May 2020

SANTA CLARA COUNTY INFORMATION TECHNOLOGY USER RESPONSIBILITY STATEMENT INSTRUCTIONS

In May 1995 the Board of Supervisors charged each County organization with the responsibility for ensuring that all County employees had read and signed a statement of responsibility concerning use of the County's networks and information systems. The resulting County-wide User Responsibility Statement is intended as a *minimum* statement of User responsibility, and individual County Agencies and Departments may require Users to read and sign additional statements to meet any special requirements that apply within their own environments.

- The County User Responsibility Statement must be signed by anyone who might reasonably require access to a County network and/or information system. This includes all County employees, as well as any other individual who needs authorized access for County business purposes. All Users who are allowed to access County resources remotely must also sign an additional attachment specifically related to remote access; this is included as Attachment A of the User Responsibility Statement. In addition, Users who are granted approval to use a personally-owned device for County business must also sign Attachment B of the User Responsibility Statement.
- By signing the Statement or its attachments, Users acknowledge that they have read and understand the contents and that violation of any of the provisions may result in disciplinary action, up to and including termination of employment and/or criminal prosecution.
- If an individual refuses to sign the Statement, the Department can choose to read the Statement to the individual, who will be required to verbally acknowledge understanding of the Statement's contents in the presence of two or more responsible managers. These managers will attest in writing that this reading and verbal attestation of understanding occurred. Failing this verbal acknowledgement of understanding, the involved individual will be denied access to all County information systems and networks.
- Each County organization is responsible for storing and maintaining the signed Statements of its own Users.
- All County organizations shall have their Users re-execute the Statement and/or attachments annually, or whenever there is an update or other change to the Statement or attachments (Department Heads will be notified by the County CIO's office of any updates or changes to the Statement or attachments).
- Each County organization should identify a "User Responsibility Statement Administrator." This is an occasional personnel function that should NOT be filled by a member of the organization's information system support staff. Because it is a

personnel function, a good choice would be an employee in an administrative position who is responsible for other routine personnel issues.

The User Responsibility Statement Administrator is responsible for the following tasks:

1. Identifying employees and other Users within the organization that will need to read and sign the Statement, as well as the relevant attachments.
2. Managing the signing process, including arranging for any briefings to be held in conjunction with Users signing the Statement and attachments.
3. Maintaining the signed Statements and attachments.
4. Ensuring that new employees and other new Users read and sign the basic Statement and any relevant attachments, and that the Department signing process is performed by all Users on an annual basis.

SANTA CLARA COUNTY IT USER RESPONSIBILITY STATEMENT

This User Responsibility Statement establishes a uniform, County-wide set of minimum responsibilities associated with being granted access to Santa Clara County information systems and/or County networks. A violation of this Statement may lead to disciplinary action, up to and including termination.

Definitions

County information systems and networks include, but are not limited to, all County-owned, rented, or leased servers, mainframe computers, desktop computers, laptop computers, handheld devices (including smart phones, wireless PDAs and Pocket PCs), equipment, networks, application systems, data bases and software. These items are typically under the direct control and management of County information system support staff. Also included are information systems and networks under the control and management of a service provider for use by the County, as well as any personally-owned device that a User has express written permission to use for County business purposes.

County-owned information/data is any information or data that is transported across a County network, or that resides in a County-owned information system, or on a network or system under the control and management of a service provider for use by the County. This information/data is the exclusive property of the County of Santa Clara, unless constitutional provision, State or Federal statute, case law, or contract provide otherwise. County-owned information/data does not include a User's personal, non-County business information, communications, data, files and/or software transmitted by or stored on a personally-owned device if that information/data is not transported across a County network or does not reside in a County-owned information system or on a network or system under the control and management of a service provider for use by the County.

A *mobile device* is any computing device that fits one of the following categories: laptops; Personal Digital Assistants (PDAs); handheld notebook computers and tablets, including but not limited to those running Microsoft Windows CE, PocketPC, Windows Mobile, or Mobile Linux operating systems; and "smart phones" that include email and/or data storage functionality, such as BlackBerry, Treo, Symbian-based devices, and iPhones. Note that the category "Mobile Device" does not include devices that are used exclusively for the purpose of making telephone calls.

A *public record* is any writing, including electronic documents, relating to the conduct of the people's business as defined by Government Code section 6252.

"*Remote access*" is defined as any access to County Information Technology (IT) resources (networks or systems) that occurs from a non-County infrastructure, no matter what technology is used for this access. This includes, but is not limited to, access to County IT resources from personal computers located in User's homes.

