Administrative Policy 9 - 2

Information Technology Use

And

Security Policy

Manual

For an accessible version of this content, please see http://sonomacounty.ca.gov/CAO/Administrative-Policies/IT-Use-and-Security-Policy/

(This page intentionally left blank)

Table of Contents

Information Technology Use and Security 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:

Origination Date:

Purpose

This Policy manual provides directives to all users on the general use and protection of Local Agency IT resources and data.

Scope

This Policy manual applies to all Local Agencies. Where a conflict exists between this Policy manual and a Local Agency's policy, 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.

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, risk mitigation measures to be undertaken by the Local

Agency, initiatives, actions and a time frame for achieving the minimum compliance level with the policies set forth herein. The ISSC will review such requests, confer with the requesting Local Agency and forward to the CISO along with a recommendation for action.

Adverse Action

Failure to comply with this Policy manual may result in disciplinary action up to, and including termination, in accordance with County Civil Service Rules, or a Local Agencies' separate and distinct disciplinary rules and procedures

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 the 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/IEC 27002 (Code of Practice for Information Security Management framework) and to meet County compliance obligations. This manual together with the IT Professional Policy manual establishes the foundation for information technology and security in the County to assure appropriate and authorized access, usage and integrity of information.

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. 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. Users

Users are all workforce members (employees or any other individual performing work on behalf of, or with approval of Local Agencies) authorized to access Local Agency IT resources and are responsible for:

1. Complying with County Information Technology and Security policies;

2. Maintaining the security of Local Agency IT resources and data associated with their role(s) as defined in this Policy manual;

3. Storing original Local Agency data on the Local Agency network to ensure compliance with County or Local Agency records retention policy,

4. Protecting Sensitive information against loss, unauthorized use, access, or disclosure, by the following:

    a. Using Sensitive information only for the stated legal and/or business purpose.

    b. Disclosing Sensitive information as permitted by law or with the express consent of the Data Owner.

    c. Not making copies of Sensitive information except as required in the performance of assigned duties.

    d. Keeping Sensitive information out of plain sight.

5. Not sharing User accounts and passwords;

6. Creating, changing and storing passwords in accordance with established policies and standards;

7. Locking or logging off unattended workstations.

8. Using only assigned Local Agency electronic messaging accounts, i.e., e-mail, to conduct Local Agency business communication, and refraining from conducting Local Agency business with personal electronic messaging accounts (e.g., Yahoo, Gmail). Law enforcement and/or other Local Agency workforce may be exempted from these restrictions during the performance of legitimate job responsibilities;

9. Not violating copyright law, and conforming to software licensing restrictions by:

    Only using software that has been installed by their Local Information Service Provider or other authorized individual.

10. Not engaging in any use of Local Agency IT resources that violates federal, state, local laws, Local Agency or County policy;

11. Reporting any known or suspected information security incident to their manager/supervisor, Information Security Representative or Local Information Service Provider;

12. Compliance with VII. Mobile Computing Policy if using a mobile device to work on or access Local Agency IT resources or data.

B. Local Agency Department Head/General Manager

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

1. Enforcing this Policy manual within their Local Agency;

2. Ensuring all Users of Local Agency IT resources and data are made aware of County information technology and security policies and that compliance is mandatory;

3. Ensuring all Users receive education regarding their security responsibilities before accessing Local Agency IT resources and data;

4. Establishing supplemental information technology and security policies, standards, procedures, or guidelines as needed for their business purposes, provided they are not less restrictive than County policies. Prior to final approval Local Agency Department Head/General Manager and/or Designee are responsible for:

   a. Providing supplements to Human Resources for review.

   b. Providing notice to employee organizations regarding any proposed supplements; and

   c. Providing supplements to Local Agency's Local Information Service Provider to review for consistency with County/Local Agency IT security policies.

5. Provide training in support of established procedures and guidelines

6. Obtaining a signed acknowledgment from Users that they have had an opportunity to read and will comply with this Policy manual before accessing Local Agency IT resources and data;

7. Designating or serving as an information security representative; and

8. Submitting to the ISSC any needed requests for exceptions to this Policy manual.

C. 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;

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

D. 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 policies and standards;

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

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

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

E. 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, this 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.

F. Information Security Steering Committee

The Information Security Steering Committee (ISSC) 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 annually and policy waivers.

