#

**Kiosk Security Policy**

Version: 2.1

**TABLE OF CONTENTS**

Purpose 3

Scope 3

System Boot 3

Data Storage and Backup 3

Memory Protection 3

Network Security Controls 4

Physical Security Controls 4

Minimum Components 4

Restricted User Environment 4

User Logon 5

Event Logging 5

Review & Revision 5

Enforcement 5

Exceptions 5

## Purpose

The purpose of this document is to list the specific security controls that are applied to all kiosks at ACME.

## Scope

This document applies to computer systems at ACME that meet all of the following conditions:

1. Runs a single defined application (or very few defined applications)
2. Presents a limited end-user interface and offers strictly limited functionality
3. Is intended to be used by multiple individuals

Depending upon the intended use of the particular kiosk system, kiosk users can include any combination of employees, contractors, vendors, and customers.

Kiosks, if not managed exclusively by ACME IT, are subject to this policy and the “Third Party Managed Systems Policy.”

Windows XP, UNIX, or Linux based kiosk systems are subject to this policy and their matching OS Policy if they are managed entirely by ACME IT.

Windows XP Embedded (XPe) based kiosk systems are subject to this policy and the “Windows XP Embedded Policy.”

ACME’s retail POS 469x system and ACME Fuel Systems are not in scope.

## System Boot

The system must boot from a trusted source. Use strong controls to prevent an unauthorized individual from changing the boot device. Use physical or logical controls to prevent access to the BIOS and device ports.

A reboot should automatically restore all configuration settings back to their normal operating parameters.

## Data Storage and Backup

Systems in scope may process, but should not store, information that is classified as ACME Confidential or ACME Restricted.

Keep local data storage on the device to a minimum. Data backups are not recommended. Use secure disk wiping processes to erase any traces of Confidential or Restricted data that must momentarily pass through the system. Format all local storage with the most robust and most secure file system natively available (where technically feasible).

Systems that, for operational reasons, must store Confidential or Restricted data 1.) will require a formal signed exception from ACME Information Security and 2.) will be subjected to additional compensating security requirements provided by ACME Information Security.

Reference ACME’s Information Asset Management Policy for more information on ACME’s data classification.

## Memory Protection

Use memory protection options that mark certain areas of memory as non-executable (e.g. stack overflow protection, buffer overflow protection, no-execute features) where technically feasible.

The operating system and appliation must fail in a secure manner, meaning that the system integrity must be preserved during a software malfunction. Software malfunctions must not expose critical data such as payment information, passwords or encryption keys either through onscreen debugging information, log files, or memory dump files.

## Network Security Controls

Use a centrally managed host firewall (where technically feasible). Disable, block, or remove all unused network ports and services (inbound and outbound).

Systems in a **retail facility** must follow VLAN assignment rules:

* Systems that are managed exclusively by ACME IT or by a ACME subsidiary and that do not access or process payment or patient information belong in store VLAN 212 (Main Store VLAN).
* Third Party Managed Systems that do not access or process payment or patient information belong in store VLAN 36 (General Extranet VLAN).
* Systems that access or process payment or patient information will be highly scrutinized prior to VLAN assignment and will also be subjected to additional compensating security requirements provided by ACME Information Security.

## Physical Security Controls

Use physical security controls to prevent unauthorized access to the device and its storage media. Protect physical device ports and connections (e.g. USB, PS2, serial, parallel, 1394, floppy, zip, CD-ROM, and others) from unauthorized access or manipulation. Disable unused physical device ports (if technically feasible). Lock the entire unit including all peripherals inside a secured cabinet or box to prevent unauthorized access (where physically possible).

Publicly facing systems that process ACME Confidential or ACME Restricted data must employ a strategy to minimize the risk of unintentional disclosure through ‘shoulder surfing’ and other direct observation techniques.

## Minimum Components

Eliminate all unnecessary services. Ensure that the operating system and other software contain only the necessary components.

## Restricted User Environment

Users are not allowed to have administrative access to the system.

The system must present a severely restricted user environment. Users can not exit to a desktop, command prompt, or any other administrative tool. All unnecessary components should be removed or hidden and restricted from use by end users. All unnecessary permissions must be removed from the user’s session.

Do not maintain persistence between user sessions. When the user terminates or completes a session, the screen or display should refresh and all data from the previous session should be erased. Users should be able to manually initiate a screen wipe or terminate their session so they feel confident about walking away from the kiosk.

A 10 minute inactivity timeout will return the system to the start or welcome screen. All user initiated applications will be gracefully closed after this timeout.

## User Logon

Authenticate the user (through the application and/or the operating system) if the kiosk system allows the user to access informaton classified as ACME Internal, ACME Confidential, or ACME Restricted. Kiosks that only allow the user to submit their own information (e.g. name, payment information, phone, address) do not require authentication.

## Event Logging

Forward operating system log events (e.g. including access and authorization events), in real time, to ACME’s central logging infrastructure (if technicaly feasible).

Forward application log events (e.g. access and authorization events), in real time, to ACME’s central logging infrastructure (if technically feasible).

Log the connection and disconnection of keyboards and USB storage devices (where technically feasible).

Systems are exempt from logging requirements if they 1.) do not connect to ACME’s network and 2.) only process information that is classified as Public.

## Review & Revision

This policy will be reviewed and revised annually.

## Enforcement

Strict compliance with this policy is essential for the effective protection of ACME. Any violation will be forwarded to the appropriate manager, Information Security, and HR representative for appropriate action up to and including termination of employment.

## Exceptions

ACME Information Security must approve any exceptions to this policy. You can initiate the security exception process by sending a detailed email to the following email address: security@acme.com