Users includes County employees who are on the permanent County payroll, as well as any other individual who has been authorized to access County networks and systems.

Key Points

1. General Code of Responsibility

The following General Code of Responsibility defines the basic standards for User interaction with County information systems and networks. All Users of County information systems and networks are required to comply with these minimum standards.

1.1 Users are personally responsible for knowing and understanding the appropriate standards for User conduct, and are personally responsible for any actions they take that do not comply with County policies and standards. If a User is unclear as to the appropriate standards, it is that User's responsibility to ask for guidance from appropriate information systems support staff or Department management.

You are responsible for your own behavior.

If you're unclear about a security standard, it's your responsibility to ask for guidance.

1.2 Users must comply with basic County standards for password definition, use, and management.

You must comply with County password standards.

1.3 With the exception of County-owned and approved devices issued to specific authorized County users, only authorized information systems support staff may attach any form of computer equipment to a County network or system unless express written permission to do so is given by Department management. This includes, but is not limited to, attachment of such devices as laptops, PDAs, peripherals (e.g., external hard drives, printers), and USB storage media.

Don't attach computer equipment of any kind to County systems or networks without permission.

1.4 The use of personally-owned USB storage media on any County computer system is prohibited. All such devices must be County-owned, formally issued to the User by the Department, and used only for legitimate County business purposes.

Use only County-owned and issued USB storage media.

1.5 Users must take precautions when connecting County owned computing equipment to a non-County network and must use a secure connection when performing County duties. Users are prohibited from connecting non-County computer peripherals including USB storage media, to County-owned computing equipment unless express written permission is given by executive management in the User's department and by the

Don't attach County equipment of any kind to non-County computers or networks.

Key Points

User's direct supervisor that the practice will align with the policies of the Information Security Office.

1.6 No User, including information systems staff, may install, configure, or use any device intended to provide connectivity to a non-County network or system (such as the Internet), on any County system or network, without express written permission. All such connections must be approved in writing by the County Chief Information Officer (CIO) or designee. If authorized to install, configure or use such a device, the User must comply with all applicable County standards designed to ensure the privacy and protection of data, and the safety and security of County systems.

Don't install or activate communication devices, such as modems, on County computers or networks.

1.7 The unauthorized implementation or configuration of encryption, special passwords, biometric technologies, or any other methods to prevent access to County resources by those individuals who would otherwise be legitimately authorized to do so is prohibited.

Don't use encryption except when directed to do so.

1.8 Users must not attempt to elevate or enhance their assigned level of User privileges unless express written permission to do so has been granted by Department management. Users who have been granted enhanced privileges due to their specific jobs, such as system or network administrators, must not abuse these privileges and must use such privileges only in the performance of appropriate, legitimate job functions.

Don't attempt to enhance your assigned user privileges.

1.9 Users must use County-approved authentication mechanisms when accessing County networks and systems, and must not deactivate, disable, disrupt, or bypass (or *attempt* to deactivate, disable, disrupt, or bypass) any security measure or security configuration implemented by the County.

Don't attempt to disable or bypass County login procedures.

1.10 Users must not circumvent, or attempt to circumvent, legal guidelines on software use and licensing. If a User is unclear as to whether a software program may be legitimately copied or

Follow the terms of all software licensing agreements.

Key Points

installed, it is the responsibility of the User to check with Department management or information systems support staff.

1.11 All software on County systems must be installed by authorized systems support staff. Users may not download or install software on any County system unless express written permission has been obtained from Department management or authorized system support staff.

Don't download or install software without permission.

1.12 Loss or theft of County-owned computer equipment, or of personally-owned computer equipment that has been approved for use in conducting County business, is to be reported immediately to designated Department management, administrative, or systems support staff. Users are also expected to be aware of security issues, and are encouraged to report incidents involving breaches of security, such as the installation of an unauthorized device, or a suspected software virus.

Immediately report the loss or theft of computer equipment, and also report any suspected security incidents.

1.13 Users must respect the sensitivity, privacy and confidentiality aspects of all County-owned information. In particular:

- Users must not access, or attempt to access, County systems or information unless specifically authorized to do so, *and* there is a legitimate business need for such access.

Don't access computers or data unless such access is related to your job.

- Users must not allow unauthorized individuals to use their assigned computer accounts; this includes the sharing of account passwords.

Don't share your user accounts or passwords with anyone.

- Users must not knowingly disclose County information to anyone who does not have a legitimate need for that information.

Don't share information with someone not entitled to have it.

- Users must take every precaution to ensure that all information classified as either Confidential or Restricted (or an equivalent classification) is protected from disclosure to unauthorized individuals.