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.

G. HIPAA County Privacy Officer

The HIPAA County Privacy Officer is responsible for:

1. Making required publication, consumer notice and regulatory filing, in response to data breaches involving Electronic Protected Health Information (ePHI) and/or personal information.

H. 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 they own 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;

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; and

5. Designating or serving as the Data Steward.

I. 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.

J. 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. Information Technology and Security Governance Policy

This Policy serves as the governing policy for Information Technology and Security. Security measures for Local Agency IT resources and data must be implemented to provide:

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

2. Authentication – Establishes the identity of the sender and/or receiver of information.

3. Data Integrity - Ensures information is complete, accurate and protected against unauthorized modification.

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

5. Accountability - Ensures correct use and individual responsibility of Local Agency IT resources and data.

6. Auditing - Ensures the collection of data and processes to provide assurance of the effectiveness of controls.

7. Appropriate Use – Ensures Users conform to County rules, ordinances, policies, state and federal laws.

IV. Use of Local Agency IT Resources and Data Policy

This Policy establishes acceptable use of Local Agency Information Technology (IT) resources and data.

A. <u>General Use and Ownership</u>

1. Access to Local Agency IT resources may be provided for conducting Local Agency business. Access may be wholly or partially restricted without prior notice or consent of the User.

2. The Data Owner retains the rights of ownership to all data created on IT resources, unless the legal ownership is otherwise defined by law.

3. Local Agency IT resources and data are to be used for conducting business authorized by and related to Local Agency operations.

4. Local Agency data must only be used for authorized purposes and must not be disclosed to anyone not authorized to receive such data.

5. All Users of Local Agency IT resources and data must sign an acknowledgment of this Policy manual prior to being granted access.

B. IT Resource Monitoring

1. Data Owners and/or Data Stewards with express consent of the Data Owner may monitor any and all aspects of Local Agency data access and use.

2. Local Information Services Providers may monitor and log all activities on the IT resources they own, control or manage for security, network maintenance, and/or policy compliance.

C. User Access Monitoring

1. Monitoring or investigating User access to Local Agency IT resources and data must be approved by the Data Owner, Data Steward or designee.

2. County Counsel approval with the express consent of the Data Owner is required for monitoring of User's work generated data files, Internet access logs, or electronic messaging (e.g., e-mail, and instant messaging).

3. Upon request by the Data Owner, Data Steward or designee, Local Information Service Providers may monitor or investigate User access to Local Agency IT resources and data, without advance notice to the User.

D. No Expectation of Privacy

Users have no expectation of privacy when using Local Agency IT resources, or in any data they access, create, store, send or receive on any Local Agency IT resources.

E. Public Records Act Compliance and Records Retention

1. Any records created while conducting Local Agency business using Local Agency IT resources, including personal and county provided mobile devices, may be subject to disclosure.

2. To ensure compliance with County or Local Agency records retention policy, original Local Agency data must be stored on the Local Agency network.

F. Use of Sensitive Information

Sensitive information as defined in this Policy manual is 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.

To protect Sensitive information against loss, unauthorized use, access, or disclosure the following must be adhered to:

1. Sensitive information must only be used or disclosed as permitted by law and/or policy.

2. Sensitive information that is not controlled by law or policy can only be disclosed with express consent of the Data Owner.

3. Copies of Sensitive information must not be made except as required in the performance of assigned duties.

4. Sensitive information must be kept out of plain sight and must not be displayed in any form when it is not being used.

5. Unattended workstations must be locked or have password protected screen savers enabled in accordance with Local Information Service Provider standards.

G. User Accounts and Passwords

1. User accounts and User passwords must not be shared.

2. User passwords may only be created, changed and stored in accordance with established policies and standards.

H. Use of Electronic Messaging

1. Users must only use assigned Local Agency electronic messaging accounts conduct Local Agency business, and are prohibited from conducting Local Agency business using personal electronic messaging services, social media accounts or email accounts (e.g., texting, Twitter, Facebook Messenger, Yahoo, Gmail). Law enforcement and/or other Local Agency workforce may be exempted from these restrictions during the performance of legitimate job responsibilities.

