**THE BOARD OF SUPERVISORS OF THE COUNTY OF STANISLAUS**
**ACTION AGENDA SUMMARY**

**DEPT:** Strategic Business Technology, mc | **BOARD AGENDA #** *B-6

**Urgent** ☐ **Routine** ☒ | **AGENDA DATE** February 14, 2012

**CEO Concurs with Recommendation YES** ☒ pnt **NO** ☐ (Information Attached) | **4/5 Vote Required YES** ☐ **NO** ☒

SUBJECT:

Approval to Accept the Revised Stanislaus County Information Technology Security Policy and Security Status Report

STAFF RECOMMENDATIONS:

1. Approve the revised Stanislaus County Information Technology (IT) Security Policy.

2. Accept the Security Status Report.

FISCAL IMPACT:

The cost of implementing the revised IT Security Policy will vary by department. Departments that currently rely on the Strategic Business Technology (SBT) department to provide their network resources should have no costs associated with the revised policy. SBT has purchased software to meet the policy requirements that has a one-time cost of approximately $500. The updated policy area that is creating a potential for expense is the requirement for "Remote Access Control" for network devices.

[Continued on Page 2]

BOARD ACTION AS FOLLOWS:

No. 2012-064

**On motion of Supervisor** Withrow, **Seconded by Supervisor** Monteith
**and approved by the following vote,**
**Ayes: Supervisors:** Chiesa, Withrow, Monteith, De Martini, and Chairman O'Brien
**Noes: Supervisors:** None
**Excused or Absent: Supervisors:** None
**Abstaining: Supervisor:** None

1) X **Approved as recommended**
2) _____ **Denied**
3) _____ **Approved as amended**
4) _____ **Other:**
**MOTION:**

**ATTEST:** CHRISTINE FERRARO TALLMAN, Clerk — Elizabeth A. Kemp, Deputy

**File No.**

**FISCAL IMPACT: (Continued)**

Departments that do not rely on SBT to provide their network services will have anywhere between zero impact up to $12,000 initial start-up costs per department, with on-going support costs of approximately 15% - 20% annually. The estimated impact to General Fund departments not supported by SBT is $11,000 initially, which include the Sheriff's Department, Probation, and the Ag Commissioner's Office. These departments, as well as others, provide their own network services and will have varying expenses based on the network infrastructure they support and the products or vendors they choose to use which satisfy the requirements of the revised IT Security Policy.

**DISCUSSION:**

The current Stanislaus County IT Security Policy was developed in late 2004 and early 2005. Since that time, the policy and processes that were put in place have contributed greatly to the overall security posture of the County.

As technology advances and new IT Security threats emerge, the County IT Security Policy needs to be revised and updated to reflect and to secure against this ever changing IT environment. Recognizing that our current IT Security Policy is aging and that IT security technology has advanced since 2005, the IT Security Special Interest Group (SIG) worked collectively with the County IT Steering Committee and the County IT Managers Group to develop a revised IT Security policy.

The revised IT Security Policy was developed over a 12 month period and representatives from the groups mentioned above met regularly to complete this task. All Department Heads and County labor groups were notified of the proposed revisions and were given the opportunity to provide feedback. As a result, most departments were involved and have worked diligently in the development of this policy. The IT Security SIG meets quarterly and will continue to work with County IT Groups to keep the security policy up to date and continue to refine the implementation of IT security.

**Enhancements to the Policy**
Most of the revisions to the Policy were minor; however there are a few notable additions and revisions. They are as follows:

- The Policy was condensed to eliminate numerous redundancies between the end user policy and the department policy. We now have one policy that is used for both the department and the end user.

- A section was added to deal specifically with smart phones and the potential security threats that these devices pose.

- Wireless encryption standards have been raised to be at par with current best practices for wireless security.

- Standards were added for centralized user management of network devices.

**Current Status of IT Security**
There is currently an audit process that is followed to ensure that departments are following the approved policy. There is a regular self-assessment by each department; followed by peer reviews and an external perimeter audit that has been performed biennially by an external security auditor. During these assessments, IT security concerns are sometimes found and the County Information Security Manager is available to departments upon request to assist in the remediation process. The County Information Security Manager also participates in the auditing process, co-ordinates the peer reviews and works closely with the external security auditor.

Since the original adoption of the IT Security Policy in 2005, there have been two external perimeter audits completed and a County-wide peer review. The security threats identified during the audits and review were minimal and remediated promptly. The County is currently scheduled to have another external perimeter audit performed in the first quarter of 2012.

