#

**Third Party Managed Systems Policy**

Version: 1.0f

**Revised:** March 25, 2009

**TABLE OF CONTENTS**

Purpose 3

Scope 3

Legal Agreements 3

Periodic Review and Validation 3

Remote Access 3

Physical Access 3

System Management Strategy 3

Software and Configuration Management 4

Data Storage and Backup 4

Encryption 4

Memory Protection 4

Malware Protection 4

Network Security Controls 5

Minimum Components 5

Restricted User Environment 5

Event Logging 5

Windows Security Settings 5

UNIX Security Settings 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 computers at ACME that are not exclusively managed by ACME.

## Scope

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

1. Connects directly to ACME’s internal network through either a wired or wireless connection
2. Is not managed exclusively by ACME IT or by a ACME subsidiary
3. Is not a personally-owned computer or device

A **third party** is any business entity that performs IT services on behalf of ACME. If a third party is responsible for one or more aspect of a computer system then it is considered a third party managed system. This includes, but is not limited to management of the application, middleware, database, operating system, or hardware platform.

## Legal Agreements

Third party organizations must comply with specific ACME Legal and Security requirements prior to commissioning any third party managed systems.

Two legal documents are required prior to granting administrative level access to a third party: Master Services Agreement (MSA) and Vendor Security Agreement (VSA).

The MSA must thoroughly define an unambiguous device management strategy if a third party will manage any aspect of the computer system’s lifecycle. The specific managed items must be thoroughly defined between ACME and the third party.

## Periodic Review and Validation

ACME reserves the right to periodically validate the third party managed system meets all of the requirements in this policy. Validation procedures include, but are not limited to, vulnerability scanning, penetration testing, network monitoring, and other forms of system audits.

## Remote Access

* Remote network access must go through an ACME managed remote access portal.
* Traditional VPN network access not permitted except in cases where application portal access is un-suitable.
* Analog modems are not permitted.

## Physical Access

* Physical access to retail facilities, to perform computer systems maintenance, repair, or troubleshooting tasks, must be approved and coordinated with ACME IT prior to coming on site.
* Physical access to data center facilities must be approved and coordinated with the data center manager.

## Authentication Strategy

Use ACME’s authentication infrastructure such as Radius, TACACS, LDAP, AD, and Two-Factor (where operationally necessary and practical).

Local password repositories are deprecated and will be highly scrutinized and subject to additional compensating security requirements provided by ACME Information Security.

## Availability Monitoring

Use ACME’s system monitoring and backup infrastructure (e.g. Tivoli, and Symantec Net Backup) (where operationally necessary and practical).

## Software (including OS) Management

Use one of three approved methods outlined below for software (e.g. operating system, firmware, drivers, run-time image, application updates and patches) deployment, updates, and management.

1.) *Use ACME Infrastructure.* Utilize ACME’s existing system management infrastructure (e.g.SMS, SUS, WSUS, and HP Opsware).

*2.) Use run-time image replacement*. Replace the entire image on a device with an updated run-time image. Update the run-time image at least once per quarter and include all current patches and application updates. Be capable of pushing an urgent update within 24 hours if requested by ACME.

3.) *Use a separate enterprise software management system.* Use a managed software update solution to coordinate and track all software deployment and updates. Apply software updates uniformly across all devices that perform the same role. Update the system software at least once per quarter and include all current patches and application updates. Be capable of pushing an urgent update within 24 hours if requested by ACME.

Manual or ad-hock image updating is not permitted.

## Configuration Change Management

Use a centrally managed system configuration control strategy to ensure that only authorized system configuration changes (e.g. permissions, init scripts, system registry, startup folder, and others) can be performed.

## Data Storage and Backup

Keep local data storage on the device to a minimum. 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).

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

## Encryption

Use online storage encrypiton and network session encryption if the system stores information that is classified as or ACME Restricted. Use robust, centralized key management policies and practices. Use only FIPS-approved cryptographic algorithms (e.g. AES, 3DES, DSA, RSA, ECDSA, and SHA-1).

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

## Memory Protection

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.

## Malicious Software Protection

Use a centrally managed and monitored malicious software protection solution that protects against viruses, worms, Trojan horses, rootkits, backdoors, spyware, botnets, keystroke loggers, dialers and data-stealing malware. Update it at least every 90 days and be capable of pushing an urgent update within 24 hours if requested by ACME. Send status alerts and alarms to the central console.

## 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 **North American facility** must follow VLAN assignment rules:

* Third Party Managed Systems that do not access or process payment or patient information belong in store VLAN 6 (Extranet VLAN).
* Third Party Managed 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.

Systems in a **data center** facility must be connected to a server layer switch that has a firewall service module. Depending upon the identified risk of the system, specific firewall rules may be mandated by Information Security.

## 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.

## 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).

## Windows Security Settings

The following controls apply only to Third Party Managed computers that are not a member of any ACME Windows Domain.

* General user accounts must only be ‘Domain Accounts’, not local to workstations or servers.
	+ Local Guest and Administrator accounts are **exempt** from this requirement.
	+ Application-specific accounts may be created on servers if required for proper functioning of an approved application.
* The Users local group must only contain a global group such as Domain Users.
* All user accounts, with the exception of the built in accounts of guest and administrator, must be in global groups only.
	+ Global groups should be assigned to local groups.
* The renamed Administrator account must be the only user account in the Administrators local group.
* User accounts must never appear in local groups or be directly specified in the Access Control List (ACL) for any object.
* Universal groups should be used to define functional groups that span domains. In order to reduce replication traffic, nest global groups within universal groups and make membership changes in the global groups. If only a single domain is present, universal groups should not be utilized.
* Users must only be members of the administrative groups if absolutely necessary. If necessary, delegation must be used to limit administrator access to specific OUs. Administrative groups include:
	+ Enterprise Administrators
	+ Schema Administrators
	+ Domain Administrators
* Implement “Restricted Groups” to enforce membership to critical system groups.
* Set the Account Lockout threshold to “6”.
* The console must only be logged in to as needed by authorized support personnel.
* The console must automatically lock after a certain period of inactivity.
* Remote server console access must be restricted to authorized support personnel and its use must be limited according to business necessity.
* The registry should be secured such that unauthorized users cannot modify the list of programs that are run upon startup.
* Remove any unnecessary or insecure services and/or protocols. These are examples of services or protocols that should be turned off, but which may be enabled if there is a valid reason for turning them on:
	+ Remote Access Server
	+ FTP Publishing Service
	+ Simple Mail Transport Protocol
	+ World Wide Web Publishing Service
	+ Microsoft Distributed Transaction Coordinator (MSDTC)
	+ Indexing Service
	+ Internet Information Services
	+ Management and Monitoring Tools
	+ Message Queuing Services
	+ Other Network File and Print Services
	+ Networking Services
	+ Remote Installation Services
	+ Remote Storage
	+ Script Debugger
	+ Terminal Services Licensing
	+ Windows Media Services
	+ AppleTalk
	+ DLC
	+ NetBEUI
	+ Network Monitor
	+ SNMP must be disabled.

## UNIX Security Settings

Third Party Managed computers that run UNIX or Linux must comply with the controls in the corresponding ACME UNIX or Linux OS security policies.

## 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.