I. Use of the Internet

1. Local Agency IT resources that allow access to the Internet are provided to facilitate the effective and efficient use of Local Agency business. With Local Agency approval, Users are permitted access to the Internet to assist in the performance of their assigned duties, and must comply with all acceptable use described in this Policy and any other Local Agency or County Policy.

J. Personal Use/Union Use

Except as otherwise stated, reasonable and limited personal use of Local Agency IT resources or use of Local Agency e-mail between recognized County unions and Local Agency workforce is allowed under the following circumstances:

1. Does not involve unacceptable use as defined in section IV.N of this Policy or in any other County Policy;

2. Does not interfere with Local Agency IT resources and;

3. Does not interfere with the User's job performance and/or obligations as a public employee.

K. Use of Authorized Software

All software installation and use must conform to licensing restrictions. These products include those that are not appropriately licensed for use by the Local Agency or those that violate the rights of any person or organization protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software is prohibited.

1. Only software that has been installed by the Local Information Services Provider or other authorized individuals may be used.

2. Software purchased by the Local Agency must not be loaded on a personally owned device, unless specifically authorized by the Local Agency Department Head/General Manager and/or Designee and the manufacturers licensing agreement.

L. Use of Authorized Devices

1. To maintain the security of the Local Agency network, only devices authorized by the Local Information Service Provider may be connected. Any device found to be in violation of this Policy is subject to immediate disconnection from the Local Agency network.

M. Unacceptable Use

Any use which violates federal, state, local laws, Local Agency or County policies is prohibited. Law enforcement and/or other Local Agency workforce may be exempted from these restrictions during the performance of legitimate job responsibilities.

The following activities are prohibited on Local Agency IT resources; examples include, but are not limited to:

1. Representing yourself as someone else, real or fictional, or sending information anonymously;

2. Sending messages or accessing data with content that violates any county policies, rules or other applicable laws;

3. Sending messages or accessing data that contain inappropriate, defamatory, obscene, harassing or illegal material;

4. Sending information that violates or unlawfully infringes on the rights of any other person (including but not limited to copyrights and software licenses);

5. Engaging in activity that may harass, threaten or abuse others;

6. Conducting political activity, business for fraudulent activity, personal profit or gain, or other improper activities as defined in Local Agencies Incompatible Activities Policy;

7. Downloading, installing or running security programs or utilities such as password cracking programs, packet sniffer, or port scanners that reveal or exploit weaknesses in the security of Local Agency IT resources;

8. Engaging in activity that may degrade the performance of Local Agency IT resources;

9. Accessing or attempting to access Local Agency IT resources which have not been authorized;

10. Restricting or denying authorized Users access to Local Agency IT resources; and Circumventing Local Agency security measures.

V. Data Classification Policy

This Policy directs Local Agencies to classify their data to ensure the required security measures are applied.

Local Agencies may not rely on this Policy to make determinations or implement the requirements of the California Public Records Act (Government Code Sections 6250-6265).

A. Data Categories

Data Owners must classify Local Agency data into one of the following categories:

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

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

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

B. Data Classification Assignment

1. Default classification assignment for data is Restricted.

2. Any collection of data containing different classification assignments must be classified as a whole at the level applicable to the data with the highest assignment.

3. Classifications assigned to Local Agency data must be reviewed upon changing usage or law, and reclassified if necessary.

4. The classification level of replicated data must remain consistent with the original data.

C. Security Requirements

1. Each data category has security requirements based on law, regulation, common business practice, liability or reputational factors.

2. Security controls must be applied to each data category based upon the identified security requirements, and commensurate with the value of the information and risk of loss.

VI. Information Security Incident Management Policy

This Policy establishes requirements for reporting and responding to information security events and vulnerabilities.

A. Information Security Incident Reporting

1. Users must immediately report any known or suspected Information Security Incident (e.g., virus/worm attacks, actual or suspected loss or disclosure of confidential data) or system vulnerability to their manager/supervisor, Information Security Representative or Local Information Services Provider. Local Agencies must ensure that their Local Information Service Provider is informed.

