Administrative Policy 9 - 4

Information Technology

Professionals

Policy

Manual

This page intentionally left blank

Table of Contents

Information Technology Professionals Policy Manual

Approved by: Board of Supervisors of the County of Sonoma ("County"), and the Boards of Directors of the Northern Sonoma County Air Pollution Control District, the Russian River County Sanitation District, Sonoma Valley County Sanitation District, Occidental County Sanitation District, South Park County Sanitation District, and the Board of Directors of the Sonoma County Agricultural Preservation and Open Space District (collectively referred to hereinafter as "Special Districts"), and the Sonoma County Water Agency ("Agency"), and the Board of Commissioners of the Sonoma County Community Development Commission ("Commission"). The County, Special Districts, Agency and Commission are collectively referred to herein as "Local Agencies" or singularly as "Local Agency."

Authority:
Approval Date:
Effective Date:

Purpose

This Policy manual provides direction to all individuals responsible for the implementation, configuration, maintenance and support of Local Agency IT resources.

Scope

This Policy manual applies to all Local Agencies. Where conflict exists between this Policy manual, Local Agency's policy, or state/federal regulations, the more restrictive policy will take precedence.

Maintenance

This Policy manual is subject to a policy review at least annually by the Information Security Steering Committee (ISSC).

Exceptions

Requests for exceptions to this Policy manual must be reviewed by the Information Security Steering Committee (ISSC) and approved by the Chief Information Security Officer (CISO) or Designee. Local Agencies requesting exceptions must provide such requests to the ISSC. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception and risk mitigation measures to be undertaken by the Local Agency. The ISSC will review such requests, confer with the requesting Local Agency and forward to the CISO a recommendation for approval or denial. Appeals will be directed to the Board of Supervisors for resolution. All exceptions are reviewed annually by the ISSC.

Amendments

Requests for amendments (i.e., changes, deletions, additions) to this Policy manual must be presented by the Department Information Security Representative to the Information Security Steering Committee (ISSC). If the ISSC agrees to the change, the Policy manual will be updated, reviewed and approved through the normal County approval process.

Policy

I. Introduction

Information is an asset, which, like other important business assets, has value to an organization and consequently needs to be suitably protected. The County of Sonoma has an obligation to the public and is mandated by laws and standards (see Appendix A) to protect information maintained on Local Agency IT resources from unauthorized use, disclosure, modification, loss or denial.

This Policy manual has been developed to be in alignment with the International Organization for Standardization (ISO) 27002 Code of Practice for Information Security Management framework and to meet County compliance obligations. This manual, together with the Administrative Policy 9-2: Departmental Computer Use, establishes the foundation for information technology security in the County to assure appropriate and authorized access, usage and integrity of information. Compliance with this Policy manual is mandatory.

II. Roles and Responsibilities

Information security extends well beyond Information Technology (IT). Information security is a critical business function that touches all aspects of an organization including, fiscal, legal, human resources and IT. The County of Sonoma (County) is fully committed to information security and asserts that

every person employed by or on behalf of the County has important responsibilities to maintain the security of Local Agency IT resources and data.

A. Chief Information Security Officer

The County Information Systems Director serves as the Chief Information Security Officer and is responsible for:

1. Overseeing and managing the County Information Technology and Security Program, which includes;

   (a) Developing and maintaining the County information security strategy;

   (b) Providing information security related technical, regulatory and policy leadership;

   (c) Facilitating the implementation of County information technology and security policies; and

   (d) Approving or denying policy waivers.

B. Information Security Steering Committee

The Information Security Steering Committee is the coordinating body for all County information security-related activities and is composed of the County Privacy Officer, Information Security Officer and individuals designated by the IT Governance Council. The Information Security Steering Committee is responsible for:

1. Developing and proposing County information technology and security policies, standards, and guidelines;

2. Reviewing County information technology and security policies and policy waivers annually;

3. Reviewing Local Agency policy exception requests and making recommendations for CISO approval or denial;

4. Maintaining documentation of policy waivers;

5. As requested, reviewing Local Agency information technology and security policies for compliance with County policies; and

6. Identifying and recommending industry best practices for information security.

C. Local Agency Department Head/General Manager

The Local Agency Department Head/General Manager and/or Designee are responsible for:

1. Periodically reviewing security processes to ensure compliance with relevant security policies and standards;

2. Establishing supplemental information technology and security policies as needed for their business purposes, provided they are not less restrictive than County policies;

3. Establishing procedures and guidelines as needed in support of this Policy manual; and

4. Designation of an information security representative.

D. Information Security Representative

The Information Security Representative is designated by the Local Agency Department Head/General Manager to coordinate information security within their Local Agency and is responsible for:

1. Assisting in the development of any Local Agency information technology and security policy;

2. Reviewing Local Agency information technology and security policies for compliance with County policies; and

3. Representing the Local Agency's information security concerns countywide.

E. Local Information Services Providers

The County Information Systems Department, the Human Services Department Information Integration Division, the Sonoma County Sheriff's Office Technical Services Bureau, and the County Water Agency Computer Application and Instrumentation Support Section serve as Local Information Service Providers and are responsible for:

1. Providing network infrastructure, network access, data storage and e-mail services to Local Agencies;

2. Maintaining an inventory of Local Agency IT resources;

3. Configuring Local Agency IT resources in accordance with County information technology and security standards;

4. Implementing and maintaining technology-based services that adhere to the intent and purpose of applicable information technology and security policies, standards and guidelines; and

5. Investigation, remediation and documentation of information security incidents; and

6. Establishing and implementing standards, procedures, and guidelines as needed for this Policy manual.

F. Data Owner

The Data Owner is the Local Agency Department Head/General Manager or other individual authorized by law, regulation or policy to collect and manage the data that supports their business operations and is responsible for:

1. Identifying applicable law, regulations, or standards that contain information security requirements for the data they own;

2. Classification of Local Agency data and IT resources based upon law, regulation, common business practice, liability or reputational factors;

3. Establishing as needed, Local Agency policies and procedures for the data and IT resources they own; and

4. Responsible for ensuring mitigation of known or suspected information security incidents, and notification to individuals or agencies in the event of a data breach involving unencrypted personal information.

