Table of Contents

ACME Platform SSP

# ACME Platform overview

This is the frontmatter for the ACME System Security Plan

# Control responses and guidance

## Access Control (AC)

### AC-1 - Access Control Policy and Procedures

#### Control Statement

The organization:

* [a.] Develops, documents, and disseminates to executives:
  + [1.] An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
  + [2.] Procedures to facilitate the implementation of the access control policy and associated access controls; and
* [b.] Reviews and updates the current:
  + [1.] Access control policy monthly; and
  + [2.] Access control procedures weekly.

#### AC-1 Summary information

###### Table of Parameters

| Parameter ID | Values | Label or Choices |
| --- | --- | --- |
| ac-1\_prm\_1 | executives | organization-defined personnel or roles |
| ac-1\_prm\_2 | monthly | organization-defined frequency |
| ac-1\_prm\_3 | weekly | organization-defined frequency |

#### What is the solution and how is it implemented?

### AC-2 - Account Management

#### Control Statement

The organization:

* [a.] Identifies and selects the following types of information system accounts to support organizational missions/business functions: privileged;
* [b.] Assigns account managers for information system accounts;
* [c.] Establishes conditions for group and role membership;
* [d.] Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
* [e.] Requires approvals by ACME interal method for requests to create information system accounts;
* [f.] Creates, enables, modifies, disables, and removes information system accounts in accordance with standard operations;
* [g.] Monitors the use of information system accounts;
* [h.] Notifies account managers:
  + [1.] When accounts are no longer required;
  + [2.] When users are terminated or transferred; and
  + [3.] When individual information system usage or need-to-know changes;
* [i.] Authorizes access to the information system based on:
  + [1.] A valid access authorization;
  + [2.] Intended system usage; and
  + [3.] Other attributes as required by the organization or associated missions/business functions;
* [j.] Reviews accounts for compliance with account management requirements daily; and
* [k.] Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

#### AC-2 Summary information

###### Table of Parameters

| Parameter ID | Values | Label or Choices |
| --- | --- | --- |
| ac-2\_prm\_1 | privileged | organization-defined information system account types |
| ac-2\_prm\_2 | ACME interal method | organization-defined personnel or roles |
| ac-2\_prm\_3 | standard operations | organization-defined procedures or conditions |
| ac-2\_prm\_4 | daily | organization-defined frequency |

#### What is the solution and how is it implemented?

## Custom Controls (CC)

### CC-1 - Energy consumption

#### Control Statement

All services should report energy consumed by their service.

#### Summary information

#### What is the solution and how is it implemented?

### CC-2 - Carbon reporting

#### Control Statement

All services must calculate and report total scope 3 energy consumption.

#### Summary information

#### What is the solution and how is it implemented?

## Identification and Authentication (IA)

### IA-5(1) - Password-based Authentication

#### Control Statement

The information system, for password-based authentication:

* [(a)] Enforces minimum password complexity of blocking the flow of the encrypted information, ACME internal method;
* [(b)] Enforces at least the following number of changed characters when new passwords are created: ACME internal method;
* [(c)] Stores and transmits only cryptographically-protected passwords;
* [(d)] Enforces password minimum and maximum lifetime restrictions of ACME improved method;
* [(e)] Prohibits password reuse for ACME final method generations; and
* [(f)] Allows the use of a temporary password for system logons with an immediate change to a permanent password.

#### IA-5(1) Summary information

###### Table of Parameters

| Parameter ID | Values | Label or Choices |
| --- | --- | --- |
| ia-5.1\_prm\_1 | blocking the flow of the encrypted information, ACME internal method | organization-defined requirements for case sensitivity, number of characters, mix of upper-case letters, lower-case letters, numbers, and special characters, including minimum requirements for each type |
| ia-5.1\_prm\_2 | ACME internal method | organization-defined number |
| ia-5.1\_prm\_3 | ACME improved method | organization-defined numbers for lifetime minimum, lifetime maximum |
| ia-5.1\_prm\_4 | ACME final method | organization-defined number |

#### What is the solution and how is it implemented?

### IA-5(4) - Automated Support for Password Strength Determination

#### Control Statement

The organization employs automated tools to determine if password authenticators are sufficiently strong to satisfy assistants.

#### IA-5(4) Summary information

###### Table of Parameters

| Parameter ID | Values | Label or Choices |
| --- | --- | --- |
| ia-5.4\_prm\_1 | assistants | organization-defined personnel or roles |

#### What is the solution and how is it implemented?

## Privilege Rating (PR)

### PR-1 - Right to access and deletion of records

#### Control Statement

Any service or offering MUST:

* [a] Have a privacy focal to respond to deletion requests.
* [b] Have an automated method for allowing users to access all of their data
* [c] Have an automated method to allow users to request, and subsequently execute, deletion of personal records.
* [d] The process must be documented.

#### Summary information

#### What is the solution and how is it implemented?

### PR-2 - Registering exemptions to right to delete

#### Control Statement

#### Summary information

#### What is the solution and how is it implemented?

## System and Communications Protection (SC)

### SC-1 - System and Communications Protection Policy and Procedures

#### Control Statement

The organization:

* [a.] Develops, documents, and disseminates to as needed:
  + [1.] A system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
  + [2.] Procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls; and
* [b.] Reviews and updates the current:
  + [1.] System and communications protection policy hourly; and
  + [2.] System and communications protection procedures bi-monthly.

#### SC-1 Summary information

###### Table of Parameters

| Parameter ID | Values | Label or Choices |
| --- | --- | --- |
| sc-1\_prm\_1 | as needed | organization-defined personnel or roles |
| sc-1\_prm\_2 | hourly | organization-defined frequency |
| sc-1\_prm\_3 | bi-monthly | organization-defined frequency |

#### What is the solution and how is it implemented?

### SC-2 - Application Partitioning

#### Control Statement

The information system separates user functionality (including user interface services) from information system management functionality.

#### SC-2 Summary information

#### What is the solution and how is it implemented?