Protect sensitive data from those not authorized to see it.

Key Points

- Users must not make or store paper or electronic copies of information unless it is a necessary part of that User's job.

Don't make copies of information unless this is required by your job.

1.14 Users must respect the importance of County-owned systems and data as a valuable asset, and should understand that any data stored or processed on any County computer, or transmitted over any County network, is County property. In particular:

- Users must not change or delete data or information unless performing such changes or deletions is a legitimate part of the User's job function.

Don't change or delete data unless doing so is part of your job.

- Users must avoid actions that might introduce malicious software, such as viruses or worms, onto any County system or network.

Don't introduce computer viruses onto County computers.

- A User who leaves employment with the County must not retain, give away, or remove any County data or document from County premises, other than information provided to the public or copies of correspondence directly related to the terms and conditions of employment. All other County information in the possession of the departing User must be returned to the User's immediate supervisor at the time of departure.

When leaving County employment, don't take County data with you.

1.15 Users should be aware that electronic information transported across any County network, or residing in any County information system, is potentially subject to access by County technical support staff, other County Users, and the general public. Users should not presume any level of privacy for data transmitted over a County network or stored on a County information system.

You should have no expectation of privacy for electronic data stored on County computers.

1.16 Users must respect all intellectual property rights, including but not limited to rights associated with patents, copyrights, trademarks, trade secrets, proprietary information, and confidential

Respect all intellectual property rights associated with data that you deal with while doing your job.

Key Points

information belonging to the County or any other third party.

1.17 All information resources on any County information system or network are the property of the County and are therefore subject to County policies regarding acceptable use. No User may use any County-owned network, computer system, or any other County-owned device or data for the following purposes:

- Personal profit, including commercial solicitation or conducting or pursuing their own business interests or those of another organization

Don't use County computers to conduct your personal business.

- Unlawful or illegal activities, including downloading licensed material without authorization, or downloading copyrighted material from the Internet without the publisher's permission

Don't use County computers for illegal activities.

- To access, create, transmit, print, download or solicit material that is, or may be construed to be, harassing or demeaning toward any individual or group for any reason, including but not limited to on the basis of sex, age, race, color, national origin, creed, disability, political beliefs, organizational affiliation, or sexual orientation, unless doing so is legally permissible and necessary in the course of conducting County business

Don't create or send demeaning or harassing material.

- To access, create, transmit, print, download or solicit sexually-oriented messages or images, or other potentially offensive materials such as, but not limited to, violence, unless doing so is legally permissible and necessary in the course of conducting County business

Don't view, download, or send pornography or other potentially offensive materials.

- Knowingly propagating or downloading viruses or other malicious software

Don't download or transmit malicious software.

- Disseminating hoaxes, chain letters, or advertisements

Don't send chain letters.

Key Points

1.18 Users that are employed by, or are otherwise associated with, a HIPAA impacted Department, are responsible for understanding and carrying out their responsibilities and duties as identified in the County HIPAA policies and procedures training, and other HIPAA-related materials that may be distributed from time to time.

Handle all protected health information according to HIPAA regulations.

2. Internet and Email

The following items define the basic standards for use of County Internet and email resources. All Users of County information systems and networks are required to comply with these minimum standards.

2.1 In general, Users must not use County systems or networks for personal activities. However, reasonable incidental (*de minimus*) personal use of County resources, such as Internet access and email, is allowed as long as such use does not violate the County's acceptable use policies, and does not interfere with the performance of work duties or the operation of the County's information systems. If a User is unclear as to what is considered appropriate incidental personal use, it is the responsibility of the User to ask for guidance from Department management.

Limit personal use of County computers.

2.2 When conducting County business, Users may not configure, access, use, or participate in any Internet-based communication or data exchange service unless express written permission has been given by Department management. Such services include, but are not limited to, Internet Instant Messaging (such as AOL Instant Messaging), Internet email services (such as hotmail and gmail), peer-to- peer networking services (such as Kazaa), and social networking services (such as blogs, MySpace, Facebook and Twitter).

Don't use Internet email or data exchange services (such as FaceBook, MySpace, or other social networking sites) to conduct County business.

Key Points

2.3 It is the User's responsibility to become familiar with the specific County policies, procedures, and guidelines associated with the use of Internet-based communication and data exchange services. Users who have been granted permission to use an Internet-based communication or data exchange service for conducting County business are expected to adhere to all relevant County policies, procedures, and guidelines associated with the use of these services.

You are responsible for understanding County guidelines for using Internet data exchange services, such as social networking sites.