**Policy Implementation**
Departments will be given a period of 12 months to comply with any revisions to the original policy that would cause a department to take on additional expenditures. This 12 month period should give departments enough time to plan and budget appropriately for any additional expenses that may occur as a result of the elevated security standards.

**Ongoing Management of IT Security**
The County IT Security Manager will continue to work with County departments to perform an external perimeter audit of County IT systems on a biennial basis and assist where necessary in the remediation of identified security threats. The County IT Security Manager will continue to coordinate peer reviews in alignment with the revised IT Security Policy. The County IT Security Manager will continue to hold regular IT Security (SIG) meetings as a vehicle for future policy updates and discussion on regular security concerns.

**POLICY ISSUES:**

The revised Stanislaus County IT Security Policy and Security Status Report is consistent with the Board's priorities of Efficient Delivery of Public Services and A Safe Community by providing an increased IT security posture and as a result, an increase in the reliability of our IT infrastructure.

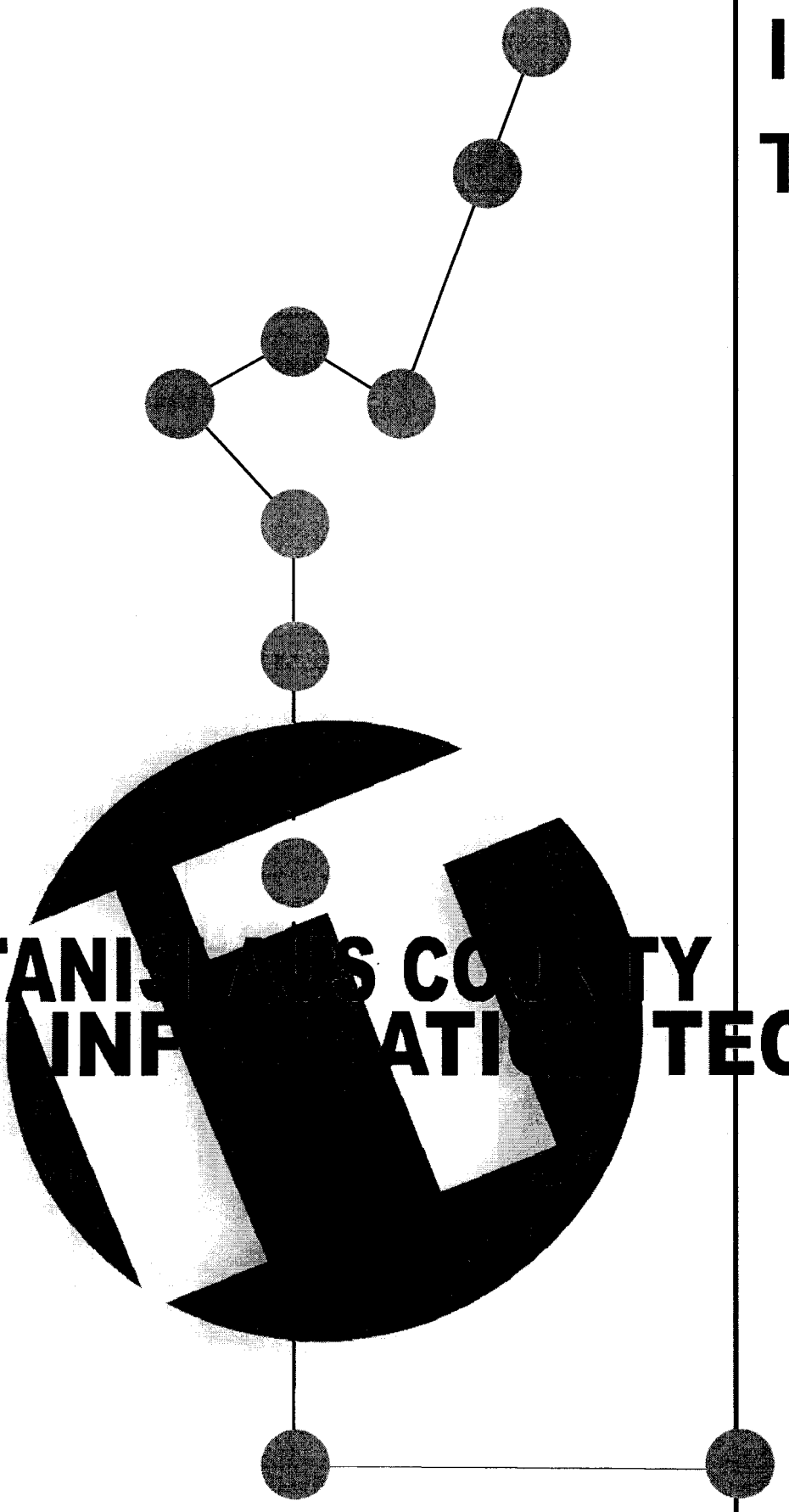
**STAFFING IMPACTS:**

Existing staff from Strategic Business Technology will continue to provide support for the IT Security SIG and ongoing peer and external perimeter audits. There are no additional staffing impacts associated with this item.

**CONTACT PERSON:**

Mike Baliel, IT Security Manager, Telephone: 209-342-1737

# Information Technology Security Policy Manual



Stanislaus County
Striving to be the Best

STANISLAUS COUNTY
INFORMATION TECHNOLOGY

## 1. PRECEDENCE

This document does not supercede or override any regulations promulgated by State or federal agencies, such as the requirements mandated by the Department of Justice, that are more stringent or impose additional requirements than this policy.

## 2. CONTENTS



## 3. NON-COMPLIANCE

An employee who violates this policy will be subject to the appropriate disciplinary action, which may include suspension, demotion or termination from County employment. Any criminal misuse of County computer resources will be investigated for possible legal prosecution. An employee found to have violated this policy may have his/her access to the County or departmental computer system, the Internet, the Intranet or the Email system limited or revoked completely. Any attempts to circumvent County IT Security measures shall themselves be viewed as violations of this policy.

Any employee aware of accidental non-compliance, misuse or suspicion of misuse, shall report the incident to a supervisor immediately.

Stanislaus County Departments that cannot, for whatever reason, comply with the requirements of this document, shall maintain a document describing the non-complying system or process. This document shall include a mitigation plan with specific budget and timetables identified, if applicable. It is understood that some current Stanislaus County

