SOLANO COUNTY INFORMATION TECHNOLOGY

Acceptable Use Policy

This Information Technology Acceptable Use Policy ("Policy") provides employee guidance for the proper use of the electronic information systems of Solano County. The electronic systems covered by this document include computer equipment, Internet access, computer software, data, databases, electronic files, voice mail, fax machines, wireless devices, flash drives, smart phones, Personal Digital Assistants, handheld computers, tablets, and any other similar information technologies that Solano County currently uses or may use in the future (referred to as "System" hereon). This Policy works in concert with the Information Technology (IT) Security Policies Manual. This Policy is also an elaboration of the "Proprietary System" notice that is displayed when an employee logs onto the System through a computer workstation or via the Internet. All County personnel are obligated to adhere to the security policies within this document known as the "Acceptable Use Policy"

I. Approved Business Tools Only

Solano County-approved electronic communications resources, including but not limited to e-mail and Web browsers and Solano County computers are to be used to conduct Solano County business. Personal e-mail accounts, Web-based e-mail services, anonymous re-mailers, Instant Messaging, and other "non-approved" communications tools must not be used, nor should the Solano County name be used or any of Solano County's business disclosed over these types of connections.

II. Ethical Responsibility

All County personnel have an ethical obligation to use Solano County's Internet and intranet resources in a responsible and professional manner, just as in the case of any other company resources, such as telephones, electronic fax machines, computers, or e-mail. All County personnel will follow proper security measures and procedures to protect the County's information technology assets from security breaches. All County personnel must immediately report known or suspected misuse to their Department Head, to their authorized department designee, to their IT Manager, or to the Solano County Help Desk.

III. Personally Identifiable Information (PII) Handling

Employees may have work duties which involve the handling of data that include personally identifiable information (PII), classified in the highest tier of sensitive data as "confidential." Examples of PII include:

- Social Security Numbers
- Driver's License Numbers
- Bank Account Numbers
- Credit/Debit Card Numbers
- Private Personnel and Payroll Information
- Personal Medical Records

The unauthorized disclosure, theft or loss of this information would severely impede the County's business and place the County at risk of legal liability. Therefore, employees must adhere strictly to their specific Department and/or County policies and procedures for handling PII in protecting the accuracy, availability, integrity and confidentiality of information.

As part of this control for PII, employees accessing electronic systems and applications must acknowledge the information in the "warning banner" identifying the data being accessed as potentially confidential, subject to system logging and to be used for authorized business purposes only. The employee must accept these terms by providing a positive response to continue. Failure to accept the terms will result in being directed to exit the system/application.

IV. Data Protection

All County personnel:

- Shall safeguard and secure portable devices which contain sensitive County data at all times.
- Shall take reasonable precautions to ensure that portable electronic devices in their possession are protected from theft, damage, and adverse compromise of sensitive information. Employees shall ensure that while in transit between workplaces, the portable device and media is secure in a carrying case, computer bag or brief case, and remains in their presence at all times
- Must comply with policy that sensitive data can only be placed onto a portable device for; 1) a strict business need, 2) only a minimum amount of information is stored to mitigate exposure, and 3) if the device is encrypted
- Must store critical information on servers and not workstations. Data that is not stored on a server must be backed up routinely, based on frequencies set by Department Heads or their authorized designees. No sensitive data shall be saved to non-County owned equipment.
- Must report misuse, damage or theft of data and unauthorized access to sensitive data immediately to their Department Head, their authorized designee, their IT Manager, or the Solano County Help Desk.
- Must not enter information into a computer or database that is known to be false and/or unauthorized, or must not alter an existing database, document, or computer disk with false and/or unauthorized information.
- Are prohibited from accessing other individuals' e-mail, data, and voicemail files and computers without the other's knowledge.

V. Password Policy Requirements

All system passwords shall follow the minimum standards as described below: Password syntax, expiration, and revocation standards shall be uniform across all Solano County systems.

In conjunction with the user's ID, system passwords are considered confidential and, as such, shall not be shared or openly displayed. The following rules apply to all County personnel:

1. Password Change Interval: 90 Calendar days
2. Password History: Systems shall not allow reuse of any of the last 10 passwords

3. Unsuccessful Password Attempts: User account locked after 3 unsuccessful attempts
4. Password Length: Passwords must contain at least 8 characters.
5. Password Format:
    a. May not contain user ID or any part of user's name
    b. Must contain characters from 3 of the following 4 classes:
        i. Uppercase letters (A, B, C…)
        ii. Lowercase letters (a, b, c…)
        iii. Numerals (1, 2, 3…)
        iv. Non-alphanumeric (,), !, @, #, $, %, +, -, =, &, #, <, >…)

VI. Legitimate Use of Resources

Solano County's electronic communications resources, including but not limited to the Internet, World Wide Web and e-mail, are to be used for legitimate business purposes. **Incidental and occasional personal use of Solano County electronic equipment and/or resources is acknowledged. Incidental and occasional personal use is defined as short in duration, requires a minimum of personal time to accomplish, and does not use significant resources or bandwidth.**

VII. No Privacy of Use

Employees will have no expectation of privacy when they use Solano County electronic equipment for personal purposes, and any communications made with such equipment will be treated in the same manner as business communications.

