies to all personnel; all information assets owned or operated by SWRCB; and all forms of physical and logical access to SWRCB information assets, including using wired, wireless, and remote access network connections. All SWRCB and Regional Water Quality Control Boards (Water Boards) personnel must comply with this policy.

3. Policy Directives

3.1 Access to SWRCB IT infrastructure network must uniquely identify and positively authenticate users prior to providing network access.

3.2 Access to all information systems with information classified as non-public must uniquely identify and positively authenticate users prior to providing access to use SWRCB owned or operated information assets and associated facilities.

3.3 Access to SWRCB information assets and associated permissions must be approved by the respective Water Boards information asset owner or Water Boards official.

3.4 Connectivity to SWRCB cloud-based services will require Multi-Factor Authentication (MFA) using a hard token or authenticator application. Text messages and phone calls are prohibited authentication methods for MFA.

3.5 Records of all user account creations, deletions and changes to user access and permissions must be maintained for a period of 12 months at minimum.

SWRCB must:

3.6 Develop a comprehensive identity and access management strategy based on statutory and organizational business requirements, including:

3.7 Supporting unique identification, individual user types and groups, job roles and/or access methods;

3.8 Limiting access to information assets and associated facilities to authorized users, processes, or devices, and to authorized activities and transactions;

3.9 Defining roles and assigning responsibilities pertaining to access control tools, technologies and processes;

- 3.10 Developing and implementing standards, technologies and processes to support its access control strategy;
- 3.11 Formally defining and documenting user account types and groups, and access use cases, commensurate with employment responsibilities; and,
- 3.12 Employing multi-factor authentication for remote access, and risk-based user authentication methods to accommodate approved logical access use cases.
- 3.13 Publicly available or published access and authentication credentials, such as default credentials, anonymous credentials and guest credentials, must not re-used, and must be replaced as a matter of standard procedure.
- 3.14 Ensure that access to non-active personnel is deactivated prior to or immediately after termination, as appropriate;
- 3.15 Review and validate user access and associated access permissions and privileges every 12 months.

Administrator and Privileged Accounts

Certain Water Boards information technology support personnel and network administrators will require specific privileges to perform their duties.

For all Administrators and/or Privileged Account holders, SWRCB must:

- 3.16 Identify and document all Administrator and Privileged Account holders.
- 3.17 Ensure that such users acknowledge the privileges and only use those accounts to fulfil the specific job responsibilities for which the privileges apply.
- 3.18 Automated processes with access to information systems will follow the same standards for password rotation, limited access and auditing as named user accounts.
- 3.19 Review and validate the continued business need for all Administrator and Privileged Accounts on an annual basis, or when staffing, resource, or job function changes occur.

User Permissions

- 3.20 User access and permissions must be based on the principles of least privilege and

separation of duties.

Audit Records

3.21 SWRCB must define and document all auditable system events related to data and information access that must be recorded.

3.22 SWRCB must ensure access control management systems are configured to capture and record audit and security information related to access events.

3.23 Audit and security records must be securely stored and protected against tampering; audit and security records will be maintained for a period of 12 months.

Monitoring and Alerting

Monitoring and alerting of anomalous or suspicious activities and events is most effectively accomplished through automated and real-time reviews of audit and security logs.

3.24 SWRCB will implement suitable controls to monitor for unauthorized changes to user access. Where feasible, unauthorized changes should generate automated alerts to notify responsible SWRCB individuals.

3.25 In the absence of automated monitoring and alerting, the Information Security Officer (ISO) must review access records on a quarterly basis. Access records include: new user account creation requests, user access revocation requests, active user lists, and user termination lists.

4. Roles and Responsibilities

Water Boards Executive Director

4.1 The Water Boards Executive Director owns this policy and is responsible for ensuring that all users of SWRCB Information Assets are aware of this policy and acknowledge their individual responsibilities.

4.2 The Water Boards Executive Director is responsible for ensuring that this policy will be reviewed, updated accordingly, and approved by appropriate parties every two (2) years.

4.3 The Water Boards Executive Director is responsible for the periodic auditing and assessment of compliance with this policy.

Water Boards Owners of Information Assets and/or Program Management

4.4 Owners of information assets must ensure that this policy is implemented and implementation is reviewed at minimum annually.

4.5 Information System Owners must periodically review accounts with elevated privileges and verify that continued privilege account access is required.

4.6 Owners of information assets must ensure access technology and process controls are commensurate with the sensitivity or criticality of information assets under their purview.

4.7 Owners of information assets must audit and assess user access rights and privileges to ensure alignment with individual job roles and functions on an annual basis.

Water Boards Information Asset Custodians

4.8 Asset custodians must implement access technology and process controls as approved by owners of information assets.

4.9 Asset custodians must implement user access and associated rights and privileges as requested and approved by owners of information assets.

4.10 Asset custodians must revoke or modify individual user access rights and privileges upon notification from the owners of information assets.