information systems do not comply with certain requirements in this document. Departments shall undertake to correct/replace these systems to improve overall County IT security. Should a Stanislaus County Department need assistance in devising or implementing a mitigation plan for their non-complying system, that Department shall report it to the IT Security Manager and to request from the IT Security Manager such assistance.

Employees will not be held accountable for non-compliance when necessary items or actions to maintain compliance are within the Department's responsibility.

## 4. POLICY IMPLEMENTATION

Upon approval of this policy by the Board of Supervisors all County employees shall be expected to adhere to this policy as it is written. All employees have a responsibility to read, understand and comply with this policy.

The initial distribution of this policy, to all County employees, shall be through County payroll. It will be each Department's responsibility to ensure that each employee receives and signs the initial policy within thirty (30) days, absent a valid reason (e.g. vacation, leave of absence, etc.).

This policy shall apply to all County employees including, but not limited to, regular full-time, part-time, seasonal, temporary, supervisory, management, department heads, volunteers and Personal Service Contractors. This policy shall also apply to independent contractors who utilize any County computers or the County computer system.

As this policy may be frequently updated as technology and security threats change, a copy of the latest version of this policy shall be given to each employee annually by the Department. The supervisor should consider the employee's compliance with this Policy in evaluating the employee's performance. Any changes to this Policy that are of sufficiently significant nature, as determined by the Stanislaus County Security Special Interest Group and approved by the Stanislaus County Board of Supervisors and Department Heads, shall require all County employees to re-sign this Policy.

It is the Department's responsibility to ensure that all new Department hires have acknowledged receipt and reviewed this policy within 30 days of initial hire date. The Stanislaus County Security Special Interest Group, in conjunction with the CEO's office and SBT, will offer training sessions in regards to this policy. The training classes may be scheduled by contacting SBT and coordinating with the County IT Security Manager.

## 5. CONFIDENTIALITY/PRIVACY/DATA OWNERSHIP

a) Any Internet-related activity, such as web site visits, downloads, chat sessions or web forum postings can and will be tracked and recorded.

b) The CEO's office and County Counsel, have the right to review any Internet or email activity of any employee at any time for any reason. The Department Heads or their designee, have the right to review any Internet or email activity of any of their employees

at any time for any reason. The County reserves the right to inspect any and all files stored in private areas of the County information systems in order to assure compliance with this policy.

c) All electronic data, including email, created or received utilizing County information systems is the property of the County. Subject to applicable legal privileges and confidentiality requirements, all electronic data entered or received on County information systems is public and is subject to disclosure upon the demand of the County at any time.