VIII. Illegal Uses of Resources

Use of Solano County's electronic communications systems must be in compliance with all applicable laws, policies, and procedures. Any misuse of the Solano County System is expressly prohibited. "Misuse" includes:

a. Non-Business Purposes. Examples include: disseminating non-work related pictures, videos, chain letters, spam, or messages; playing computer games; personal Web surfing; conducting personal business; use of the Internet for music playing from radio stations or websites, for streaming-video, and any other personal use that requires resources that use up bandwidth and processor time. Personal use is defined as electronic communications that contain non-business information, sent or stored on Solano County-owned equipment that includes, but is not limited to, local fixed disk drives, local area network (LAN) drives, and removable storage media stored at a user's workstation, or communications over the Internet. County personnel must not place any Solano County business-related information or links to Solano County's Web sites on their personal Web pages, or in personal e-mail or Web postings.

b. Personal Profit Activities. Using the System for personal profit;

c. Inappropriate Content. Using the System to send, receive, print, display, perform, or otherwise disseminate material that, to a reasonable person, may be abusive, obscene, pornographic, defamatory, harassing, grossly offensive, vulgar, threatening or malicious;

d. Infringement of Proprietary Rights. Using the System to copy, send, receive, store, print, display or otherwise disseminate files, graphics, software, or other material that actually or potentially infringes the copyright, trademark, patent, trade secret, or other intellectual property.

e. Security and Access. Attempting to access a part of the System assigned to another person or for which you have not been granted authorized access, or using or otherwise undermining or circumventing security devices, procedures, or access restrictions within the System, or anywhere else via the System; sharing, writing down, or storing in a readable format any confidential user codes, user account IDs, passwords, remote access accounts, passwords, and tokens or other codes intended to restrict access to information assets; using CMOS (bootup) passwords on the System;

f. Software. Downloading, using, or installing any unauthorized or unlicensed software or data, including screen savers, games, time or logic bombs, lockout or disabling devices or code, Trojan horses, viruses, or worms, or peer to peer file sharing applications; performing unauthorized duplication of software; ("Unauthorized" means software that has not been authorized by the appropriate level of management AND approved by the Software Inventory Technical Business Analyst. "Unlicensed" means software or data that has not been acquired through Solano County's normal purchasing procedure, that is not licensed to Solano County, or, in the situation of a contractor retained by Solano County, not authorized by the express terms of the contract, or both); installing Solano County software on non-Solano County equipment; using mechanisms to bypass authorized remote access mechanisms, for example, remote control software and applications such as PCAnywhere or GoToMyPC.com; configuring file and print sharing;

g. Hardware. Performing unauthorized installations or moves of computer equipment or components; using non-Solano County equipment on the Solano County network;

h. Sensitive Data. Using the System to copy, send, receive, print, display, or otherwise disseminate sensitive information that contains or includes confidential, restricted, private or proprietary information of either Solano County, its personnel, clients, or customers, without authorization to any person who is not authorized to receive such data; using unsecure written communication, such as unencrypted e-mail, when transmitting confidential or sensitive information; not locking an unattended workstation using a password; storing sensitive data on portable devices without encryption.

i. Encryption. Installing or using any encryption algorithm or software program not authorized by Solano County to encrypt or encode information without the express permission of Solano County;

j. Internal Investigations. Refusing to cooperate in or interfering with an internal investigation or audit;

k. Correspondence with the Public. Not obtaining appropriate approvals from your Department Head or authorized designee and/or County Counsel for electronic communications deemed to be correspondence or a communication with the public, unless it is for legitimate business purposes.

l. Other. Using the System to engage in any other activity deemed by Solano County to be in conflict with the spirit and intent of this Policy or in conflict with any other legal obligation you have to Solano County.

IX. Electronic Mail (E-Mail)

All the security requirements for Internet electronic mail also apply to internal e-mail use.

a. Confidentiality of Contents. Written communication, such as e-mail, generally should not be used when transmitting confidential or sensitive information. Solano County, however, reserves the right to review, monitor, etc., all e-mail messages which use the System, whether transmitted internally or externally. Occasionally, Solano County may be required to disclose e-mail messages in a legal proceeding. Messages transmitted externally that contain confidential, privileged or otherwise sensitive information must be encrypted in accordance with the Information Data Classification and Handling Policy so as to be considered secure. For guidelines on day-to-day electronic communications within Solano County (internal) as well as communication between Solano County and third parties who are not on the Solano County network (external), please refer to Electronic Communication Guidelines. To request e-mail encryption, please contact the Solano County Help Desk.

b. E-mail Management. E-mail should be checked regularly, deleted or archived periodically, and requests for e-mail storage quota adjustments approved only by Department Heads.