G. Data Steward

The Data Steward is designated by the Data Owner to protect the confidentiality, integrity, and availability of the data that supports their business operations and is responsible for:

1. Assisting the Data Owner in the classification of Local Agency data;

2. Implementing protection requirements for the data and IT resources entrusted to their stewardship; and

3. Authorizing access to Local Agency data in accordance with the classification of the data.

H. Data Custodian

The Local Information Service Provider serves as the Data Custodian and is responsible for:

1. Implementing the necessary safeguards to protect Local Agency data and IT resources at the level classified by the Data Owner or the Data Steward;

2. Granting access privileges as authorized by the Data Owner or Data Steward;

3. Complying with any additional security policies and procedures established by the Data Owner and/or Data Steward;

4. Advising the Data Owner and/or Data Steward of vulnerabilities that may present a threat to their Local Agency data and of specific means of protecting that data; and

5. Notifying the Data Owner of any known or suspected information security incident.

III. Access Control Policy

This Policy establishes logical access controls Local Information Service Providers must implement to secure Local Agency IT resources and data.

A. Secure Log-On Procedures

Access to Local Agency IT resources and data must be controlled by secure log-on procedures.

1. Logon Banners

When technically feasible, logon warning banners must be displayed on any information system that hosts nonpublic services. Logon warning banner content must inform Users that Local Agency IT resources are for authorized County/Local Agency business only,

User activities may be monitored, and Users have no expectation of privacy.

2. Unsuccessful Login Attempts

The number of consecutive attempts to enter an incorrect password must be limited. User IDs must be temporarily disabled (locked out) after a prescribed number of unsuccessful access attempts have been made as determined by Local Information Service Provider standards.

B. Password Management

Password standards must be developed and implemented to ensure all Users follow proven password management practices. These password standards must be mandated by automated controls when technically feasible and include but are not limited to the following:

1. Prohibiting the storage and transmission of passwords in clear text;

2. Prohibiting use of default vendor passwords;

3. Changing temporary password at the first login and reset;

4. Changing passwords at regular intervals;

5. Development of procedures to verify a User's identity prior to providing a replacement password (i.e., password reset); and

6. Enforcing choice of strong passwords.

C. Use of System Utilities

Use of system utilities that are capable of overriding other controls must be restricted.

1. Access to system utilities must be limited to Users and Administrators with an approved need to run or use those utilities.

2. Temporary access may be granted only after a business requirement for access has been documented and approved.

3. When technically feasible, unneeded system utilities, options, and/or services must be removed or disabled.

D. Session Time-Out

As determined by Local Information Service provider standards, security measures must be implemented to require authentication or re-authentication after a prescribed period of inactivity for desktops, laptops, or any other Local Agency IT resources where authentication is required.

E. Connection Limitation

Restrictions on connections must be used to provide additional security for high-risk application or remote communication capabilities. As determined by Local Information Service Provider standards, the following controls must be applied and maintained:

1. Connection time (e.g., office hours);

2. Connection location; and

3. Requiring re-authentication at timed intervals.

F. Application Access Control

To prevent unauthorized access to information stored in Local Agency application systems, access must be restricted to Users and support personnel whose work assignment requires access to those applications.

IV. Business Continuity Management Policy

This Policy establishes requirements for Local Information Service Providers to develop and maintain a business continuity plan.

A. Business Continuity Plan

Local Information Service Providers must develop and implement a business continuity plan to maintain or restore operations and ensure availability of information, following interrupts to or failures of business processes. The Plan includes:

1. Identification of and agreement on all responsibilities and operational procedures;

2. Disaster recovery/business continuity procedures;

3. A data backup plan to ensure recovery of data;

4. Specification of alternative operational procedures;

5. Documentation of the above plan elements; and

6. Testing and updating of the plan.

V. Change Management Policy

This Policy establishes requirements for the Local Information Service Provider's change management process to ensure all changes are assessed, approved, implemented and outcome reviewed and to minimize impact of change related incidents to business operations and Users.

A. Change Management

Local Information Service Providers must have a documented process to control changes to the Local Agency IT resources they support, including software, system documentation and operating procedures.

Change management includes the following documented processes and procedures:

1. Risk assessments, an analysis of actual and potential impacts of changes, and necessary countermeasures or mitigation controls;

2. Planning and testing of changes; including fallback (abort/recovery measures)

3. Review for compliance with County/Local Agency security policies and Local Agency security requirements;

4. Approval and authorization of changes;

5. Appropriate notification of all affected parties prior to implementation, on the nature, timing, and likely impacts of the changes;

6. Verification of changes to ensure the approved change was made, and to assess the post-implementation security state;

7. Documentation and maintenance of change records for audit purposes and the investigation of security incidents; and

8. Periodic review of the change management process for its effectiveness.

VI. Cryptography Policy

This Policy establishes requirements for the use and management of cryptography.