2.4 Users are responsible for understanding and following the County's policy with respect to the retention of email messages, including immediately deleting non-business related email messages once these messages have been read.

Follow County standards for retaining and deleting email messages.

2.5 Users may not use an internal County email account assigned to another individual to either send or receive email messages unless they have received delegated access from the account owner.

Don't use anyone else's email account.

2.6 Users may not configure their County email account so that it automatically forwards messages to an external Internet email system unless express written permission has been given by the Department Head. When automated forwarding is used, it must be for legitimate business purposes only, and is to be implemented with the User's full understanding of, and willingness to accept responsibility for, the associated risks for disclosure of sensitive information.

Don't automatically forward County email to an Internet email system.

3. Remote Access

The following items define the basic standards for remote access to County information systems and networks. All Users of County information systems and networks are required to comply with these minimum standards. Users actually granted remote access privileges must sign the statement provided as Attachment A.

Key Points

3.1 All remote access to County resources must be via the secure, centralized, County-controlled mechanisms and technologies approved by the County CIO or designee, and installed by authorized County systems support staff. Users are not permitted to implement, configure, or use any remote access mechanism other than the County-owned and managed remote access systems that have been formally approved and implemented by authorized system support staff.

Use only existing, approved County remote access systems.

3.2 Written approval for use of County remote access mechanisms is to be granted to a specific User by the appropriate Department Head or designee. Remote access to County resources will be implemented on a case-by-case basis based on job-related necessity, and only for those Users that have read and signed both the County's general User Responsibility Statement and the Remote Access agreement (Attachment A).

Get approval for all remote access to County systems.

3.3 Remote access sessions may be monitored and/or recorded, and complete information on the session logged and archived. Users have no right, or expectation, of privacy when remotely accessing County networks, systems, or data. Audit tools may be used to create detailed records of all remote access attempts and remote access sessions, including User identifier, date, and time of each access attempt.

Remember that remote access sessions may be monitored and/or recorded.

3.4 All computer devices used to access County resources from a remote location must be configured according to County-approved security standards. These include approved, installed, active, and current: anti-virus software, software or hardware-based firewall, full hard drive encryption, and any other security software or security-related system configurations that are required and approved by the County.

Computers used for remote access must be configured according to County standards.

3.5 Users that have been provided with a County-owned device intended for remote access use, such as a laptop or other Mobile Device, will

Key Points

take all reasonable measures to ensure that the device is protected from damage, access by third parties, loss, or theft. Loss or theft of such devices must be reported immediately to designated Department management or support staff.

Take measures to prevent the loss or theft of County-owned Mobile Devices used for remote access, and report loss or theft of such devices immediately.

3.6 Users will practice due diligence in protecting the integrity of County networks, systems, and data while remotely accessing County resources, and will immediately report any suspected security incident or concern to their Department management and IT support staff.

Take appropriate measures to protect County computers and data when using remote access.

3.7 Remote access sessions are subject to all other relevant County IT security policies and standards, including Local User Authentication (passwords), Data Classification, Internet Use, and Email.

When using remote access, continue to follow all County security policies.

4. Personally-Owned Devices

The following items define the basic standards for the use of personally-owned devices to conduct County business. All Users of County information systems and networks are required to comply with these minimum standards. Users actually granted the privilege of using a personally-owned device to conduct County business must also sign the statement provided as Attachment B.

Note that in the case of Mobile Devices, the following provisions apply only to those devices that include email and/or data storage capability (such as BlackBerry devices and other "smart" phones), and do not apply to devices that are used strictly for the purpose of making telephone calls. This Section does not apply to authorized use of Outlook Web Access, provided that Users do not store or retain any downloaded County data on a non-County-owned device.

4.1 Use of personally-owned devices to conduct County business is prohibited unless express written permission is obtained from both the Department Head and IT Manager. If the User in question is a Department or Agency Head,

Use of a personally-owned device to conduct County business requires approval.

Key Points

express written permission must also be obtained from the County Chief Information Officer or designee. The use of personally-owned devices to conduct County business is a privilege, not a right, and employment at the County does not automatically guarantee the granting of this privilege.

4.2 The personally-owned device in question must use existing, County-approved and County-owned access/authentication systems when accessing County resources. Installation by Users of any hardware, software, or network interface components that provide unauthorized network connectivity, either wired or wireless, is prohibited.

If you are allowed to use your own computer or mobile device for County business, you must still use County-approved user login procedures.

