



# COUNTY OF SACRAMENTO

## Inter-Departmental Correspondence

**For the Agenda of: March 1, 2007**

Date: January 30, 2007

To: Information Technology Policy Board Members

From: Debbie Nadolna, Chair  
Technology Review Group

Subject: Public Access Computers Security (PACS) Policy and Standards

### **Recommendation:**

- Approve the Public Access Computers Security Policy
- Approve the Public Access Computers Security Standards described in Appendix A

### **Background:**

County of Sacramento departments and agencies provide quicker and more efficient service to the walk-in public by providing public access computers in facilities convenient to the public. The need to provide prompt and courteous service to the public is of utmost concern of the County of Sacramento.

Recent advancements in technology have revolutionized the way the County does business. The digitalization of routine tasks and the increased need to collect and disseminate information have brought to the forefront the need to provide the public with access to submit or retrieve electronic data stored by the County of Sacramento computer systems. Providing the public with access to the County of Sacramento's electronic data comes with obvious inherent risks that can be successfully managed and mitigated with the cooperation and collaboration of all departments. However, there is currently no policy or set of standards for consistent implementation of public access computers.

The concern of the lack of a security policy or standards was brought to the TRG for discussion and direction. A team was formed to develop the policy and standards for public access computers security. The team consisted of the following individuals:

Felix Flores	OCIT
Bryan Door	PSD
Fred D'Amico	Voter Registration
John Grigg	Probation
Christopher Ireland	DHA
Doug Kudlick	Finance
Mark Stuart	Assessor
Jason Spackman	MSA
John Hinkley	Sheriff's Department
Lewis Walker	Superior Court

The team researched and analyzed various documents from other organizations both public and private to help in determining the content of the policy and standards.

## Discussion:

Public access computer systems are defined as any computer system made physically available to or accessible by the public for accessing County data and/or the internet. The purpose of the policy and standards documented below are to secure County data and systems from unauthorized access. The policy and standards which govern making County data and systems accessible to constituents are documented in other County policies.

It is important for the security of the County of Sacramento networks, computer systems, and data to protect them from potential malicious use and/or theft. Due to the nature of public access computers being exposed to the public, and the need to put them in convenient locations accessible by the public, it is important to have a common set of policies and standards that help protect the County's assets and data.

## Scope:

This document defines the policies and standards related to the secure implementation and management of all County of Sacramento public access computer systems. This policy provides direction to ensure that the County of Sacramento has done its due diligence to protect the County networks, computer systems and data from anonymous public access through the use of County supplied and approved public access computer systems.

This policy applies to all public access computers connected to County of Sacramento resources and data. This includes all County departments and agencies.

This policy applies to all organizational units, employees, contractors, and others implementing and managing public access computers with access to the County network infrastructures.

This policy applies to all public access computers currently in existence and any new systems acquired after the effective date of this policy document. Existing public access computers must become compliant within **180** days from the date of approval of this policy by the ITPB and the County Executive (CEO).

## **Policy Statement:**

1. Public access computer systems will be physically secured to prevent theft or malicious use.
2. Public access computer systems must restrict access to County of Sacramento data and services based on the approved and designated function of the device.
3. Implementation of security on any public access computer system will meet or exceed the Minimum Security Standards defined in *Appendix A* of this document.
4. All new implementations of, or architectural modifications to any public access computer must be reviewed and approved for compliance to the policy and standards in this document before implementation.
5. A post implementation review of any new public access computer system or any public access computer system that has been architecturally modified will be performed to verify compliance with the policy and standards of this document.
6. Ongoing regular security audits will be conducted of the public access computer system's security to ensure compliance to the policies and standards in this document.
7. Any public access computer system(s) found to pose a significant risk to other information systems, any individual's identity or privacy, or found not in compliance with this policy must be removed from service until such time the risk or non-compliance can be mitigated.
8. The Security Perimeter Team will be responsible for ensuring the compliance of the policy and standards in this document. The Security Perimeter Team will perform compliance reviews, as stated in this document, in coordination with the applicable department implementing public access computers.

## **Policy Updates:**

Regular assessments will be conducted on these policies and standards to validate relevance and applicability to the current environment. A review team will be assembled consisting of a member of the Security Perimeter Team and representatives solicited from the County Departments.

Requests for changes to this public access computers security policy will be submitted to the TRG for review and recommendation to the ITPB for approval.

## **Impact of Implementing the Policy:**

This policy and standards may require changes to existing public access computers to become compliant. Support staff awareness is critical and training may be needed.

# Appendix A

## Public Access Computers Security (PACS) Standards

### Minimum Security Standards

This section identifies minimum standards for securely deploying Public Access Computers throughout the county for use by the county constituents.

#### **Physical Standards**

1. Public access computer cases will be locked or located in a physically secure location (i.e. closet, cabinet, or other immobile secure container.)
2. All unneeded I/O and storage devices will be disabled and/or removed.
3. Boot devices and Boot order will be modified to prevent boot from removable media unless needed by design.
4. BIOS admin password will be applied.
5. LAN jacks and other network connections must be protected from tampering.

#### **Network Standards**

1. All un-needed network protocols will be removed from the public access computer system.
2. WAN connected public access computer systems will use static or reserved/manual DHCP IP Addresses.
3. MAC address filtering will be applied on the connecting switch for all WAN connected public access computer systems.
4. Wireless Devices will comply with County of Sacramento, Wireless Data Networking Policy and Standards.
5. WAN connected public access computers will be configured to route all traffic through a firewall. The firewall will be configured to only allow access to the resources necessary for the device's function.
6. WAN connected public access computers will be isolated from WAN resources using isolated network segments.

## **Operating System Standards**

1. Antivirus software will be installed and kept current on all systems.
2. Host based firewall will be implemented.
3. Systems will be maintained to current security patch levels.
4. Public access computers that need to access web sites will use host or network based filtering to restrict access to only the required web sites.
5. All unneeded applications, services, and operating system components will be disabled or removed.
6. No public access computer will allow the copying of data to or from removable media unless required by the application.
7. Public access computers will use a non-admin, restricted logon for public use.
8. Public access computer systems will not store personal, protected, or private information.