

ACME CORPORATION

Physical Security Standard

Prepared by Information Security

Dawn Murphy

2011

MINNEAPOLIS MINNESOTA

Physical Security Standard

Contents

1. Overview	3
1.1 Scope.....	3
1.2 Scope Limitations	3
2. Related Internal Policies.....	3
3. Additional Requirements	3
3.1 Document Review	3
3.2 Duty to Report Suspected Policy Violations.....	3
3.3 Lockbox Pin Rotation	4
4. External References and Supporting Documentation	4
4.1 PCI-DSS Specific Requirements	4
4.2 Client Specific Requirements	4
5. Standard Information Section.....	4
5.1 User Access to Information Processing Facilities.....	4
5.1.1 User Identification Badge Required	4
5.1.1.1 Visibility of Badges	4
5.1.2 Access Card Required.....	4
5.1.3 Access Limits	5
5.2 Visitor Access to Information Processing Facilities.....	5
5.2.1 Visitor Definition	5
5.2.2 Visitor Badge Information.....	6

1. Overview

The purpose of the *Acme Corp Physical Security Standard* document (this "Standard") is to define and describe the requirements and controls necessary for creating and maintaining a secure computing facility.

1.1 Scope

The standards and guidelines described herein apply to all Acme Corp individuals and processes that support the physical security controls implemented to protect all Acme Corp offices and VeriSpace-based Acme Corp data center. Without limiting the generality of the foregoing, all employees, consultants, and contractors, whether permanent or temporary, full-time or part-time domestic or international (collectively, "Users") must comply with this Standard. Portions of the Standard are more restrictive in scope than others, but all Users should read this Standard in its entirety.

1.2 Scope Limitations

This Standard does not apply to the Berbee data center in Brooklyn Park, MN or the Level 3 data center in Austin, TX.

2. Related Internal Policies

- *Acme Corp Information Resource User Responsibilities*
- *Acme Corp Information Security Policy*
- *Acme Corp Incident Response Plan*

3. Additional Requirements

The following sections describe the additional requirements that are necessary to implement and achieve compliance with this Standard.

3.1 Document Review

This Standard must be reviewed for necessary changes and updated accordingly at least every 7 months from the creation of the document, or at last **Intermediate** or **Major** version change, or any time the governing policy has changed.

Document review, updating and approval must follow the process described in *Information Security Document Creation and Update Process* document.

3.2 Duty to Report Suspected Policy Violations

All suspected violations of this Standard and all suspected security breaches must be reported as quickly as possible by contacting Acme Corp Information

Physical Security Standard

Security. Contact information can be found on the Acme Corp Information Security ePoint site.

3.3 Lockbox Pin Rotation

For any lockbox which is used to protect keys, the pin must be changed at least every year or directly after the departure of anyone who knew the pin. Additionally, the pin must be different than the last 12 pins used.

4. External References and Supporting Documentation

- *ISO/IEC Standard 27002-2005 (17799)*
- *The Payment Card Industry Data Security Standard v1.2 (PCI-DSS)*

4.1 PCI-DSS Specific Requirements

All settings and controls which are explicitly required by the PCI-DSS are denoted by coloring the text in RGB value 84, 141, 212, followed by the PCI-DSS section number.

4.2 Client Specific Requirements

All settings and controls which are explicitly required by Acme Corp Behavioral Analytics Service clients are denoted by coloring the text in MS Word 2007 in Red, Accent 2, and Darker 25%.

5. Standard Information Section

The following sections detail the requirements for allowing User Access to any Acme Corp Information Processing Facility.

5.1 User Access to Information Processing Facilities

5.1.1 User Identification Badge Required

All users are required to obtain and display an Acme Corp-issued Identification badge while on-premise at any Acme Corp Information Processing Facility. (PCI-DSS 9.2)

5.1.1.1 Visibility of Badges

User Badges must be worn in a visible position at all times while on-premise at any Acme Corp Information Processing Facility. (PCI-DSS 9.2)

5.1.2 Access Card Required

Access to all Acme Corp Information Processing Facilities must be secured, at a minimum, by an access card reader, and as such, all Users are required to

Physical Security Standard

obtain an Acme Corp-issued access card. Users will be allowed access to facilities via assigned access cards. (PCI-DSS 9.2)

5.1.2.1 Access Card Request Process

All access cards must be requested via the process and procedures described in the Acme Corp Physical Access Request Process document. No access card will be issued without an accompanying approval request.

5.1.3 Access Limits

A User's access is limited to those Information Processing Facilities, days and times that were requested and approved for them by the resource owner as part of the physical access request process.

5.1.3.1 Access Change

If a User requires access other than what they have been granted, a new request for the access must be submitted and approved before the User can gain access.

Further information regarding this process can be found in the *Acme Corp Physical Access Request Process* document.

5.1.3.2 Access Card Control

All physical access that has been granted, via access cards, must be reviewed annually, this review must consist of contacting the approvers with a list of existing access rights for review and reaffirm that the access is necessary and granted. The approval/reaffirmation must be conducted using a track-able mechanism.

5.2 Visitor Access to Information Processing Facilities

The following sections detail the requirements for allowing and tracking visitor access to any Acme Corp Information Processing Facility.

5.2.1 Visitor Definition

Acme Corp defines a visitor as any non-User. Visitors include, but are not limited to; vendors, guests of regular employees, clients and prospective clients, or anyone who needs to enter the facility for a short duration, usually not more than a day, and not covered within other parts of this Standard.

5.2.2 Visitor Badge Information

All visitors are required to obtain and wear an Acme Corp-issued visitor identification badge while on-premise at any Acme Corp Information Processing Facility, (PCE-DSS 9.3.2)

The only exception to this is in the case of deliveries to the facility or shipping of packages from the facility (see section 5.2.3 below for further information). No visitor is allowed beyond the front desk or reception area without obtaining a visitor badge.

5.2.2.1 Government-issued Photo ID Required

All visitors must show a government-issued photo ID in order to obtain a visitor badge (PCI-DSS 9.3.1)

5.2.2.1.1 Government-issued Photo ID Exception

In the event that a visitor is under the age of 16 and thus cannot obtain a Government-issued photo ID, the person being visited must vouch for this visitor. In doing so, all actions taken by the visitor are the responsibility of the visited party, including all penalties incurred as a result of the visitor's actions.

5.2.2.2 Sign in Required

All visitors must sign into a Visitor Access Log, which will track the following *information* (PCI-DSS 9.4)

- Date and time of the visit
- Visitor's name
- Visitor's badge number
- Name of the person or organization visited
- Purpose of the visit
- Data Center visit
- Record of ID check
- Badge return check

If a visitor is unable to sign into the Visitor Access Log, then it is the responsibility of the person who is being visited to complete the log on their behalf.

5.2.2.3 Vendor Badge Control

For all information Processing Facility locations, Acme Corp Information Security will designate one individual to be in charge of all

Physical Security Standard

visitor badge issuance and collection (the "Visitor Badge Primary"), including ID checks, log maintenance, and badge creation.

Additionally, to accommodate for instances where the Visitor Badge Primary is not available, Acme Corp Information Security will designate an individual to act as the backup (the "Visitor Badge Backup").