A. Cryptographic Controls

Local Information Service Providers must establish standards on the use of cryptography. Controls must include:

1. Compliance with all relevant agreements, laws or regulations;

2. A risk assessment to determine the required level of protection; and

3. Cryptography key management.

a) Keys must be securely distributed and stored.

b) Access to keys must be restricted to only those individuals who have a business need to access the keys.

VII. Information Systems Acquisition, Development and Maintenance Policy

This Policy provides direction for the integration of information security into the lifecycle of information systems that hold and process Local Agency data.

A. Security Requirements of Information Systems

1. To ensure security is built into all Local Agency information systems, all security requirements must be identified and documented at the design stage for new information systems or enhancements to existing systems.

2. Security controls must be commensurate with the risks and the relative sensitivity of the system and the information it stores and/or processes.

B. Separation of Development, Test and Production Environments

1. Development and test environments must be logically or physically separated from production environments.

2. Media used for development and test activities must be clearly labeled as such and must not be used on production systems unless all test data has been removed.

3. Local Agency data that is used for development and test activities must be protected and controlled.

4. If production data is used in a test environment, the following must be adhered to:

   a. Production data used in a test environment must be protected as if it is still production data.

   b. A copy of the production data must be made so that live data cannot be altered.

   c. The physical or electronic output of tests using the production data must be strictly controlled and promptly destroyed when no longer needed.

C. System Planning and Acceptance

1. Advance planning and preparation must be performed to ensure the availability of adequate capacity and resources. The security requirements of new systems must be established, documented, and tested prior to their acceptance and use.

2. The capacity demands of Local Agency IT resources must be monitored and projections made of future capacity requirements to ensure adequate power and data storage requirements can be filled.

3. Acceptance criteria must be developed and documented for new information systems or enhancements to existing systems.

4. Acceptance testing must be performed to ensure security requirements are met prior to the system being migrated to the production environment.

D. Correct Processing in Applications

To prevent errors, loss and unauthorized modification or misuse of information in application systems; processes must be established and maintained for:

1. Input data validation - Data input to an information system must be validated to ensure it is correct and appropriate.

2. Internal processing - Internal processing checks must be performed to minimize the risk of processing failures or deliberate acts leading to a loss of integrity.

3. Output data validation – Data output from an information system must be validated to ensure the processing of stored information is correct and appropriate.

4. Message integrity - Message integrity controls must be used for information systems where there is a security requirement to protect the authenticity of the message content.

5. Error response – Responsibilities and procedures must be defined for responding to detected errors.

E. Software Maintenance

1. When technically feasible, all system software must be maintained at a vendor-supported level to ensure software accuracy and integrity.

2. Modification of commercial-off-the-shelf software security controls is limited to essential changes that are strictly controlled and documented.

3. All known security patches must be reviewed, evaluated, and appropriately applied in a timely manner. See also Section XII. Technical Vulnerability Management Policy.

F. Change Control

Changes to software must be controlled by the use a formal change control procedure as specified in Section V. Change Management Policy.

VIII. IT Resource Management Policy

This Policy establishes the appropriate protection of Local Agency IT resources.

A. Inventory of IT Resources

Local Information Service Providers must maintain an inventory listing of significant Local Agency IT resources. Listing should include:

1. Core attributes for each IT resource, including make/model/format, creation/manufacture date;

2. IT resource unique identifier (e.g., serial number, asset number, service tag number, or Universal Product Code);

3. Assigned owner; and

4. Location.

B. Responsibility of IT Resources

IT resources must have owners assigned from within the Local Agency who are responsible for ensuring appropriate protection from unauthorized use, access, disclosure, modification, loss or deletion.

C. Classification of IT Resources

IT resources must be classified and labeled based on the most restrictive classification of its individual data elements. For example, IT resources containing confidential data and restricted data must be classified as Confidential. IT resources containing Restricted data and Public data must be classified as Restricted.

D. Return of IT Resources

Procedures must be established to ensure Local Agency IT resources are returned upon a User's separation from County employment or change of work assignment.

E. Secure Disposal or Re-Use of IT Resources

1. To prevent the unauthorized disclosure of Local Agency data, Local Agency IT resources containing storage media must be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.

2. All Local Agency IT resources must be sanitized according to classification of data, prior to sale, transfer or disposal.

3. Local Agency IT resources containing confidential data must be obliterated and/or made indecipherable before disposal.

4. If licensed software is present on any Local Agency IT resource being sold, transferred, or otherwise disposed of, the terms of any licensed software agreements must be followed.

5. To verify Local Agency data is inaccessible, a sample of Local Agency IT resources must be tested.

IX. Network Management Policy

This Policy establishes requirements for access control and security management of Local Agency networks.

A. Network Security Management

All Local Agency networks must be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and application using the network, including information in transit. Local Information Service Providers must at minimum, implement the following:

1. Managing and monitoring network security is separate from computer operations when possible;

2. When necessary, special controls are implemented to safeguard the confidentiality and integrity of sensitive data passing over public networks (i.e., the Internet);

3. Security requirements of network services must be identified and documented, which include specification of:

(a) Technologies applied for security of network services, (e.g., authentication, encryption and connection controls;

(b) Technical parameters and rules for secured connection with the network; and

(c) Procedures and processes to control and/or restrict access.

B. Network Connections

All connections to Local Agency networks must be authorized by the Local Information Service Provider.

