

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

DEPT: CHIEF EXECUTIVE OFFICE

BOARD AGENDA # *B-8

Urgent Routine **X**

AGENDA DATE October 16, 2001

CEO Concurs with Recommendation YES **Mark** NO
(Information Attached)

4/5 Vote Required YES NO

SUBJECT:

ADOPTION OF STANISLAUS COUNTY INFORMATION TECHNOLOGY SECURITY POLICY

STAFF
RECOMMEN-
DATIONS:

1. ADOPT THE ATTACHED STANISLAUS COUNTY INFORMATION TECHNOLOGY SECURITY POLICY FOR ALL COUNTY DEPARTMENTS

FISCAL
IMPACT:

Currently, Departments do not identify their individual Information Technology (I.T.) costs, the fiscal impact can not be directly assessed. However, most departments are already involved in I.T. security and this policy should not significantly increase costs. Departments will need to make the implementation of this policy a priority in their budgets.

BOARD ACTION AS FOLLOWS:

No. 2001-808

On motion of Supervisor Caruso , Seconded by Supervisor Blom
and approved by the following vote,

Ayes: Supervisors: Mayfield, Blom, Simon, Caruso, and Chair Paul

Noes: Supervisors: None

Excused or Absent: Supervisors: None

Abstaining: Supervisor: None

1) X Approved as recommended

2) Denied

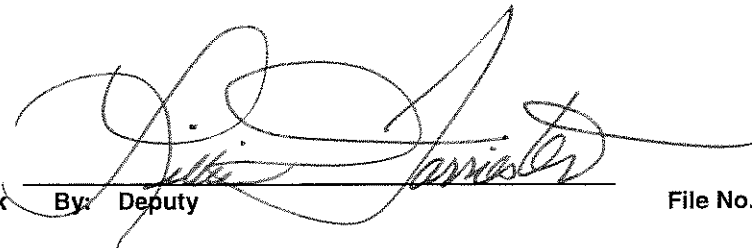
3) Approved as amended

MOTION:

ATTEST: CHRISTINE FERRARO TALLMAN, Clerk

By: Deputy

File No.



DISCUSSION: There is currently no I.T. security policy in place for the County. Up to this point, I.T. security has not been managed countywide. As a result, a Special Interest Group (SIG), consisting of staff from each department selected by each department head, met and developed a countywide policy for I.T. security. Business risk issues and the importance of protecting the citizens' information were an integral part of this process. Once the SIG had completed the policy, it was circulated to all department heads for comment and then ratified in their September department head meeting.

The policy does not proscribe tasks for each department, but defines security requirements expected of each. There will be an audit to ensure the policy has been followed.

Once a year, the security SIG will meet, review the policy, and where required, change the policy to improve security for the County's I.T. systems.

POLICY ISSUE: The citizens of Stanislaus County entrust important personal and business information to the County. As such, the County must ensure that it is careful with this information and that it is protected and secured consistent with the Board goal of promoting efficient government operations. Without citizens' confidence, the County will not be able to successfully implement E-government initiatives. Consequently, the County's Information Technology Strategic Plan will not be successful without an effective security policy.

**STAFFING
IMPACT:**

There are no staffing impacts associated with this action. An I.T. security role will be created in each department and performed by existing staff.



Stanislaus County – I.T. Security Policy

August 20, 2001

Security Special Interest Group

BACKGROUND

There is currently no policy on Information Technology (I.T.) security in Stanislaus County Government. There have been attempts, by some departments to deal with the issue, which have not always been effective and have resulted in a fragmented application of I.T. security.

I.T. security has not been a primary focus of management, due to lack of understanding of the problem and that business management sees it as an I.T. technical issue.

With no funding specifically provided for I.T. security management, there is little ongoing training in security or an awareness of the risks by users and technical staff. As there has been no crisis to this point, there has been little management involvement.

As I.T. is now part of the daily operation of our departments, the lack of security is most certainly a major business risk which must be well managed.

THE GOALS

The goal of this policy is that in order to protect the information we have on our I. T. systems (mainly about our citizens), we must ensure that good I.T. security management practice is in place. As well as complying with Federal and State laws and regulations, we must protect all I.T. assets by balancing high security with the access needs of the authorized customers and staff, while ensuring we refuse access to unauthorized users.

THE SCOPE

The scope of this document is to define a Countywide I.T. security policy, which will establish a baseline standard by which all departments can manage their I.T. security. Departments may then wish to enhance their policies and standards from the baseline.

The definition of I.T. security is :

The protection of the citizens' data and our I.T. assets by management of the access to the network, hardware, software and data by implementing good practice security processes and technology. The personal accountability of all staff will be required if I.T. security is to be effective.

THE STRATEGIC CONTEXT

While failure to properly manage I.T. security creates a legal risk for the organization, a greater risk is that of losing the confidence of our citizens in our ability to be a good custodian of their information. Without citizen confidence, our E-Government strategy (ITSP) will not be possible. Our organizational investments, especially in new technology, must be managed like any other business risk.