   The above requirement does not authorize or condone an intentional search for system weaknesses and/or malfunctions.

B. Information Security Incident Response

Local Information Service Providers must have a current documented working plan for reporting on, responding to, recovering from and preventing recurrence of information security incidents. The plan must be labeled Confidential and distributed on a need-to-know-basis.

The plan must incorporate the following practices:

1. Collection and protection of evidence, to include a chain-of-custody;
2. Documentation of information security incidents;
3. Implementation of remediation strategies;
4. Notification to the County Privacy Officer of information security incidents involving actual or suspected loss or disclosure of electronic protected health information (ePHI);
5. Notification to the Data Owner of information security incidents involving actual or suspected loss or disclosure of personal information;
6. Reporting to the Chief Information Security Officer (CISO) and or authorized designee and
7. Application of lessons learned from incidents.

VII. Mobile Computing

This section establishes requirements for the use of mobile devices (both personally owned and Local Agency provided) to work on or access Local Agency resources and data.

A. Personally Owned Devices

Personally-owned devices include, but are not limited to, smartphones, laptops, notebooks, tablets(e.g. iPads, Android) including, but not limited to

any such devices for which Staff Development or other similar County-provided funds were used to purchase the device in whole or in part.

1. The Expectation of Privacy: The County of Sonoma will respect the privacy of a user's voluntary use of a personally-owned device to access Local Agency IT resources. Users cannot be required and/or can refuse to use their personally-owned devices to work on or access Local Agency resources.

2. The County of Sonoma will only request access to the personally-owned device and password in order to implement security controls; to respond to litigation hold (aka e-discovery) requests arising out of administrative, civil, or criminal directives, Public Record Act Requests, and subpoenas; or as otherwise required or permitted by applicable state or federal laws. Such access will be performed by an authorized Local Information Service Provider technician or designee using a legitimate software process.

3. Users should receive prior approval from their manager to use their personally owned mobile device to access Local Agency IT resources or data.

4. Users should be aware that the Data Owner retains ownership of Local Agency data created or stored on their personally-owned device. Users should also be aware that they can view but not store and/or download confidential or restricted data when technically feasible on their personally owned device.

5. Users are responsible for backing up their personal data, settings, media, and applications on their personally owned device.

6. Users should be aware that some personally owned devices may require the purchase of a software application and corresponding software license and/or subscription, to allow the device to comply with County and/or Local Agency policy and/or standards, and that they may be responsible for all costs of required software applications.

7. Users are responsible for maintaining their personally-owned device with the manufacturer's security and operating system updates.

8. Users will not install software on their personally owned device that bypasses the built-in security features and controls.

9. Users should use the built-in encryption feature on their personally-owned device when available.

10. Users should remove Local Agency data from their personally-owned device, prior to removing access to Local Agency IT resources or data, leaving county employment, or disposing of their personally-owned device.

11. Users should be aware that it is their responsibility to immediately report a lost or stolen personally-owned device to their manager/supervisor and Local Information Services Provider. Users should be aware that if their personally-owned device is lost or stolen, their personally-owned device will attempt to be remotely wiped of all data.

12. Users should be aware that is their responsibility to setup their individual cellular plan with their provider and to pay all or a portion of the charges incurred, in accordance with applicable law. Any service or billing issues with the cellular or data provider may be the user's sole responsibility and obligation.

13. Physical Protection: Unattended mobile devices must be physically stored in a safe and secured manner.

B. Local Agency Provided Devices

1. The Data Owner retains the right of ownership to all data created or stored on mobile devices in support of Local Agency business.

2. Use of a mobile device to work on or access Local Agency IT resources and data must be first approved by the User's supervisor/manager based on its benefit to Local Agency operations.

3. The Local Agency may install security controls to manage the local agency provided mobile device.

4. Right to IT Resource Monitoring: The Local Information Service provider has the right to monitor any and all aspects of Local Agency data access and use from mobile devices.

5. Physical Protection: Unattended mobile devices must be physically stored in a safe and secured manner.

6. Users of mobile devices accessing or storing Local Agency data must comply with all applicable local, state and federal laws related to the use of mobile devices.