4.3 The User shall allow the County to configure personally-owned devices as appropriate to meet security requirements, including the installation of specific security software that is mandated by County policy. When reasonably possible and practical, the County shall strive to provide a minimum of 24-hours notice to the User before configuring the personally-owned device. While the device is in the County's possession, the County shall not access, alter, retrieve or delete the User's personal information, communications, data, software or files stored on the device unless (a) it is reasonably necessary to do so to configure the device to meet security requirements, or (b) the User agrees to the specific access, alteration, retrieval or deletion.

You must allow authorized IT staff to configure, and periodically update, security software on any personally-owned device used to conduct County business.

4.4 Users authorized to use a personally-owned device must follow designated Department procedures for ensuring that software updates and patches are applied to the device according to a regular, periodic schedule. All software installations and updates are subject to verification by management-designated Department staff.

Follow Department procedures for updating and patching software on personally-owned devices.

Key Points

4.5 Users have no expectation of privacy with respect to any County-owned communications, information, or files on any personally-owned device. Except as otherwise provided in this policy or as required by law, the County shall not access any of the User's personal information, communications, data or files on the User's personally-owned devices.

4.6 Clause removed subject to revision.

4.7 If a user is contacted on a personally-owned device by someone from the County conducting County business, and the User has not obtained permission to conduct County business with that personally-owned device, then the County may not access that device regarding that User-received communication other than through legally permissible methods such as a subpoena, request for voluntary disclosure, etc. The preceding sentence shall not limit the County's right to direct a User to disclose the communication at issue upon reasonable notice.

The County will not require you to allow access to your personally-owned device for unsolicited, incoming County communications if that device has not been approved for use in conducting County business

4.8 The User shall adhere to all relevant County security policies and standards, just as if the personally-owned device were County property. This includes, but is not limited to, policies regarding password construction and management, physical security of the device, device configuration, and hard drive sanitization prior to disposal. This does not restrict the User's personal use of the device so long as that personal use does not include or result in (a) the User's failure to adhere to all relevant County security policies and standards, or (b) the breach of the County's security policies or standards

Even when using your own computer or other device for County business, you must still follow all County security policies.

Under most circumstances, you can continue to use an approved device for personal use as well as County business.

Key Points

4.9 The User will make no modifications of any kind to operating system configurations implemented by the County on the device for security purposes, or to any hardware or software installed on the device by the County, without the express written permission of the County CIO's Office.

Don't modify any security configuration settings or security software on your computer.

4.10 The User must treat the work- related or County-owned communications, information or files as County property. The User must not allow access to or use of any work-related or County-owned communications, information, or files by individuals who have not been authorized by the County to access or use that data.

The User must immediately report to designated Department management or support staff any incident or suspected incident of unauthorized access and/or disclosure of County resources, data, or networks that involve the device, including loss or theft of the device.

4.11 The User must immediately report to designated Department management or support staff any incident or suspected incident of unauthorized access and/or disclosure of County resources, data, or networks that involve the device, including loss or theft of the device.

Immediately report the loss or theft of a personally-owned device that has been used for County business.

Key Points

Acknowledgement of Receipt

This Acknowledgement hereby incorporates the main body of the User Responsibility Statement. Attachments A and B are additional signature pages that apply only to those individuals that have been granted either remote access privileges (Attachment A) or permission to use a personally-owned device (Attachment B). These Attachments should only be signed if either of these conditions apply.

All Users must sign this Acknowledgement; Users with permission to use Remote Access should also sign Attachment A, and Users with permission to use personally-owned devices must complete and sign Attachment B.

The User should understand that the County's failure to enforce any provision of this Statement does not mean that the County will not enforce that or any other provision in the future. The User should also understand that if a clause, sentence or paragraph of this Statement is determined to be, invalid by a Court or County commission, this does not affect the validity of any other portion of the Statement.

By signing below, I acknowledge that I have read and understand all sections of the County of Santa Clara's User Responsibility Statement. I also acknowledge that violation of any of its provisions may result in disciplinary action, up to and including termination of employment and/or criminal prosecution.

Violation of any of the provisions in this User Responsibility Statement may result in disciplinary action.

If at any time, I have questions or doubts, or I feel ambivalent or unclear on any matter related to IT security and/or data confidentiality, I understand that it is my responsibility to request clarification from my supervisor or other appropriate manager before taking any action.

It is your responsibility to ask for clarification if you don't understand any aspect of the County IT security policy.

IT User Responsibility Statement
Acknowledgement Form

I acknowledge that this Statement will still be in effect following a transfer to another County Agency or Department, and that all of its provisions will continue to apply to me as long as I am a County employee or other individual who needs authorized access for County business purposes.

User Signature:

_____

Print User Name:

_____

Agency/Department:

_____

Date Signed:

_____