## 6. INFORMATION SYSTEMS COMMUNICATION

a) Each employee is responsible for the content of all text, audio or images that they place or send over the County's information systems, or which appear on their computer. No electronic communication shall be sent which hides the identity of the sender or represents the sender as someone else unless authorized by the Department Head.

b) All messages communicated on the County's information systems shall contain the employee's name unless authorized by the Department Head. Any messages or information sent by an employee are statements that reflect upon the County.

c) All communications sent by employees via the County's information systems shall comply with this and other County policies and shall not disclose any confidential or proprietary County information without proper authorization.

## 7. UNACCEPTABLE USE

a) County information systems access or individual computer usage shall not be used for transmitting, retrieving, receiving or storing of any communications of a discriminatory or harassing nature or materials that are perceived as being obscene. Harassment of any kind is prohibited by County policy.

b) No messages with derogatory or inflammatory remarks about an individual's race, age, disability, religion, national origin, physical attributes or sexual preference shall be transmitted. No abusive, profane or offensive language shall be transmitted through the County's information systems.

c) Electronic media shall not be used for any other purpose that is illegal, against County policy, causes discredit to the employee 's department or the County, or is contrary to the County's best interest.

d) County computers and information systems shall be used only for authorized County business. It is unacceptable for employees to use County information systems for personal gain or profit, or for personal reasons that would result in depleting resources, impeding the organization's ability to conduct business, or cause any interruption or delay in service to the public. The occasional limited use by County employees to check home email, or access appropriate internet sites during lunch, break or after hours does not constitute inappropriate use in and of itself. Additionally, employees shall only access

information systems with which they have authority to do so.

## 8. PORTABLE DATA

a) When an individual department has a business need for staff to utilize portable data, specific departmental procedures shall be used to insure the highest level of security is attained. When transporting or transmitting County information in portable format (i.e. a DVD or USB flash drive) the staff person shall be responsible for its security and shall take all reasonable precautions (keep in personal possession, in locked brief cases, encrypt when possible, et cetera) to insure that it does not fall into unauthorized hands.

b) Removing electronic data from the work-site is prohibited without proper written authorization. Staff is discouraged from creating or modifying County documents at home on personal computers.

## 9. MOBILE USERS

a) County shall not, as standard practice, purchase computers, software, software licenses, Internet or phone services or office equipment such as printers, fax machines, calculators, or furniture for staff who work from home (in-home telecommuters). Purchase of such items, as well as consumable supplies, must be at the direction and approval of a Department Head, and shall be in compliance with County budget, purchasing and management information services policies.

b) Software may in some instances be provided for use on non-County-owned systems when the Department Head approves purchase of the necessary licenses. County IT staff shall only install such software on an employee's personal computing device, when the Department Head provides prior written approval. In this case, the employee must bring the device to the County location. Virus protection software and Operating System patches shall be maintained and up-to-date on any computers or devices that will connect in any way to the County information systems.

c) In addition, the selection, installation, maintenance, repair or replacement of employee-owned equipment and software is the responsibility of the employee. Computer equipment shall have a configuration that is compatible with County's Information Technology (IT) standards and infrastructure.

*d)* County-issued cell phones and or mobile devices, may contain privileged or confidential information such as contact information or even emails or documents. Some "smart phones" and similar mobile devices like Blackberry, iPhones or iPads may actually connect automatically to County email systems or other information technology systems owned or maintained by the County. Any such devices that store emails and/or connect to County IT systems shall be configured to automatically lock after a period of disuse and require a password to be unlocked. The "timeout" period, after which the phone or mobile device locks, shall not exceed thirty minutes and shall not exceed sixty minutes for sworn officers. Reasonable care should be taken to use a password that is not easily guessed. Lost or stolen phones/mobile devices in this category must be reported to the department telecom coordinator as soon as possible so that protective measures, such as disabling the

device may be employed. Notification must take place within 24 hours. Phones or mobile devices previously used for storing email or other sensitive County information shall be completely purged of all information before being transferred to another employee, returned to the vendor or discarded. Non-County-owned smart phones or mobile devices may only be used to store emails or connect to County IT systems with the written approval of the Department Head or their designee and signed by the owner of the device. Those connecting non-County-owned devices must agree in writing that, should they leave County employment or otherwise have their access revoked by the County, their phone may be reset to factory condition by departmental IT staff. *See 'Email Access Form' located on the last page of this policy.*