C. Network Access Control

To prevent unauthorized access to network services the following controls, at minimum, must be implemented:

1. Access to a Local Agency's network must require all authorized Users to authenticate themselves through use of an individually assigned User-ID and an authentication mechanism, (e.g., password or token).

2. Network access controls must ensure that Users can only access the Local Agency IT resources and data they have been specifically authorized to use.

3. Where technically feasible, access to a Local Agency network must be limited to identified devices or locations.

4. Physical and logical access controls must be implemented and maintained to protect diagnostic and configuration ports.

5. Access controls must be implemented between segments as necessary.

D. Remote Access Control

1. Remote access connections to a Local Agency network must be done in a secure manner to preserve the integrity of the network, data transmitted over the network, and the availability of the network.

2. To maintain information security during remote access to Local Agency IT resources, individual accountability must be maintained.

3. Use of a common access point is required. All remote connections to Local Agency IT resources must be made through managed central points of entry.

4. All Virtual Private Network (VPN) connections must have split tunneling disabled. In the case where split tunneling must be enabled to accommodate a business need, a risk assessment must be performed to ensure that the connection will not compromise the Local Agency network.

X. Operations Management Policy

This Policy establishes information security requirements for operations management.

A. Operating Procedures

1. All Local Information Service Providers must have documented operating procedures related to information security including but not limited to:

(a) Processing and handling information;

(b) Securely, handling and transporting storage media;

(c) Handling unexpected outages or technical difficulties; and

(d) Restart and recovery procedures.

2. Procedures must be verified by the Local Information Service Provider's Information Security Representative to ensure they implement the desired Policy or Standard.

3. Procedures must be kept up to date by authorized staff and stored in a secure location.

B. Separation of Duties

1. To reduce the risk of accidental or deliberate system misuse, separation of duties must be implemented where practical.

2. Whenever separation of duties cannot be implemented, other compensating controls such as monitoring of activities, audit trails and management supervision must be implemented. At a minimum, the audit of security must remain separate and

independent from the security function (i.e., security administration and security audits must be performed by different persons).

C. Protection from Malicious Code

Software and associated controls must be implemented across Local Agency networks to prevent and detect the introduction of malicious code. The type of controls and frequency of updating signature files must be commensurate with the value and sensitivity of the information at risk.

D. Back-Up, Storage, Restoration

Local Information Service Providers must develop and maintain plans to meet the IT backup and recovery requirements of the Local Agency they support.

Procedures and requirements of the plan include:

1. Ensuring backups are protected from being destroyed or read by unauthorized personnel;

2. Storing a full backup copy in an environmentally protected, access-controlled, off-site storage location;

3. Ensuring backup procedures and implementing activities (recording, retaining, and purging) comply with the California Public Records Act and County/Local Agency retention schedules; and

4. Performing and documenting regularly scheduled restoration tests to ensure backup data can be recovered.

E. IT Resource Monitoring

Administrative Policy 9-2: Information Technology Use and Security Policy manual Section IV.B. *Use of Local Agency IT resources and Data* establish the Local Information Service Provider's right to monitor and log all activities on the IT resources they own, control or manage for security, network maintenance and/or policy compliance.

1. Where technically feasible, audit logs recording policy exceptions and other security related events must be

produced and kept to assist in future investigations and access control monitoring.

2. All logged events must reflect accurate date and time stamps.

3. All audit logs must be retained in accordance with Local Information Service Provider standards.

4. All audit logs must be classified as restricted data and protected accordingly.

5. Review of audit logs must be commensurate with the nature and degree of criticality of the Local Agency IT resources and data involved.

XI. Physical and Environmental Security Policy

This Policy establishes requirements for physical and environmental security controls.

A. Facility Controls

Physical and environmental security controls for each facility must be reasonable and commensurate with the nature and degree of criticality of the Local Agency IT resources and data involved.

B. Secure Perimeters

Security perimeters must be used to protect areas that contain Local Agency IT resources and data. Security perimeters include, but are not limited to, entry point with proximity card access, locked doors, walls, staffed reception areas or other physical barriers.

C. Physical Entry Controls

1. Facilities housing Local Agency IT resources and data must be protected by entry controls to ensure only authorized individuals are allowed to access.

2. Public areas and other points of entry (e.g., exterior doors, loading docks) that could be used by unauthorized individuals must be controlled; and if possible isolated from data centers to avoid unauthorized access.

D. Environmental Controls

Local Agency IT resources and data must be protected against environmental threats. Controls must be applied and provide for:

1. Prevention, detection, and suppression of fires;

2. Prevention, detection, and minimization of water damage; and

3. Protection, detection, and minimization of loss or disruption of business operations due to electrical power fluctuations or failure.

E. Control Monitoring

Physical access and environmental controls must be monitored, tested and maintained regularly.

F. IT Resource Infrastructure Security

The physical IT resource infrastructure must be protected. Protective controls commensurate to the risk of losing confidentiality, integrity, or availability must be applied to:

1. The physical components of the network, including but not limited to data centers, wiring closets, server rooms and storage facilities where Local Agency IT resources are stored; and

2. Supporting facilities such as electrical supply and cabling infrastructure.

G. IT Resource Maintenance

Local Agency IT resources must be maintained to ensure their continued availability and integrity.

H. Off-Site Locations

Off-site refers to locations (e.g., home, leased locations) where Local Agencies do not have the authority to establish physical and environmental controls. To ensure the security of Local Agency IT resources located off-site, controls must be applied reasonable and commensurate with the nature and degree of criticality of the Local Agency IT resources and data involved, including, but not limited to

1. Authorization of Local Agency IT resources located off-site;

2. Recording of off-site authorizations and inventory of Local Agency IT resources located off site; and

3. For Users authorized to take Local Agency IT resources off-site; provide awareness of their responsibilities to protect Local Agency IT resources and data, and of security risks associated with off-site locations.