4.11 Asset custodians must maintain access records as defined by owners of information assets.

Water Boards Users

4.12 Users must report any incidents of possible misuse or violation of this policy to the SWRCB ISO, designee or appropriate security staff.

4.13 All Water Boards personnel are required to read and acknowledge they have read and understood this policy and applicable SWRCB information security and privacy policies.

5. Enforcement

5.1 Violation of the provisions described in this policy may result in possible corrective action or internal discipline as appropriate pursuant to Government Code Section 19572. Criminal or civil action may also be initiated in appropriate circumstances, including violation of State or Federal laws.

5.2 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, Privacy Officer/Program Coordinator and ISO to identify all security and privacy requirements applicable to their programs and ensure implementation of the requisite controls.

5.3 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

SWRCB has the right to audit any activities related to the use of State information assets.

7. Reporting

Violations of this policy must be reported to the Information Security Office.

8. Security Variance Process

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 a security variation as defined in the SWRCB Security Variance policy.

9. Authority

This Access Control Policy complies with California Government Code Section 11549.3.

10. State Administrative Manual (SAM) and State Information Management Manual (SIMM) Reference

SAM References	
5305.4	Personnel Management

SAM References	
5305.7	Risk Assessment
5315	Information Security Integration
5335	Information Security Monitoring
5335.1	Continuous Monitoring
5335.2	Auditable Events
5355	Endpoint Defense
5355.1	Malicious Code Protection
5360	Identity and Access Management
5360.1	Remote Access
5360.2	Wireless Access
5365.1	Access Control for Output Devices

SIMM References	
5300-A	State-Defined Security Parameters for NIST SP 800-53 Controls
5305-A	Information Security Management Program Standard

11. Definitions of Key Terms

Please refer to the SWRCB Information Technology Glossary for terms and definitions used in this policy.

OPM-11 - DATA SECURITY AND DOWNLOAD POLICY

1. Data Security and Download Policy

1.1 Introduction and Overview

The State Water Resources Control Board (SWRCB) collects, processes, transmits, and stores large amounts of data and information to support essential missions and business functions. Some data

and information maintained by SWRCB may be sensitive and may require special precautions to protect it from unauthorized modification, or deletion (see SAM Section 5305.5). Sensitive information may either be public or confidential.

SWRCB has the responsibility to classify its data and information assets, to implement suitable controls to protect it from unauthorized access, corruption, or loss, and to securely dispose of data and information assets based on data classification.

1.2 Objectives

The primary objective for this policy is to define SWRCB requirements to manage the confidentiality, integrity, and availability of SWRCB data and information assets throughout their lifecycles: from collection, creation, storage, and use to destruction and disposal.

2. Scope and Applicability

The scope of this policy extends to all state and agency data and information assets owned or operated by SWRCB, and/or operated by third parties on behalf of SWRCB and governs all state and SWRCB data and information assets in all forms and media types, including digital and physical formats.

This policy applies to all SWRCB and Regional Water Quality Control Boards (Water Boards) personnel that handle data.

3. Data Classification and Handling

Data Classification is necessary to understand which security practices and controls need to be applied to the data to provide the appropriate level of protection. The more sensitive the data, the tighter the controls need to be on that data. Specialized data handling procedures may be required for Sensitive or Confidential data; in addition, specific data may have additional handling instructions that SWRCB has agreed to contractually. Prior to handling or processing data, users will ensure they understand the proper and/or required handling procedures and are following them appropriately. Data must be maintained at the classification as specified by the originating data owner. Data owners are responsible for the classification of data. Data shall only be stored, shared, transferred, or accessed from systems that match the same classification.

4. Policy Directives

SWRCB will:

- 4.1 Ensure that roles and responsibilities for the identification, classification, and life cycle management of all SWRCB data and information assets are defined, documented, and implemented.
- 4.2 Ensure all employees and contractors be given network access in accordance with entity access control procedures and the least-privilege principle.
- 4.3 Ensure that all SWRCB information assets, including information and information systems, are categorized according to their importance to SWRCB and to relevant organizational and industry standards, as well as to their sensitivity and susceptibility to inadvertent damage, loss or exposure and corresponding impacts to SWRCB.
- 4.4 Ensure that methods to protect the confidentiality and integrity of SWRCB data and information assets according to their classification are defined, documented and implemented.
- 4.5 Ensure that conditions for access to and use of SWRCB information assets for all personnel are defined and documented.
- 4.6 Ensure that all personnel with access to SWRCB data and information assets are trained regarding data access and handling according to their roles and responsibilities.
- 4.7 Ensure that SWRCB data and information assets are used solely for their intended purpose and can only be accessed by those who require access to those assets.
- 4.8 Ensure access to non-public personal information shall be limited to authorized users who need to have access to carry out the SWRCB's responsibilities as it relates to that information.
- 4.9 Ensure that SWRCB data and information assets are securely destroyed and disposed once they are no longer required by SWRCB as defined by established procedures.
- 4.10 Ensure the methods used to destroy and/or dispose of data and information assets comply with the guidelines listed in National Institute of Standards and Technology's (NIST) Special Publication 800-88: Guidelines for Media Sanitization.
- 4.11 Ensure that the proper authorities are notified of security incidents involving data security, as required.
- 4.12 Encrypt data backups according to industry best practices. Securely store backup media or move backup to secure cloud storage.