e) In the event any County equipment is stolen, or needs replacement, repair or maintenance, County shall be responsible for its replacement, repair or maintenance if the equipment was approved by the Department Head and the telecommuter has provided the proper care and safety of the equipment. If County-owned equipment or property is stolen it is the responsibility of the telecommuter to call the police and obtain a police report number and provide the police report number to the department. If a telecommuter is moving to a new residence and has an existing business telephone line owned by County, the Department and County Telecommunications shall be notified of the move prior to the telecommuter vacating the residence, to ensure the telephone line is disconnected on a timely basis

f) In the event of equipment malfunction, the telecommuter shall notify his/her supervisor immediately. If repairs will take some time, the telecommuter shall be asked to report to a County facility until the equipment is usable.

**10. USER ACCOUNTS**

a ) Business applications shall automatically enforce passwords that reflect this policy whenever possible. Passwords shall consist of at least 6 characters for internal systems and at least 8 characters for Internet accessible systems, mix of alpha (upper and/or lower case), numeric and symbols (with at least 3 of the 4 categories satisfied). Passwords must change at least every 90 days and no sooner than every 10 days. Old passwords shall not be reused. A centralized method for password resets shall be deployed.

b) Accounts shall be disabled or deleted within 24 hours of staff termination, which includes resignation or retirement. In no event shall accounts remain accessible 72 hours after termination. When staff is reassigned within their department or transfer to another department their information systems privileges shall be modified to reflect their new duties or department. This account modification shall be performed within 24 hours of effective reassignment, and the account modification shall be performed within 72 hours of reassignment. It is recommended that any staff member on an approved leave greater than 30 days have their account disabled until they return.

c) Users shall not share accounts and passwords. As those who seek unauthorized access might attempt to mislead a workforce member into divulging their password by claiming that they are County Information Technology staff, passwords shall not be given out to any individual. *(See exceptions to this rule in item e)*

d) Users shall not use their account passwords that are currently in use on County systems with non County systems (e.g. personal email accounts, banking accounts, etc.). *The County recognizes that it is unable to track this on a normal basis. However, it is information that may become known through the course of a data or system breech investigation.*

e) In cases where systems or devices are limited in their ability to provide more than 1 administrator or "privileged" account, that account may be shared with the appropriate staff if determined necessary by the Department Head or their designee. If a system or device that falls into this category is deemed important, necessary or critical to infrastructure, the account and all changes to the password shall be shared with the Department Head or their designee immediately after such change.

## 11. SOFTWARE/HARDWARE INSTALLATION

a) Only designated departmental technical support staff, appointed by the Department Head may install software. Departments may pre-authorize installation of software by other departmental employees for selected software, such as commonly used Internet browser plug-ins. Under no circumstances shall authorization be given to install unlicensed software on county equipment or allow multiple use of single-user software. Technical support staff shall have the authority to delete unauthorized software (including but not limited to screen savers, toolbars, animated programs, games) when detected. In such cases, supervisor(s) will be notified.

b) County staff working on and/or installing County licensed software on private P.C.s is an exceptional circumstance and shall require the prior written approval of the Department Head.

As there is some risk to the County with staff going to private homes, the P.C. (or laptop / tablet computer) shall be brought to the department's I.T.area.

If there are any security or virus issues, the latest copy of virus protection software shall be installed on the P.C. (or laptop) prior to it being connected to the County network. The owner of the private P.C. is responsible for the cost of this software.

Department Head authorization of software installation is not authorization for staff to work from home.

c) All software acquired by or on behalf of the County or developed by County employees or contract personnel on behalf of the County is and shall be deemed County property. All such software shall be used in compliance with applicable licenses, notices, contracts, and agreements. Employees shall not create, obtain, possess, execute, modify, or distribute any computer programs or material in violation of copyright laws.

d) Employees shall not connect any computer hardware, either personally owned or County-owned or network hardware (including, but not limited to, wireless networking hardware) to the Stanislaus County network without Department Head or their designees approval.