CURRENT SECURITY ISSUES

Staff

There is currently resistance by some staff and departmental management to I.T. security being applied to business systems. As a result, our systems are too open to external networks and staff are not well trained in security.

Management

We do not know the current effectiveness of our I.T. security. It is not separately funded in our budgets, resulting in a lack of resources and training to ensure security. There is no clear accountability for security in some areas. The business needs are given priority over security requirements, without balancing the need for access with the need for security. There is no one person responsible for the overall security of our Countywide I.T. systems – no organizational security officer.

Lack of Security Processes

Currently, there are few formal processes to manage I.T. security, with no contingency, response plan or enforcement process if security is broken.

Changes in legislation, the signing of new contracts with new access requirements or changes in new technology are not assessed for their impact on our I.T. security.

Security is not part of our H.R. processes either in the induction or the handling of at-risk employees. When staff with high-level access leave, they do not have their access shut down nor are the system passwords changed. Security processes have not addressed introducing new software to the County's network by staff from the Internet.

Processes for the physical security (of I.T. assets) have not been completed.

Processes for virus management have not been uniformly developed or applied, which is also critical for remote access use (including Internet Service Providers).

Business Partners (County, State, Federal)

Our lack of a robust, implemented I.T. security policy is compromising our business partners' I.T. networks and data.

POLICY STATEMENTS

Security Management : General

- ◆ Security will be designed to be as user friendly as possible.
- ◆ An annual Countywide security audit will be completed by an independent entity.
- ◆ There will be an individual accountable for the role of security officer who will coordinate technical assistance, ensure the security audits are complete and be responsible for keeping track of new technologies as well as State and Federal requirements.
- ◆ The Security Special Interest Group (SIG), which is responsible for developing this policy, will be the clearing entity for security policy and standards. It will meet as necessary to ensure our security policies and standards remain up to date.

Security Management – Departmental

- ◆ Department heads are responsible for security in their respective areas.
- ◆ Each department will develop and implement processes for identifying, recording and reporting each security violation.
- ◆ Security funding will be identified in the departmental annual operating budget.
- ◆ Each department will update their business continuity plan to assess and repair damage done from security breaches.
- ◆ Implementation of new technology will require a formal security impact assessment signed by the department head before implementation.
- ◆ Each department will ensure there will be a security partnership agreement consistent with this policy signed off with each external agency.
- ◆ Each department will ensure that all external users will be required to accept a terms and conditions agreement before access to the County's network is given.

Human Resources Processes

- ◆ A security review to determine compliance will be added to the employee's annual evaluation process.
- ◆ A standard staff security training course will be provided for all new and current employees.

Viruses

- ◆ Virus protection software, updated daily, will be on every PC, mobile devices (laptop) and appropriate servers.
- ◆ All media, files, attachments, emails, and downloads introduced to the network must be scanned for viruses.

Telecommuting

- ◆ This security policy applies to both telecommuters and the equipment used.
- ◆ There is a shortlist of approved network connection methods: terminal server, firewall protected internet, VPN, and a managed modem environment.

- ◆ All remote users must be authenticated and the confidential data encrypted.
- ◆ It's the responsibility of the telecommuter to insure that their remote work environment is consistent with County policies and standards.

Network Interconnection

- ◆ Any connection between LAN and external networks must insure that there is a firewall at our end and the organization on the other end has implemented robust security (which has been verified by the security officer). This does not apply to point-to-point networks.

Physical Security

- ◆ Servers and network equipment need to have their own separate secure facility with carefully restricted access.
- ◆ Mobile devices (including laptops) which are missing must be reported to security staff immediately. The owner or borrower of the mobile device is responsible for its security.
- ◆ Confidential data on new mobile devices (including laptops) should be password protected and/or encrypted.
- ◆ Public should not be able to view confidential data on a personal computer (PC) in a public place. Before staff leave a PC, which has access to confidential information in a public place, they must secure access.

Staff Access

- ◆ The HR designee will be responsible to ensure that new staff will read the security policy and sign an agreement acknowledging that they understood and will abide by it before network access is provided.
- ◆ The manager must authorize the systems they want the staff member to have access to. The manager is also responsible for keeping the security person up to date with changes in access to the various systems.
- ◆ The authorization rights must be documented and kept by the person responsible for security.
- ◆ On receiving a resignation or release, the HR designee must immediately notify the person responsible for security of the date the staff member is leaving. The person responsible for security must ensure all rights are withdrawn on this date.
- ◆ When staff with high level access leave all system passwords must be changed.

Internet Applications

- ◆ All public web applications must have industry standard security (SSL) implemented if connected to the rest of the network.
- ◆ When designing new applications, security must be included from the beginning and balanced with ease of access.