XII. Technical Vulnerability Management Policy

This Policy ensures that relevant security vulnerabilities are identified, evaluated and corrected through an appropriate risk management process.

A. Control of Technical Vulnerabilities

Local Information Service Providers must establish and maintain a process for detecting and remediating vulnerabilities. The process must include:

1. Monitoring independent security research and vendor announcements for the availability of security updates.

2. Developing risk appropriate criteria for the timely application of vendor security updates taking into consideration:

   (a) The purpose of the system being patched, its criticality, and the level of patch support provided by 3rd party line of business application vendors;

   (b) The history of the system being patched, in particular, any unplanned outages that occurred as a result of previously applied patches;

   (c) The impact of successful exploits of the vulnerability on the security of client data and County of Sonoma business operations should the update not be applied;

   (d) The categorization of any Local Agency data maintained on affected systems (e.g. Confidential or Restricted).

3. Maintaining risk assessment reports of systems that cannot be remediated.

XIII. Third Party Security Policy

This Policy establishes information security requirements for Third Party agreements and access to Local Agency IT resources and data.

A. Third Party Access

1. The Data Owner/Steward or designee must authorize physical or logical access by third parties in advance. This access must adhere to the Principle of Least Privilege, which allows only the access needed to perform their duties.

2. Third party devices must be configured to all applicable Local Agency and County policies and standards before being allowed to connect to a Local Agency network.

3. Third party personnel requiring access to Local Agency IT resources and data must adhere to all applicable Local Agency and County policies

B. Third Party Service Delivery Agreements

To implement and maintain the appropriate level of information security and service delivery, agreements with third parties must be established and include the following:

1. Necessary controls to ensure Local Agency IT resource and/or data protection;

2. A clear and specific process of change management;

3. Agreements for reporting, notification and investigation;

4. Levels of acceptable/unacceptable service and service continuity;

5. Definitions of verifiable performance criteria;

6. Rights to monitor and audit activities;

7. Problem resolution processes, including escalation steps;

8. Intellectual property rights and ownership of data;

9. Policies regarding subcontractors;

10. Conditions for renegotiation/termination and

11. Establishment of Third Party agreements must also adhere to guidelines set forth in County of Sonoma Purchasing policies (7-1 & 7-2) and procedures.

C. Third Party Exchange of Information Agreements

To maintain the security of information exchanged with any Third Party, agreements must be established and include the following:

1. Evaluate the sensitivity of the Local Agency data to be released or shared;

2. Identified responsibilities of each party for protecting the Local Agency data;

3. Identified responsibility and liability of each party in the event of an information security incident;

4. Minimum security controls required to transmit and use the Local Agency data;

5. Security measures that each party has in place to protect the Local Agency data;

6. Methods for compliance measurements;

7. A schedule and procedure for reviewing the security controls.

D. Insurance Requirements

Third Party agreements must incorporate insurance requirements as determined by County of Sonoma Risk Management standards.

E. Background checks, and Non-Disclosure Agreements

1. All third party personnel must sign a Non-Disclosure Agreement.

2. As required, Local Agency verification of a background check for all third party personnel accessing Confidential or Restricted data.

XIV. User Access Management Policy

This Policy establishes how User access privilege to Local Agency IT resources and data must be assigned and managed

A. User Registration

Local Information Service Providers must establish and document User registration and de-registration procedures for granting and revoking access to Local Agency IT resources and data.

B. User Access Authorization

User access to Local Agency IT resources or data must only be authorized by a Data Owner, Data Steward or designee.

C. Minimum Necessary Access

1. Access to and use of Local Agency IT resources and data must adhere to the Principle of Least Privilege, which requires that each User be given no more privilege than necessary to perform their work assignment.

2. Access to Confidential data is limited to those permitted under law, regulation, and with a need to know, as identified by the Data Owner.

D. Privileged Accounts Management

The issuance and use of privileged accounts must be restricted and controlled. Processes must be developed to ensure that uses of privileged accounts are monitored, and any suspected misuse of these accounts is promptly investigated.

E. User Identification (ID) and Authentication

1. All Users must be assigned a unique User ID to establish accountability.

2. All User IDs must have a password that adheres to Local Information Service Provider standards.

3. All User IDs must have an authentication technique (e.g., knowledge, token and/or biometric-based).

4. Individuals, whose work assignment requires elevated privileges, must be issued an additional unique ID. Regular User activities (e.g., e-mail or word processing) must not be performed from privileged accounts.

5. Individual User IDs must not give any indication of the User's work assignment or privilege level, (e.g., Admin, SuperUser, and Manager).

6. Shared User IDs may only be created and assigned to support the functionality of a process, system, device or application. To establish accountability, each shared User ID must have a designated owner.

7. Guest User IDs are not allowed except where explicitly needed to satisfy a valid business requirement (i.e., public kiosk, public web site, etc.).

F. Suspension of Access

User IDs must be disabled according to Local Information Service Provider standards.

G. Access Modification

If a User's work assignment changes within a Local Agency, access must be reviewed and modified commensurate with the User's new work assignment.

H. Termination of Access

1. Access to Local Agency IT resources and data must be terminated when the User ceases to be a member of the County workforce.

