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

DEPT: Chief Executive Office **BOARD AGENDA #** *B-1

Urgent ☐ **Routine** ☒ **AGENDA DATE** January 26, 2010

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

SUBJECT:

Approval of Electronic Data Destruction Policy

STAFF RECOMMENDATIONS:

Approve the Electronic Data Destruction Policy.

FISCAL IMPACT:

By implementing this Data Destruction Policy, we will increase data protection in the County and can appropriately reuse County computer assets. This can assist in the reduction of costs of purchasing additional computer assets.

BOARD ACTION AS FOLLOWS:

No. 2010-042

On motion of Supervisor O'Brien, **Seconded by Supervisor** DeMartini
and approved by the following vote,
Ayes: Supervisors: O'Brien, Chiesa, Monteith, DeMartini, and Chairman Grover
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:

Christine Ferraro

ATTEST: **CHRISTINE FERRARO TALLMAN, Clerk** **File No.**

DISCUSSION:

This proposed Policy (attached) would provide guidance for departments on the appropriate methods of disposing of electronic devices such as computers, file servers, and cellular telephones to ensure that sensitive or confidential County data has been verifiably removed from those devices prior to the equipment being transferred out of a County department, either to be used elsewhere or to be auctioned to the public.

There have been numerous instances in other agencies of governmental data being inadvertently and inappropriately disclosed because the equipment on which that data was stored was transferred from the governmental agency responsible for safeguarding that data. Simply re-formatting the hard drive of a computer does not permanently delete the data that was stored on the device. However, it is also not necessary in most cases to resort to physically destroying the hard drive, thus reducing the value of the computer for other uses.

This proposed Policy would require County departments to formally identify which computers in use store (or could reasonably be assumed to store) data classified by that department as Highly Sensitive, Sensitive, or Public Access. This Policy requires that all computers defined as likely containing Highly Sensitive data have their hard drives removed and physically destroyed. Those containing Sensitive or Public Access data will have that information removed according to a procedure in compliance with Department of Defense standards, but which is not physically damaging to the hard drive.

Having an appropriate solution to ensuring appropriate and considered protection of County data allows for responsible reuse of County electronic assets. Allowing other divisions, departments or even non-County non-profit entities to make use of County computer equipment that no longer meets the original purpose for which it was purchased is a responsible measure in reducing waste. Some County tasks require state-of-the-art computer systems, for example, and require that those systems be replaced frequently to facilitate service delivery. Those computers that are deemed underpowered for their initial use may still provide years of functional use in other applications. Once the data is appropriately cleansed from those systems, they become eligible for reuse elsewhere.

Draft versions of this Policy were instigated by the County Information Security Special Interest Group, shared with County Information Technology Managers and ultimately approved by the County Information Technology Steering Committee. County Department Heads have also reviewed this Policy.

This effort will standardize computer data destruction processes in the County, increase data protection and support appropriate reuse of County computer assets.

POLICY ISSUES

The Board of Supervisors is asked to consider whether this proposed Policy will provide for the more effective use of County resources and promote the efficient delivery of public services.

STAFFING IMPACT

There is no staffing impact associated with this item.

STANISLAUS COUNTY
BOARD OF SUPERVISORS' RESOLUTION
APPROVED / RESOLUTION #
DATA DESTRUCTION POLICY

Introduction

Safeguarding the data belonging to the citizens of Stanislaus County and under the care of the departments of Stanislaus County is a serious obligation. The Efficient Delivery of Public Services Board of Supervisors' Priority has long focused on appropriate and judicious implementation of Information Technology Security Best Practices. Exercising due diligence in protecting County data that resides on electronic storage media as covered in this Policy is an important step in meeting the expectations of stakeholders in regards to Information Technology security.

Purpose of the Policy

Data stored electronically on County systems must be verifiably removed prior to the device(s) on which it is stored leaving the control of the department owning the data in question. Stanislaus County has an obligation to its citizens and must follow legal mandates as well to ensure that sensitive data not be transferred to third parties who should not be exposed to such data. This policy describes the steps necessary to ensure that data is appropriately destroyed prior to any transfer.

Policy Approval Process

The Data Destruction Policy approval process is as follows. The policy was developed in conjunction with the Stanislaus County Security Special Interest Group. The draft policy was approved by the Information Technology Steering Committee on August 20, 2009. The Chief Information Officer will present the recommended policy to the Board of Supervisors for final approval.

Applicable Parties/Parties & Responsibilities

The policy applies to all County Departments.

Policy Statements

Data Classification and Destruction

Each County department shall be responsible for identifying data classes based on their relative sensitivity. The following classifications should be used though not all departments will necessarily have data in all three classes. For example, many departments may not find it useful to distinguish between "Highly Sensitive" and

"Sensitive" classes; for those departments it may be sufficient to classify data as either "Sensitive" or "Public Access".