7. Remote Access: All users authorized to connect remotely to any Local Agency network and access Local Agency IT resources and data via the Internet must do so via the appropriate encrypted connection, such as a virtual private network or other secure method (e.g. SSL or TLS).

8. Data Security Measures: All users of mobile devices must employ security measures in accordance with their Local Information Service Provider standards.

9. Disposition: Local Agencies must ensure that prior to reuse, recycle, or disposal of any mobile device, that Local Agency data is removed. Any mobile device assigned to an employee no longer employed by the county that was used to access or store Local Agency data must be remotely wiped of all data. Loss or Theft: The loss or theft of any mobile device used to access or store Local Agency data must be reported as soon as possible to the User's manager/supervisor, Information Security Representative or Local Information Services Provider.

VIII. Security Awareness Training and Education Policy

This Policy defines the criteria for security awareness training and education in all Local Agencies.

A. Security Awareness Training

Security awareness training is designed to educate Users of their responsibilities to protect Local Agency IT resources and data, and to provide the knowledge and skills necessary to fulfill IT security responsibilities for the Local Agency.

1. Users must be made aware of County/Local Agency information and technology security policies and their security responsibilities, prior to accessing Local Agency IT resources and data.

2. Users must receive appropriate security awareness training and education relevant to their assigned job function, addressing topics including:

    a. Appropriate use of Local Agency IT resources and data;

    b. Responsibilities to report and/or respond to Information Security incidents;

    c. Incident response procedures;

    d. Expectation of privacy;

    e. Right to monitor;

    f. Ownership and classification of data;

    g. Personally owned devices; and

h. Virus and malicious code protection.

3. Users will have their security awareness training not less than every two years or upon a change in their access to Local Agency IT resources and data.

4. As applicable, Users must be informed of updates and/or changes to County/Local Agency Information Technology Security Policies.

5. Users must be provided periodic reminders that cover general security topics.

6. Records of User security awareness training must be documented and maintained by the Local Agency Department Head/General Manager or Designee.

County of Sonoma
Information Technology and Security
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 9-2 – Information Technology Use and Security Policy Manual, issued on December 12, 2017.

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 understand that if I voluntarily use my personally owned device to access Local Agency IT resources and data that I will comply with the personally owned section of the Mobile Computing Policy section on page 19.

I further, acknowledge that my use of Local Agency IT resources and data may be monitored, and that I have no expectation of privacy when using Local Agency IT resources or in any data I access, create, store, send or receive on any Local Agency IT resources.

_____ _____

Print Name Signature

_____ _____

Local Agency Date

Appendix A - Guidelines

I. Data Classification

The Data Classification policy of this manual directs Local Agencies to identify and classify Local Agency data.

These Guidelines provide examples to assign the appropriate data classification.

	Confidential **(highest level of sensitivity)**	**Restricted** **(moderate level of sensitivity)**	**Public** **(low level of sensitivity)**
Description	Information protected from use and/or disclosure by law, regulation or standard, and for which heightened security measures are required.	Information maintained that requires special precautions to protect from unauthorized use, access, disclosure, modification, loss, or deletion.	Information that is available for general access without review by the Data Owner and/or County Counsel.
Data Breach notification requirements	Yes. Notification required for unencrypted data. Mandated reporting and notification are not required for encrypted data.	No data breach notification requirements for Restricted data.	No data breach notification requirements for Public data.
Reputational Risk	High	Medium	Low
Disclosure Requirements	Confidential data must not be disclosed without proper prior consent from the Data Owner and/or County Counsel. To prevent inappropriate disclosure; removal, redaction, de-identification or masking of Confidential data may be required.	Restricted data must not be made available for general public access without the consent of the Data Owner and/or County Counsel. To prevent inappropriate disclosure; removal, redaction, or masking of Restricted data may be required.	Subject to Local Agency policies, Public data may be disclosed without review by the Data Owner or County Counsel

