Exhibit A

INFORMATION TECHNOLOGY USAGE POLICY			
Establishes standards and responsibilities for the appropriate use of SVBGSA information technology resources, including data protection, system access, and compliance with security protocols.			
Approved Date	Resolution	Review Cycle	Initial Date
05/08/25	2025-05	3 years	05/08/25

1. **Scope**

This policy applies to the Salinas Valley Basin Groundwater Sustainability Agency (SVBGSA) Board of Directors (Board) members, employees, contract staff assigned to SVBGSA and others with access to SVBGSA Information Technology (IT) resources (collectively "Users")

Staff who are assigned to SVBGSA from another company/organization shall also adhere to the regulations and guidelines of that company/organization.

2. **Use of IT Resources**

SVBGSA's IT resources are intended for work-related activities. Limited personal use is allowed as long as it does not interfere with job duties, violate laws, or incur significant costs. Users shall not access or distribute illegal or inappropriate material. Any actions that compromise network integrity, such as introducing malware or attempting unauthorized access, are strictly forbidden. Personal social media use must not conflict with professional responsibilities or harm the SVBGSA's reputation. Official SVBGSA social media accounts shall only be utilized to post agency-related content, not personal material.

3. **Email and Communication**

Users shall use their SVBGSA-provided email accounts for all official communications. Personal use of these accounts is discouraged. They shall remain vigilant for phishing attempts and suspicious messages, reporting any concerns to the IT department.

4. **Security and Confidentiality**

Users shall create strong passwords and never share their credentials. They shall access only the systems necessary for their roles, regularly encrypt and back up sensitive data, and always protect the confidentiality of SVBGSA information. Multi-factor authentication (MFA) is mandatory for sensitive systems, and user accounts must be deactivated immediately upon termination or when access is no longer needed.

5. **Compliance with Laws and Regulations**

Users shall comply with data privacy laws, copyright laws, and the Ralph M. Brown Act, which prohibits serial meetings conducted via email and mandates the adherence to appropriate communication protocols.

6. **Artificial Intelligence**

SVBGSA supports the responsible and ethical use of artificial intelligence (AI) technologies. AI must not be used for decision-making without appropriate human oversight and shall not access or process confidential or personally identifiable information unless explicitly permitted.

7. **Reporting and Enforcement**

Users shall promptly report any suspected misuse, breaches, or security concerns to the designated IT personnel. Violations may result in disciplinary action, which can include suspension of IT privileges, termination, or legal action, based on the severity of the violation.

8. **Data Governance**

The SVBGSA owns all data generated or processed by it. Users shall adhere to retention schedules and securely delete unnecessary information.

All SVBGSA data shall be handled according to its sensitivity. Public data is suitable for widespread distribution, while internal data is intended for use within the agency. Confidential data includes sensitive information, such as financial records or employee data, and must be properly protected. Restricted data, such as system credentials or infrastructure plans, requires the highest level of security. Users are responsible for securely storing, transmitting, and handling data based on its classification. Encryption is mandatory for confidential and restricted data to prevent unauthorized access or loss.

9. **Incident Response and Reporting**

Security incidents, including suspected breaches or malware infections, must be reported promptly and documented for future analysis and enhancements.

10. **Vendor and Third-Party Management**

Vendors shall comply with SVBGSA's security and privacy standards. Third-party access necessitates signed confidentiality agreements and suitable security evaluations.

11. Monitoring and Auditing

The SVBGSA monitors IT activity, encompassing network traffic and system access. Audit logs are kept and periodically reviewed to identify unauthorized activity.

Version History

V1: Date 05/08/25 Reso # 2025-05