5. Roles and Responsibilities

Water Boards Executive Director

- 5.1 The Executive Director owns this policy and is responsible for ensuring that all users of SWRCB information assets are aware of this policy and acknowledge their individual responsibilities.
- 5.2 The Executive Director is responsible for ensuring that this policy will be reviewed, updated accordingly, and approved by appropriate parties on an annual basis.
- 5.3 The Executive Director is responsible for the periodic auditing and assessment of compliance with this policy.

Water Boards Management

- 5.4 Management shall be committed to ensuring compliance with this and other applicable organizational policies.

Water Boards Owners of Information Assets and/or Program Management

- 5.5 Owners of information assets must ensure that this policy is implemented, reviewed, updated accordingly, and approved by appropriate parties on an annual basis.
- 5.6 Owners of information assets must ensure that roles and responsibilities for the identification, classification and life cycle management of all data and information assets under their purview are defined, documented and implemented.
- 5.7 Owners of information assets must ensure confidentiality and integrity controls commensurate with asset classification are implemented for data and information assets under their purview.
- 5.8 Owners of information assets must ensure that conditions and rules for access, availability and use of data and information assets under their purview are commensurate with asset classification.

Water Boards Information Asset Custodians

- 5.9 Asset custodians must assist owners of information assets in identifying data security controls commensurate with the classification of the data.
- 5.10 Asset custodians must document, implement, monitor, and maintain data security protection

controls as defined by owners of information assets.

5.11 Asset custodians must revoke or modify individual user access rights and privileges upon notification from the owners of information assets.

5.12 Asset custodians must develop and implement tools, technologies, processes and procedures to support, monitor and maintain data security controls.

5.13 Asset custodians must notify respective owners of information assets and the Information Security Officer (ISO) and/or the Privacy Officer/Program Coordinator of all security incidents pertaining to the security of SWRCB's data, particularly if the incident is related to personally identifiable information (PII).

5.14 Asset custodians must maintain data security records as defined by owners of information assets.

Information Security Officer

5.15 ISO must assist owners of information assets and information asset custodians in the identification of data security controls and processes.

5.16 ISO must participate in incidents involving data security.

5.17 ISO must ensure that data security controls, methods and processes meet SWRCB and applicable regulatory requirements for security and privacy.

Water Boards Users

5.18 All Water Boards personnel are prohibited from downloading data or information which would violate SWRCB's Acceptable Use Policy or violate any local, state, or federal law.

5.19 All users must be granted approval for the download and installation of software which is not already on an approved software list.

5.20 Users must use and protect SWRCB information assets in accordance with this policy and applicable information security and privacy policies.

5.21 All Water Boards personnel are required to read and acknowledge they have read and understood this policy and applicable SWRCB information security and privacy policies.

6. Enforcement

6.1 Violation of the provisions described in this policy may result in possible corrective action or internal discipline as appropriate pursuant to Government Code Section 19572. Criminal or civil action may also be initiated in appropriate circumstances, including violation of State or Federal laws.

6.2 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 and Privacy Officer/Program Coordinator and ISO to identify all security and privacy requirements applicable to their programs and ensure implementation of the requisite controls.

6.3 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.

7. Auditing

SWRCB has the right to audit any activities related to the use of State information assets.

8. Reporting

Violations of this policy must be reported to the Information Security Office.

9. Security Variance Process

If compliance is not feasible or is technically impossible, or if deviation from this policy is necessary to support a business function, the respective manager must formally request a security variation as defined in the SWRCB Security Variance policy.

10. Authority

This policy complies with the State of California Government Code Section 11549.3.

11. State Administrative Manual (SAM) and State Information Management Manual (SIMM) Reference

SAM Reference	
5305.5	Information Asset Management
5310.4	Individual Access to Personal Information
5310.6	Data Retention and Destruction
5310.7	Security safeguards
5340	Information Security Incident Management
5340.1	Incident Response Training
5340.2	Incident Response Testing
5340.3	Incident Handling
5340.4	Incident Reporting
5350	Encryption
5365	Physical access
5365.1	Access Control for Output Devices
5365.2	Media Protection
5365.3	Media Disposal

SIMM Reference	
5300-A	State-Defined Security Parameters for NIST SP 800-53 Controls
5305-A	Information Security Program Management Standard

12. Definitions of Key Terms

Please refer to the SWRCB Information Technology Glossary for terms and definitions used in this

policy.

13. Revision History

Date	Description of Change	Reviewer
6/17/2019	Final	SWRCB Information Security Office
3/10/2020	Annual review	
5/20/2021	Integrated elements from CA Dept. of Technology policy template	
8/4/2022	Annual review	