2. Data Owners/Data Stewards/Designees must terminate a User's access to Local Agency IT Resources and Data when the work assignment no longer requires access.

I. Access Review

User access privileges must be periodically reviewed by the Data Owner/Data Steward or designee to ensure access is commensurate with the work assignment. Local Information Service Providers must provide reports of User access privilege to Local Agencies.

XV. Compliance Policy

This Policy establishes the requirements for Policy compliance activities relevant to information security.

A. Security Process Review

Local Information Service Providers must regularly review security processes to ensure compliance with relevant security policies and standards.

B. Technical Compliance

Local Information Service Providers must regularly check information systems for compliance with security policies and standards, including but not limited to penetration tests and vulnerability assessments.

C. Independent Compliance Reviews

Independent reviews of information security should be regularly conducted.

D. Information Systems Audit Controls

1. Audit controls must be used in such a way to minimize risk of disruption to the production environment.

2. Access to audit tools must be limited to prevent misuse or compromise.

Appendix A – Information Security Laws and Standards

I. Federal Laws

A. Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Congress enacted HIPAA, in part, to protect the privacy and security of protected health information (PHI) maintained by covered entities. Covered entities include most healthcare providers (i.e., those who use HIPAA- mandated electronic codes for billing purposes), health insurance companies, and employers who sponsor self- insured health plans. The U.S. Department of Health and Human Services (HHS) is responsible for enforcing HIPAA. The two principal sets of regulations issued by HHS to implement HIPAA are the Standards for Privacy of Individually Identifiable Health Information (the "HIPAA Privacy Rule") and the Security Standards for Individually Identifiable Health Information (the "HIPAA Security Rule"). The HIPAA Privacy Rule requires covered entities to implement policies and procedures to ensure that (a) workforce members use and disclose PHI only for permissible purposes and (b) patients and insureds can exercise their HIPAA-mandated rights, such as the rights to access and to amend PHI. The HIPAA Security Rule requires covered entities to implement policies and procedures to ensure the confidentiality, integrity, and availability of PHI in electronic form; to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI; and to protect against reasonably anticipated uses or disclosures of electronic PHI in violation of the HIPAA Privacy Rule.

B. Health Information Technology for Economic and Clinical Health (HITECH) Act

The HITECH Act, effective February 17, 2010 supplements the requirements of the HIPAA Privacy Rule and the HIPAA Security Rule. The Act requires covered entities to notify patients and insureds whose PHI is compromised by a security breach. It extends many of the requirements of the HIPAA Privacy Rule and the HIPAA Security Rule to vendors — such as insurance brokers, billing services, and third-party administrators — who create or receive PHI when providing services to covered entities. The HITECH Act increases the penalties that HHS can impose on a covered entity for violating HIPAA or its implementing regulations.

II. State of California Laws

A. Data Breach Notification Law (CA Civil Code 1798.29)

California's Data Breach Notification Law requires any agency that owns or licenses computerized data that includes personal information to disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

B. Social Security Numbers Protection (CA Civil Code 1798.85-1798.89)

Limits the use of social security numbers by restricting public posting and display to others, e.g., in printed or mailed materials unless required by law, on identification cards, and over the Internet without proper security measures.

C. California Public Records Act (Government Code 6250-6276.48)

The California Public Records Act (PRA) established in 1968, describes what information is available to the public. The PRA also defines required communications to the requestor and the records that are confidential under law and therefore, exempt from disclosure.

III. Standards

A. Payment Card Industry Data Security Standard (PCI DSS)

PCI DSS is an information security standard for organizations that store, process and transmit card holder data.

B. Federal Bureau of Investigation Criminal Justice Information Services Standard (FBI CJIS)

CJIS is an information security standard for organizations that store, process and transmit Criminal Justice Information.

C. International Organization for Standardization (ISO) 27002

ISO 27002 is an information security standard that provides best practice recommendations on information security management.

County of Sonoma
Information Technology Professional
Policy Manual
Acknowledgment

I acknowledge that I have received, have been given the opportunity to read and will comply with the County of Sonoma Administrative Policy# 9-4 – Information Technology Professional Policy Manual, issued on_____”

I understand I have the obligation to know the responsibilities to maintain the security of Local Agency IT resources and data associated with my role(s) as defined in this Policy manual.

I further acknowledge that the County of Sonoma retains the right to examine all electronic storage media, data files, logs and programs used on County of Sonoma computer systems and equipment.

_____ _____

Print Name Signature

_____ _____

Local Agency Date

County of Sonoma
Security Policy/Standard Waiver

Local Agency Name: _____ **Date**: _____

Waiver Requester Name/Title: _____

Phone Number: _____ **Email:** _____

County Policy/Standard: _____

Exception Scope:
Identify the scope of the exception being requested (i.e., for all systems/Users? One system/group of Users:

Justification for Exception:
Explain why compliance with this policy/standard is not possible due to technical limitations, conflict with business requirements, or other circumstances:

Exception Risk
Explain the potential impact or risk attendant upon granting the exception:

Compensating Controls
In the absence of the controls specified by this policy/standard, what compensating controls will be implemented?

Approval and Conditions

I, hereby, acknowledge that I have reviewed the aforementioned request for a policy/standard waiver and certify that the compensating controls necessary to justify the policy/standard waiver are adequate.

[1]County Chief Information Security Officer or approved designee	Date
Local Agency Department Head, General Manager or approved designee	Date

Upon approval, scan and e-mail to issc@sonoma-county.org. The approver shall retain the original.