	Confidential **(highest level of sensitivity)**	**Restricted** **(moderate level of sensitivity)**	**Public** **(low level of sensitivity)**
Common Data Elements **(not all-inclusive)**	Personal Information as defined by California Civil Code Section 1798.82: An individual's first name or first initial and last name in combination, with any one or more of the following: • Social Security Number • Driver's license number • California Identification (ID) number • 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 • Health insurance information	Network/Systems Data Event logs Risk assessments Disaster recovery plans Configurations Employee Data Employee ID numbers Employee applications	Business Data Job postings Board Agendas and Meeting Minutes Maps Budget Administrative Policies Employment Data Salary Job Classification Memorandum of Understanding

	Confidential **(highest level of sensitivity)**	**Restricted** **(moderate level of sensitivity)**	**Public** **(low level of sensitivity)**
	• Cardholder Information Credit card number/primary account number and one or more of the following: • Cardholder name • Security Code • Expiration date Peace Officer Bill of Rights (California Government Code 3300-3313) A peace officer's : • Personnel records • Home address • Phone number • Date of birth • Photograph		

Appendix B – 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 insured's 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 insured's 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. 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.

C. 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.

Privacy Electronic Communications (SB178) CA Civil Code 1798.90 SB178 describes that a government entity is prohibited from access to electronic communication or electronic device communication without a search warrant, wiretap order or electronic reader records except for emergency situations.

III. Standards

A. Payment Card Industry Data Security Standard (PCS 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.

Appendix C – Security Policy/Standard Waiver

County of Sonoma
Security Policy/Standard Waiver

Local Agency Name: **Date:**

Waiver Requestor 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.

E-Discovery:

- Discovery documents produced in electronic formats rather than hardcopy.
- A process that includes electronic documents and email into a collection of "discoverable" documents for litigation. This normally involves both software and a process that searches and indexes files on hard drives or other electronic media. Extracts metadata automatically for use as an index.
- The process of finding, identifying, locating, retrieving, and reviewing potentially relevant data in designated computer systems.

- The process of identifying, preserving, collecting, processing, searching, reviewing and producing Electronically Stored Information(ESI) that may be relevant to a civil, criminal, or regulatory matter.

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.

Electronically Stored Information(ESI) – Writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations—stored in any medium from which information can be obtained either directly or, if necessary, after translation by the responding party into a reasonably usable form

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 Microsoft windows domain, by the distinguished name on a digital certificate or by a Microsoft 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 who is responsible for coordinating 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 Technology (IT) Resources – Information Technology (IT) resources include but are not limited to the following:

- Computers and any electronic device including personally owned devices, which, create, store or process Local Agency data:
- 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 written directive advising data custodians of certain documents to preserve all data including Electronically Stored Information (ESI) 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 Local Agency 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.

Personally owned Devices – The following is a representative and non-inclusive list of mobile devices wholly owned by a user to work on or access Local Agency data:

- 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

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.

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.

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

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

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

Secure Socket Layer (SSL) – Encryption technology that provides a secure connection between a web system and a user's web browser.

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.

Storage – See Store.

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 malicious individuals and malware. 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:

1. Password must be 8 characters in length.
2. Passwords must combine three or more of:
    a. Uppercase letters of European languages (A through Z)
    b. Lowercase letters of European languages (A through Z)
3. Base 10 digits (0 through 9).
4. Non-alphanumeric characters (special characters) (for example, $, #, %)

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.

Telework – A work flexibility arrangement under which an employee performs the duties and responsibilities of such employee's positions, and other authorized activities, from an approved worksite other that the location from which the employee would otherwise work.

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

Threat – Any potential danger to an IT Resource.

Transport Layer Security (TLS) - secure protocol that provide communication security in the county work. TLS is the successor to SSL.