## 12. ACCESS

a) Access to Stanislaus County information systems, except for those devoted to public use, shall be authorized only for Stanislaus County workforce members, department approved partners and software programs having a need for specific information in order to accomplish a legitimate task. All such access shall be defined and documented.

b) Appropriate Stanislaus County information system owners, Department Heads or their chosen delegates shall define and authorize all access to Stanislaus County information systems. Such information system owners/stewards and delegates shall be formally designated and documented.

c) Appropriate Stanislaus County information system owners, Department Heads or their designated delegates shall review workforce member and software program access rights to Stanislaus County information systems to ensure that access is granted only to those having a need for specific information in order to accomplish a legitimate task. All access shall be regularly reviewed and revised as necessary.

d) As appropriate, Stanislaus information systems shall support one or more of the following types of access control to protect the confidentiality, integrity and availability of data contained on Stanislaus County information systems:

   i) User based: each user is assigned specific privileges based on their individual status

   ii) Role based: each user is assigned to one or more predefined roles, each of which has been assigned the various privileges needed to perform that role

   iii) Context based: rights are not assigned to users, but are assigned based on the particular circumstances of a transaction

e) As appropriate, security controls or methods that allow access to Stanislaus County information systems shall include, at a minimum:

   i) unique user identifiers (user IDs) and a secret identifier (password) that enable persons and entities to be uniquely identified. User IDs shall not give any indication of the user's privilege level. Group identifiers shall not be used to gain access to Stanislaus County information systems,

   ii) when unique user identifiers are insufficient or inappropriate, group identifiers shall be used to gain access to Stanislaus County information systems upon review by the appropriate owner/controller of the data being accessed,

   iii) the prompt removal or disabling of access methods for persons and entities that no longer need access to Stanislaus County data and information systems,

   iv) logging of changes to the configuration of a network using TACACS+ or similar technology for devices that support logging solutions of this type. The solution should uniquely identify who made the change, when the change was made, and "where possible" a reference number linked to documentation describing and authorizing the

change by whatever party has oversight of the equipment in question.

f) Neither Stanislaus County workforce members nor software programs shall be granted access to Stanislaus County information systems until properly authorized. Only staff formally designated by the Department Head to work on information systems shall connect, move, tamper with or remove computer or network equipment from the Stanislaus County network.

g) Stanislaus County workforce members shall not provide unauthorized users access to Stanislaus County information systems.

h) Special system privileges, such as the ability to bypass normal resource access controls, shall be restricted to those directly responsible for system management and/or security. This access shall be authorized by the Department Head and documented.

i) Access to Stanislaus County information systems shall be managed in order to protect the confidentiality, integrity, and availability of all data. This pertains to any data, code or scripts stored or shared in any form on Stanislaus County owned resources. This includes: electronic information, information on paper and information shared orally or visually (such as telephone and video conferencing). County departments shall have a formal process for granting and reviewing appropriate access to Stanislaus County data and access to other information systems. The process shall include:

   i) capability for authorizing appropriate levels of access to Stanislaus County data and information systems,

   ii) procedure for tracking authorization of access to Stanislaus County data and information systems,

   iii) procedure for regularly reviewing and revising, as necessary, authorization of access to Stanislaus County data and information systems,

   iv) procedure for the Department Head or designee to authorize access to information systems based on both the right and the need to know basis,

j) The type and extent of access authorized to Stanislaus County information systems shall be based on risk analysis. At a minimum, the risk analysis shall consider the following factors:

   i) the importance of the applications running on the information system,

   ii) the value or sensitivity of the data on the information system,

   iii) the extent to which the information system is connected to other information systems

k) Where risk analysis shows it is necessary, appropriate encryption shall be used to protect the confidentiality, integrity and availability of data contained on Stanislaus County information systems. *See Data Encryption Standards page 14.*

l) The Department Head may determine there is a legitimate business need to provide Independent Contractors with access to County data or services. This shall be permitted only if the following requirements are met:

i) Independent Contractors shall enter into an agreement with Stanislaus County prior to accessing any information on the Stanislaus County information systems,

ii) Independent Contractors shall have the minimum access required to complete the tasks assigned,

iii) Independent Contractors access shall be enabled only for the time period required. Whenever possible, access should be configured to automatically expire,

iv) Independent Contractors shall be given a copy of, and comply with, all applicable Stanislaus County IT policies related to information systems,

v) accounts shall be terminated within 8 hours of the last day the Independent Contractor has worked,

vi) the standard work contract with any Independent Contractors who will be given network access shall include a copy of the Department and/or County IT Security policy and it shall include specific language about penalties that will be assessed if the policy is violated.

m) The Department shall maintain documentation on Independent Contractors who have been given network access, with appropriate detail (IP/MAC address being used, duration and terms of their access). Appropriate background investigations will be conducted on contractors who have access to sensitive information such as the Criminal Justice information systems.