Please note: This waiver and its applicability must be reviewed at least annually by the requesting Local Agency. Waivers must be renewed every three years or when significant changes which affect the system categorization e.g., Confidential, Restricted or Public), justification for noncompliance and/or compensating controls are made.

[1] In most cases, the Information Systems Director who serves as the Chief Information Security Officer will be the appropriate approver, unless otherwise noted in the individual policy or standard for which the waiver is submitted.

Information Technology and Security Terminology Glossary

Accountability - The system's ability to determine the actions and behavior of a single user within a system. Accountability shows that a particular user performed a particular action. Audit logs and monitoring are used to track a user's activity.

Administrative Measures – Defines and guides an individual's actions to preserve the security of IT resources and data; e.g., policies, procedures, security awareness training. Also referred to as administrative controls.

Administrator Accounts - Accounts that have elevated privilege to IT resources. Such accounts have the capability to circumvent security controls, configure systems, and may create other accounts as well as assign access rights to them. These accounts are limited to staff whose business function requires the use of such an account.

Availability - Ensures information is accessible to authorized users when required.

Authentication - A procedure to unambiguously establish the identity of a user, machine, device or application process before allowing access to an information resource. Authentication is typically with a password but other credentials such as digital certificates may be used

Authorization - Determines which IT resources, User, machine, device or application process is entitled to access.

Back-Up - The process of making copies of data to be used in the event of a data loss.

Breach Notification - Notification required to individuals or agencies in the event of a data breach.

Change – Any notable alteration to a system, data, and/or its configuration that could affect information security, compliance and reliable service delivery.

Compliance - Ensures compliance with laws and regulations and County policies, standards and procedures relevant to information security.

Confidential Data - Information protected from use and/or disclosure by law, regulation or standard, and for which the highest level of security measures are required.

Confidentiality - Ensures information is accessible to only those authorized to have access.

Controls – Administrative, technical, or physical measures and actions taken to try and protect systems, includes safeguards and countermeasures.

Countermeasures – Controls applied to mitigate risk; reactive in nature.

County – The County of Sonoma

Credit Card Information – Credit card number (primary account number or PAN) and one or more of the following: cardholder name, service code, expiration date.

Data – Local Agency information that is stored, processed,or transmitted in electronic, optical or digital form.

Data Breach – An information security incident in which confidential data is copied, transmitted, viewed, stolen or used by an unauthorized individual.

Data Center - Centralized storage facility that houses computer, network and telecommunications equipment.

Data Classification – A method of assigning a level of sensitivity to data to determine the extent to which it needs to be controlled and secured.

Data Custodian – Individual responsible for maintaining the confidentiality, integrity and availability of data.

Data Owner – Local Agency Department Head/General Manager or other individual authorized by law, regulation or policy to collect and manage the data that supports their business operations.

Data Steward – Individual assigned by the Data Owner to protect the confidentiality, integrity, and availability of the data that supports their business operations.

Decryption – The process of converting encrypted data back into its original form, so it can be understood.

Designee – Individual designated by a Local Agency Department Head/General Manager to perform some duty or carry out a specific role.

Efficiency - Ensures that implemented security safeguards do not unduly interfere with efficient and effective service delivery.

Electronic Protected Health Information (ePHI) – Individually identifiable health information that is transmitted by electronic media, or maintained in electronic media.

Elevated Privilege – Administrative permission to IT resources. See also – Administrator Accounts.

Encryption - A process that transforms readable data into a form that appears random and unreadable to unauthorized users.

Exploit - A process or tool that will attack a vulnerability in an asset.

Guest Account – Also, known as a Guest User ID, used to access very limited network resources (i.e., the Internet).

Guidelines – General recommendations or instructions that provide a framework for achieving compliance with information security policies.

High-Risk application – The loss of confidentiality, integrity, or availability of the data or system that could have a significant adverse impact on the county's operations.

Identification - Means to distinguish individual Users, machines, devices and application processes. Multiple identifiers can be associated with a given subject for different purposes. An individual user, for example, may be known by an account name in a Windows domain, by the distinguished name on a digital certificate or by a Windows issued security identifier.

Information Security Incident – An Information Security Incident is defined as any adverse event that compromises the security of Local Agency IT resources or data, or otherwise violates Local Agency or County Information Security Policy.
Information Security Incidents may involve:

- Attempts (either failed or successful) to gain unauthorized access to Local Agency IT resources
- Unwanted disruption or denial of service
- Unauthorized or inappropriate use of Local Agency IT resources
- Unauthorized change to a Local Agency IT resource's hardware, firmware or software
- Virus, worm or other malicious code attacks
- Loss, or unauthorized disclosure, use or access of Confidential Data
- Compromised User account or password

- Loss or theft of any Local Agency IT resource

Information Security Representative – Individual designated by Local Agency Department Head/General manager to coordinate information security within their Local Agency.

Information Security Steering Committee - Coordinating body for all County information security-related activities and is composed of the County Privacy Officer, Information Security Officer and individuals designated by the IT Governance Council.

Information System - A combination of IT resources, procedures, and people that collect, record, process, store, transport, retrieve or display information for a specific purpose.