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/Page#	Details
1.0	3/2014	All	Revised policy manual entitled IT Use and Security Policy Manual
2.0	1/2016	Page 31	Added strong password and high risk application in the glossary
3.0	3/25/2016	Page 31 Page 19 Page 26 Page 16	Revised strong password Added Mobile Computing for personally owned Devices Grammatical changes Revised URL links for Federal, State and local laws Removed “H” Local Information Services Providers. This is a duplicate of “D” Removed “I” Users. This was a duplicate of “A” users. K: Personal Use/Union Use: Added Recognized Employee Unions Added Personally owned device in glossary
4.0	4/1/2016	TOC Page 19	Verified removal of duplicate “users” section

Version	Date	Chapter/Section/Page#	Details
			Updated Table of contents to include Appendix C Removed “when technically possible language under VII.G.2 Removed “when technically possible
5.0	4/7/2016	Page 19	Mobile Computing A2. Revised Mobile Computing to “Users refusing to sign the Personally Owned Mobile Device agreement will not result in disciplinary action.”
6.0	5/13/2016	Page 19	Removed Appendix C “Personally owned Mobile Device agreement”. Moved language to Mobile Computing section to include user friendly language
7.0	6/10/2016	Page 19	Minor proposed updates in the mobile computing section.
8.0	6/29/2016	Page 25	Updated security awareness training section item 3 to include regular security awareness training and upon a change a change in their access.
9.0	8/18/2016	Page 18	Removed Unacceptable use #2 and added specific statements of unacceptable use from the current computer use policy
10.0	8/18/2016	Page 19	A. Personally Owned Mobile Device

Version	Date	Chapter/Section/Page#	Details
			Revised Item #1 Expectation of Privacy to say : “Users cannot be required to use their personally owned mobile devices to work on or access Local Agency IT Resources” Item #3”: Modified sentence to “view” Users should also be aware that they can view but not store confidential or restricted data on their personally owned device Item 9: Removed: Any changes in services must be reported to their supervisor or manager.
11.0	8/24/2016	Page 18	Unacceptable Use: Feedback that the phrase “which the Local Agency may deem inappropriate” was too broad; added specific language from current Computer Use Policy, as discussed.
12.0	9/29/2016	Page 8	Added under Users: Complying with the Mobile Computing section of this policy if using a mobile device to work on or access Local Agency IT resources or data. Use of Electronic Messaging

Version	Date	Chapter/Section/Page#	Details
		Page 14	Enhanced definition of personal messaging service. Underlined the statement about law enforcement: Law enforcement and/or other Local Agency workforce may be exempted from these restrictions during the performance of legitimate job responsibilities.
		Page 19-20	Updated Personally Owned Device sub-section of the Mobile Computing Section: 11.Updated wording that the Local Agency will attempt to remotely wipe data from their personally owned device if the device is lost or stolen. 13. Added that unattended mobile devices must be physically stored in a safe and secure manner.
			Added statement under the acknowledgment form agreeing to comply with personally owned device portion of the policy: I understand that if I voluntarily use my personally owned device to access Local Agency IT resources and data, I must comply with the Personally Owned Devices sub-section of the Mobile Computing section of this policy.

Version	Date	Chapter/Section/Page#	Details
		Page 23	
13.0	11/16/2016	Page 14-15 Page 19	Use of Local Agency IT Resources and Data Policy– Use of electronic messaging: Added for clarity on page 15: “social media accounts or email accounts (e.g. texting, Twitter, Facebook Messenger,Yahoo,Gmail).” Mobile Computing (Personally Owned Devices) Broke out the expectation of privacy into two paragraphs (#1 & #2) for readability: The County of Sonoma will only request access to the personally-owned device and password in order to implement security controls; to respond to litigation hold (aka e-discovery) requests arising out of administrative, civil, or criminal directives, Public Record Act Requests, and subpoenas; or as otherwise required or permitted by applicable state or federal laws. Such access will be performed by an authorized Local Information Service Provider technician or designee using a legitimate software process.

Version	Date	Chapter/Section/Page#	Details
		Page 14-Page 15	Added in “when technically feasible” under #4. Removed “Users should not use a personal email account (e.g. yahoo.com,gmail.com) to conduct Local Agency business on their personally owned mobile device.” This is already addressed on Page 15 (Use of Electronic Messaging). Added in a sentence on Physical Protection: “Unattended mobile devices must be physically stored in a safe and secured manner.” Added this wording to the Acknowledgment, “I understand that If I voluntarily use my personally owned device to access Local Agency IT resources and data that I will comply with the personally owned section of the Mobile Computing Policy section on page 19.”

Version	Date	Chapter/Section/Page#	Details
		Page 23	