n) Departments may have a legitimate business need for department employees and/or Independent Contractors to perform work from their homes or a remote site and may use the Internet as the network medium for providing said access. Remote access shall be permitted only if all of the Access requirements are met as well as the following requirements:

i) Stanislaus County Human Resources Policies regarding employees working from home shall be observed,

ii) encryption standards for Internet communications shall be employed. *See Data Encryption Standards page 14*

iii) remote access implementations shall include suitable encryption and logging of authentication attempts, both success and failures. Such logs shall be stored centrally and reviewed regularly by system administrators,

iv) analog access shall be used with Department Head approval only,

v) two-factor authentication shall be implemented for all remote access activity when possible. This frequently takes the form of smart card or biometrics systems,

vi) Remote access implementations using VPN's shall prohibit "Split-Tunnels" when connecting from non County owned devices or when County owned devices are connected to non County owned networks. The Department Head or their designee, may authorize "Split-Tunnels on a case by case basis if a critical need for such is determined."

o) The Department Head shall determine that there is a legitimate business need to allow remote control access of County systems from the Internet, either for Departmental IT staff or for Independent Contractors. This shall be permitted only if the following requirements are met:

i) any remote control mechanism shall have logging capabilities, logs shall be stored external from the device being remotely controlled

ii) in the situation where a Department has a legitimate business need to allow remote control to be performed by someone other than the local logged in user, that Department shall have a documented procedure for permitting this activity. The procedure, at a minimum, will address who may perform such remote control and under what circumstances. It is understood that there may be legitimate business needs for allowing such remote control, e.g. for system maintenance. However, as allowing such remote control provides significant opportunity for abuse and circumvention of sound security procedures, its use is discouraged

iii) when remote control is being performed by someone other than the local logged in user, the session shall be of limited duration, with a County employee monitoring the access and ensuring that it is properly terminated. Auto logins or user account caching for remote access systems is prohibited.

## 13. ASSESSMENT/AUDIT

a) An annual risk assessment report shall be created for every department and must be stored in a secure manner. The risk assessment shall contain defined categories of risk such as:

i) highly sensitive: areas where large amounts of confidential data is stored and maintained

ii) sensitive: areas where terminals are located which can access highly sensitive data,

iii) public access: areas where the general public has direct physical access to devices connected to the County data network.

b) Self-administered audits shall be performed at least once annually. Self-administered audits will also be performed when events trigger such actions. Events that trigger such actions would include such things as changes in network topology, changes in server software or hardware configurations, or changes in operational procedures.

c) Peer and External audits shall be performed at a minimum, biennially. A core peer group made up of internal County personnel will perform peer audits with Department Head approval, knowledge and coordination. External audits shall be performed by an independent non- biased third party vendor external from the County with Department Head approval, knowledge and coordination.

d) Stanislaus County shall provide a standard automated assessment tool to facilitate the auditing process and provide consistency. The Information Technology Security SIG will determine the requirements for such a system and the processes and procedures for its use.

e) A County-wide IT Assessment team shall be formed and shall perform penetration testing on a regular basis to determine if existing security controls are effectively protecting the County's information technology systems. No penetration testing shall be performed without Department Head approval, knowledge and coordination. Each member of the team conducting penetration testing shall have previously passed a background check appropriate for the Department and information system being tested.

f) All audit results shall be reported to the specific Department. Any results that identify County security issues shall be shared with the IT Security Manager and the Security SIG.

g) Departments shall be able to identify departmental expenses related to ongoing security needs, in accordance with guidelines to be developed by the Security SIG.

h) Stanislaus County departments shall identify and audit all access controls used to protect information technology systems annually. The audit shall be provided to the Stanislaus County Security Special Interest Group where appropriate. The annual report shall be stored in a secure manner (e.g. appropriate file access permissions are employed).