Highly Sensitive: For devices storing data deemed "Highly Sensitive", complete destruction of the device using a compliant destruction method is required. File servers that may serve as aggregation points for different categories of Sensitive data may be considered "Highly Sensitive" and the storage devices associated with those servers would then be required to be destroyed completely. Appropriate methods of destruction include incineration, crushing, spindling and dissolving in acid. Whatever method of destruction is employed must be documented in the department's "Procedure for Data Destruction" and kept on file with the Chief Information Officer.

Sensitive: For devices storing data deemed "Sensitive", an acceptable data destruction program that is compliant with the U.S. Department of Defense specification DoD 5220-22M will be administered on the device. A record of the data destruction shall be attached to the device. Only those devices that have a data destruction record attached may be transferred from the department. Where the departmental data destruction method (as documented in the department's "Procedure for Data Destruction") lacks the ability to produce a record of data destruction, the department shall use a "two-pass" system. On the first pass, the device will receive a "Red" sticker indicating an initial data destruction process was carried out. On the second pass, the device will receive a "Blue" sticker indicating the final data destruction process has been administered and the device is now ready to be discarded or reused. This process shall be employed by all County departments before transferring any device identified as having stored, or possibly having stored "Sensitive" information.

Public Access: The mechanism for handling data destruction for devices on which Public Access ("Non-Sensitive") data is in all ways identical to that for "Sensitive" data.

Transfer

The data destruction requirements defined in this Policy apply in all of the following scenarios:

- The device is transferred to the General Services Agency for sale as Salvage;
- The device is transferred to another department for re-use;
- The device is transferred to any non-County agency; and/or
- The device otherwise leaves the control of the department that classified the data on the system initially.

As well, departments may find themselves in circumstances where it is unclear whether data destruction should occur. In those situations, the department should confer with

the County Information Security Manager or the Chief Information Officer for guidance. In general, it is preferable to destroy the data than to inadvertently allow sensitive data to leave the County's control. Standard labels shall be employed to clearly indicate that the device has either been appropriately wiped (in the case of Public Access or Sensitive classifications for that device) or that no permanent storage remains inside the device (i.e., the storage device has been removed and is either slated for physical destruction or wipe, or else the storage device has already been appropriately disposed of). Without such labels, General Services Agency will not accept computers or mobile computing devices for storage or Salvage.

Where the County does not own the equipment on which the data is being stored, care should be taken to ensure that Sensitive or Highly Sensitive data is not stored on such equipment, or otherwise put in place an agreement with the owner of the equipment for appropriate cleansing of all record of County data before the equipment leaves County use.

Cellular Phones and Other Portable Computing Devices

Lost devices in this category must be reported to the department telecom coordinator or Information Technology staff as soon as possible so that protective measures, such as disabling the device, may be employed. That notification must occur within 24 hours of discovery of the loss. 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 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.

County-owned cellular phones and portable computer devices must be wiped of all County data if they are identified as having stored or of possibly having stored Sensitive or Highly Sensitive data. A reliable data erase and overwrite must be conducted on such devices associated with Sensitive data and a physical destruction of the device must be performed on those associated with Highly Sensitive data. In either case, the Subscriber Identity Module ("SIM") must be removed and either securely wiped and overwritten or else physically destroyed.

If no appropriate data wiping method exists for the individual device, the device should not be permitted to store County data or else it must be physically destroyed when no longer required for County service.

Precedence

This policy does not supersede or override any regulations promulgated by State or Federal agencies that are more stringent or impose additional requirements than this policy.

Systems Covered by this policy

This policy will apply to all electronic data storage devices including, but not limited to, magnetic tapes, laptop and desktop computer and file server hard drives and flash memory devices, copiers and printers containing hard drives, cellular phones, personal data assistants (PDAs) and other portable computing and electronic storage devices.

Implementation of Policy

Upon approval of this policy by the Board of Supervisors, all departments will be expected to adhere to this policy as it is written. All exceptions shall not violate any of the written County policy and must be approved by the department head and the Board of Supervisors prior to implementation.

In the event that two organizations with differing policies interface, the highest level of security shall prevail. Should additional viable mechanisms for data destruction become available, they will be evaluated by the Chief Information Officer and may become usable by County departments. The Chief Information officer shall maintain a list of all acceptable methods of data destruction by data classification level.

Review Period

It has been determined by the policy team that this policy will be reviewed annually until determined otherwise by the policy team. Should additional methods of data destruction be approved by the Chief Information Officer, those methods shall be incorporated into any future revisions of this policy.