X. Solano County Access To Users' Electronic Communications

a. Access to User Records. When required for a Solano County business purpose, or if required to do so by law, regulation or policy, or if independent indications suggest that impropriety or security breaches may be present, a user's electronic communications records may be accessed or reviewed at any time by his or her Department Head or authorized designee or the Chief Information Officer (CIO). Solano County will attempt to limit disclosure of the contents to third parties, to the extent consistent with Solano County's business needs or legal obligations.

b. Activity Logs. Logs may be maintained that record all Internet activity over Solano County's networks. Every connection by a Solano County user to a remote server, bulletin board or Web site may be recorded, and the addresses logged and audited.

XI. Personal Equipment Connected to the Solano County Network

- A risk assessment is required for connecting non-County personal computers to the Solano County Network. Appropriate approvals and required actions within the risk assessment will be obtained and followed.
- County personnel and Vendor(s) requiring VPN access to the Solano County Network shall request authorization from the Department Head or authorized designee whose department specific system is being supported.
- By using VPN, dial-up, or any other method of connecting to the Solano County network on a personal machine, these personal machines are considered de facto extensions of the Solano County network and are subject to the same policies in this document that apply to Solano County owned equipment. It is the responsibility of those granted VPN privileges to ensure that no unauthorized users access the Solano County Network through that VPN.
- All systems connected to the Solano County network shall:
    - Use the most up-to-date anti-virus software
    - Use either enterprise or personal firewall technology
    - Have the latest security-related software patches/fixes installed
- Use of smart phone and tablet equipment shall also follow the following agreement:

Smart Phone and Tablet Support Agreement

Purpose

Solano County Department of Information Technology (DoIT) may grant personnel with access to Solano County's data including e-mail, calendar, and contacts from Blackberry, Android, iPhone, Windows Mobile smart phones, iPad, Acer, and other tablets. **All Solano County personnel must acknowledge and abide by this Smart Phone and Tablet Support Agreement in order to use their smart phone or tablet to access Solano County data, including e-mail, calendar, and contacts.**

In accordance with the Information Technology (IT) Security Policies Manual and the Acceptable Use Policy, I will do the following **prior** to connecting my smart phone or tablet to the Solano County network:

- I will get approval from my department head, authorized designee, and/or manager, per departmental policy.
- I will implement an 8 character strong password or pin on my smart phone or tablet.
- I will configure my smart phone or tablet to automatically lock after 15 minutes.
- I will avoid storing Solano County sensitive data on my smart phone or tablet, to the extent possible. If sensitive data must be stored on my smart phone or tablet, I will ensure my smart phone or tablet is encrypted.
- I acknowledge that if I install 3rd party applications, I do so at my own risk since they may pass viruses or other malware.
- I will contact the Solano County Help Desk electronically, acknowledging this *Smart Phone and Tablet Support Agreement*.

Smart Phone and Tablet Carrier Technical Support

I will directly contact my smart phone or tablet carrier for the following support:

- Ordering a device, selecting a data plan, questions about my bill, or changes in my wireless contract.
- When my device is not working.
- Voicemail configuration or issues.
- Configuring password protection and automatic screen locking.

- Application issues including those for personal e-mail such as Google or Yahoo accounts.
- Problems with Internet access or browser issues.

DoIT Technical Support

I will contact the Solano County Help Desk for the following support:

- **Immediately if my smart phone or tablet is lost or stolen.** If it is after hours, I will call the emergency after hours phone number identified on the Help Desk voicemail message. In addition to immediately contacting the Help Desk, I will also notify my departmental manager.
- To request Exchange server information to configure my smart phone or tablet device to connect to Solano County data.
- When my Solano County e-mail is not being delivered and the device is otherwise working (i.e., the phone or tablet is functional; wireless is turned on; Internet access is working).
- When I need to disconnect my smart phone or tablet permanently from the Solano County network.

I also acknowledge and agree to the following:

- DoIT may help troubleshoot smart phones and tablets as a courtesy but may not always be able to resolve an issue or be able to address the problem immediately.
- I will make myself available to help troubleshoot including typing in passwords and contacting the carrier, as required.
- I will not hold Solano County responsible for lost data or physical damage to smart phones or tablets that may occur as a result of the troubleshooting process or implementation of data protection measures. Data protection measures may include, but are not limited, to disabling, erasing, encrypting, and/or setting passwords on your smart phones or tablets.
- I will not store sensitive data on unencrypted smart phones or tablets.

XII. Changes to This Policy

Solano County may from time-to-time amend or modify this policy. In such event, you will be provided with a written or electronic copy of the amended or modified policy. Upon receipt of the amended or modified policy, you will be required to conduct yourself in accordance with its provisions.

XIII. Labor Contracts Provisions

It is understood that, in the event of a difference between the requirements of this policy and/or any other related Solano County policy, the terms of the negotiated labor agreements will take precedence.

XIV. Consequences of Non-Compliance

The loss, misuse, damage, or unauthorized modification of Solano County's information and/or electronic communication systems may lead to negative consequences for Solano County, including damage to reputation, loss of customer confidence, legal sanctions, litigation, financial loss, and/or business interruption. Consequently violations of Solano County's policies and/or standards may result in disciplinary action, up to and including termination of employment and/or contract termination and, in some cases, criminal prosecution.