Information Technology (IT) Resources - Information Technology (IT) resources include but are not limited to the following:

- Computers and any electronic device including personally owned devices, authorized for use by the Local Agency, which create, store or process Local Agency data, such as:
    - Servers, workstations, desktops, mainframes, copiers, faxes, related peripherals;
    - Mobile Devices
        - Portable computers such as laptops, notebooks, netbooks, and tablet computers
        - Portable storage media such as tapes, compact disks (CDs), digital versatile disks (DVDs), flash drives, and universal serial bus (USB) drives
        - Smart Phones, pagers, digital cameras, cell phones, digital voice recorders
- Electronic messaging systems e.g., electronic mail (e-mail), instant messaging;
- Network connections (wired and wireless) and IT infrastructure including, routers, switches, firewalls and;
- County licensed or developed software

Information Technology (IT) Resource Owner - Individual assigned from within the Local Agency who is responsible for ensuring appropriate protection from unauthorized use, access, disclosure, modification, loss or deletion.

Integrity – Ensures information is complete, accurate and protected against unauthorized modification.

Litigation Hold - A process used by the County of Sonoma to preserve all data that may relate to a legal action.

Local Information Services Provider – Provider of network infrastructure, network access, data storage or e-mail services to Local Agencies. This refers to the County Information Systems Department, Human Services Department Information Integration Division, Sonoma County Sheriff's Office Technical Services Bureau, and County Water Agency Computer Application and Instrumentation Support Section.

Logical Measures – Please see technical measures.

Logon Banner - Notice presented to an individual prior to accessing County IT Resources, which prohibits unauthorized access, and includes notice of monitoring and recording an individual's activities.

Malicious Software (Malware) – Programming or files developed for the purpose of doing harm. Malware includes, viruses, worms, Trojan horses, etc.

Mobile Devices - The following is a representative and non-inclusive list of mobile devices:

- Portable computers such as laptops, notebooks, netbooks, and tablet computers
- Pagers, digital cameras, cell phones, digital voice recorders
- Portable storage media such as tapes, CDs, DVDs, flash drives, and USB drives
- Smart Phones

Notice Triggering Data – Data if breached requires notification to individuals and/or agencies.

Patch - Software to repair a defect in an operating system, application or device.

Personal Information – Information containing any of the following in combination with a first initial or first name and a last name:

- Social Security number;
- driver's license number or California Identification Card number;
- an account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account;

- medical information, including any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional or;
- health insurance information.

Physical Measures – Controls the physical access to preserve the security of IT resources and data; e.g., locked doors, surveillance cameras, proximity identification cards. Also referred to as physical controls.

Piggybacking - The attempt to gain physical access that has not previously been authorized i.e.; one person following another without individually swiping his or her Proximity Identification Card.

Policy – High level statements providing information security directive and mandates for the County workforce.

Privilege – Access rights or permissions to IT resources/data.

Public Data - Information that is available for general access without review by the Data Owner and/or County Counsel.

Procedure – Step-by-step instructions for reinforcing information security policies.

Restricted Data - Information that requires special precautions to protect from unauthorized use, access, or disclosure.

Risk Assessment – The process of determining the likelihood that a specific negative event will occur.

Safeguards – Controls applied to mitigate potential risk; proactive in nature.

Security – Preservation of the confidentiality, integrity and availability of IT resources and data.

Security Incident Response Team – Individuals responsible for the investigation and mitigation of information security incidents.

Security Measures – A combination of controls and safeguards to preserve the security of IT resources and data.

Sensitive Information – Information classified as either Confidential - Information protected from use and/or disclosure by law, regulation or standard, and for which the highest level of security measures, or Restricted - Information that requires special precautions to protect from unauthorized use, access, or disclosure.

Shared Account (also known as a Shared User ID) – Account shared among more than one individual for a specific business purpose (i.e., an e-mail resource/calendar).

Standards – Defined minimum requirements to ensure compliance with an information security policy.

Store – The placement of data in either temporary or permanent memory (that is, in “storage”), such that the information can be accessed or retrieved.

Strong passwords- Passwords provide the first line of defense against unauthorized access to your computer. The stronger your password, the more protected your computer will be from hackers and malicious software. Passwords may not contain two consecutive characters of the user's full name or User ID (Account Name).
The strong password contains characters from three of the following categories:

- Password must be 8 characters in length.
- Passwords must combine three or more of:
- Uppercase letters of European languages (A through Z)
- Lowercase letters of European languages (A through Z)
- Base 10 digits (0 through 9).
- Non-alphanumeric characters (special characters) (for example, !, $, #, %)
- Any Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase.

Technical Measures –Utilizes technology to preserve the security of IT resources and data, e.g., anti-virus software, encryption, firewalls. Also referred to as logical controls.

Third-Party – Any non-County individual or organization that develops, installs, delivers, manages, monitors, or supports any IT Resource.

Threat - Any potential danger to an IT Resource.

User – Workforce members authorized to access Local Agency IT Resources.

User Provisioning – Creation, maintenance, privilege assignment and deactivation of individual accounts.

User ID – Unique identifier assigned to an individual, for example, JSMITH.

Vulnerability - A flaw or weakness in system security procedures, design, implementation, or internal controls that might be exercised (whether accidentally

or intentionally) and cause a security breach or a violation of the system's security policy.

Workforce – Employees or any other individual performing work on behalf of or with approval of Local Agencies.

Development and Revision History

Version	Date	Chapter/Section	Details
1.0	3/2014	All	New Policy manual entitled IT Professionals
2.0	1/2016	Glossary	Added strong password and high risk application in the glossary
		Page 26	Insurance requirements: Added web-links that reference current risk management standards
		Page 26	Third Party agreements Added web links that reference current purchasing policies
3.0	5/13/2016	Page 34	Added Acknowledgement and signature page
4.0	6/28/2016	Page 35	Added Local Department Head or /General Manager signature under security policy waiver