## 14. PERIMETER SECURITY

The County-Wide Area Network encompasses the data networks of Stanislaus County agencies. Any potential weakness at any County agency, has the ability of compromising every other County data system. There is a recognized need for some County agencies to have external network connections with partners, with the State of California, with the Federal Government and to the Internet. These links create weaknesses that shall be addressed. All perimeter security shall be protected by access controls.

a) All network security mechanisms shall at a minimum provide the following safeguards:

   i) permit only the traffic required,

   ii) must be hardened to deter compromise,

   iii) default configurations, especially in regard to system authentication shall be replaced with reasonable alternatives,

   iv) logs of all pertinent traffic permitted through the access controls shall be kept and

stored separate from the access controls,

v) a current detailed network diagram of the connection to the County network, describing its purpose and defining security measures taken shall be provided to the County IT Security Manager unless an exception is approved by the CEO.

b) Wireless data networking solutions connected to the Stanislaus County Wide Area Network extend the WAN, sometimes beyond the confines of Stanislaus County properties. Therefore, more stringent security measures shall be employed. At a minimum, wireless data network implementations will:

i) use appropriate encryption, *See Data Encryption Standards page 14*

ii) require authentication, such as the IEEE 802.1x specification which deals with enhanced security,

iii) use non-default configurations for Admin account password and Service Set Identifier (SSID). The SSID should be non-descriptive so that a casual user could not identify to whom the network belongs,

iv) not allow administration from the wireless interface. Administration may only be permitted through the wired interface of the device,

v) adjust power levels such that the radio signal does not extend further than necessary,

vi) log all access, preferably to a device on the wired network.

c) Wireless data network components should also:

i) filter traffic such that only required services are supported,

ii) suppress SSID advertisements,

iii) filter devices based on pre-determined MAC addresses.

## 15. UPDATES/PATCH MANAGEMENT

a) Operating Systems and mission-critical applications shall be updated on a regular basis. There are several components to Updating/Patch Management:

i) determining when updates are available,

ii) testing updates to determine what benefit/risk is associated with them,

iii) deploying updates in a timely fashion once it has been determined that it is safe to do

so,

iv) track which systems the update has been delivered to.

b) Each Department shall have a documented procedure for how updates/patch management is to be performed and monitored.

## 16. DATA ENCRYPTION STANDARDS

a) For local traffic that does not leave the Stanislaus County Wide Area network encryption mechanisms that are deemed acceptable include 3DES, AES, and SSL.

b) For wireless data networking components such as wireless access points, wireless bridges and wireless peer-to-peer networking, the strongest supported encryption method should be employed. At a minimum Wi-Fi Protected Access 2 (WPA2) shall be used. *See also Perimeter Security page 12.*

c) Where Stanislaus County data does or might reasonably traverse a non-Stanislaus County-owned network, such as the Internet, American Encryption Standards (AES) or 256-bit Secure Socket Layer shall be employed.

d) Stronger encryption methods shall be employed, but all encryption methods that vary from these Standards must be documented and reported to the Department Head and may be provided to the IT Security Manager and the Security SIG upon request.

## Stanislaus County

**Request for Access to the County Email System via an Email Client on a Personal Mobile Device**

## REQUEST SECTION

I, _____ (print name) hereby request Stanislaus County Email access on the following device:

| |
|---|
| Device Name: (use one request per system) |
| Device Type: (Apple iPhone / iPad, Android phone or tablet PC, Blackberry, etc) |
| Device Serial Number: |

Your signature is an indication that you have read and will abide by the Stanislaus County IT Security Policy, the Stanislaus County Data Destruction Policy and the security requirements of this request.

### Data Destruction Requirements:

Non-County-owned PDAs, smart phones and other portable computing devices may only be used to store emails or connect to County IT systems with the written approval of the Department Head and signed by the owner of the device. Those connecting non-County-owned devices to County systems or otherwise storing County email on such devices must agree in writing that, should they leave County employment or otherwise have their access revoked by the County, they agree to delete all County data from their device. If the County is not confident that the data has been deleted, the County will have the right to verify the task and delete any data items that the County believes it owns. This may include a restore to factory defaults for some devices.

### Device Security Requirements:

1. A security passcode will be required to access the device at all times.
2. The device must be set to time out and require the passcode after 30 minutes of inactivity.
3. In addition to the passcode, a mechanism must be in place to automatically erase all data or render the device useless (Device Locking State), if too many passcode attempts are made. For devices that are configurable, no more than 10 passcode attemps will be allowed.
4. In order to prevent unauthorized access to County email systems the responsible party will also notify the County immediately if the device is lost or stolen.

**Disclaimer:** County staff will not be held responsible for any damage to the device, device failures, personal data loss or personal configurations when setting up access to County email or when troubleshooting. The County assumes no liability or responsibility for your personal mobile device, its data or the software that is contained on it. Device may be subject to public records requests.

_____ _____

Signature (Requester) Date

| **Department Head:** | **Dept:** | **Approval Signature:** | **Date:** |
|---|---|---|---|
| | | | |

**Approver's Comments:**

_____