Table of Contents

ACME Platform SSP

# ACME Platform overview

# Control responses and guidance

## Access Control (AC)

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

#### Control Statement

The organization:

* [a] Develops, documents, and disseminates to organization-defined personnel or roles:
  + [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 organization-defined frequency; and
  + [2] Access control procedures organization-defined frequency.

#### AC-1 Summary information

| Parameter ID | Value |
| --- | --- |
| ac-1\_prm\_1 | organization-defined personnel or roles |
| ac-1\_prm\_2 | organization-defined frequency |
| ac-1\_prm\_3 | organization-defined frequency |

##### FedRamp Implementation Status.

* Implemented
* Partially implemented
* Planned
* Alternative implementation
* Not Applicable

##### FedRamp Control Origination.

* Service provider Corporate
* Service provider System Specific
* Service Provider Hybrid (Corporate and System Specific)
* Configured by Customer (Customer System Specific)
* Provided by Customer (Customer System Specific)
* Shared (Service Provider and Customer Responsibility)
* Inherited from pre-existing FedRAMP Authorization [Enter text here], Date of Authorization

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

##### Part a.

ACME CISO is responsible for updating documentation on intranet.acme.com/ciso/access-control, on an annual basis. This website becomes the single source of truth for all access-control policies.

##### Part b.

Add control implementation description here for item ac-1\_smt.b

### 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: organization-defined information system account types;
* [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 organization-defined personnel or roles for requests to create information system accounts;
* [f] Creates, enables, modifies, disables, and removes information system accounts in accordance with organization-defined procedures or conditions;
* [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 organization-defined frequency; and
* [k] Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

#### AC-2 Summary information

| Parameter ID | Value |
| --- | --- |
| ac-2\_prm\_1 | organization-defined information system account types |
| ac-2\_prm\_2 | organization-defined personnel or roles |
| ac-2\_prm\_3 | organization-defined procedures or conditions |
| ac-2\_prm\_4 | organization-defined frequency |

##### FedRamp Implementation Status.

* Implemented
* Partially implemented
* Planned
* Alternative implementation
* Not Applicable

##### FedRamp Control Origination.

* Service provider Corporate
* Service provider System Specific
* Service Provider Hybrid (Corporate and System Specific)
* Configured by Customer (Customer System Specific)
* Provided by Customer (Customer System Specific)
* Shared (Service Provider and Customer Responsibility)
* Inherited from pre-existing FedRAMP Authorization [Enter text here], Date of Authorization

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

##### Part a.

Add control implementation description here for item ac-2\_smt.a

##### Part b.

Add control implementation description here for item ac-2\_smt.b

##### Part c.

Add control implementation description here for item ac-2\_smt.c

##### Part d.

Add control implementation description here for item ac-2\_smt.d

##### Part e.

Add control implementation description here for item ac-2\_smt.e

##### Part f.

Add control implementation description here for item ac-2\_smt.f

##### Part g.

Add control implementation description here for item ac-2\_smt.g

##### Part h.

Add control implementation description here for item ac-2\_smt.h

##### Part i.

Add control implementation description here for item ac-2\_smt.i

##### Part j.

Add control implementation description here for item ac-2\_smt.j

##### Part k.

Add control implementation description here for item ac-2\_smt.k

### AC-2(1) - Automated System Account Management

#### Control Statement

The organization employs automated mechanisms to support the management of information system accounts.

#### AC-2(1) Summary information

##### FedRamp Implementation Status.

* Implemented
* Partially implemented
* Planned
* Alternative implementation
* Not Applicable

##### FedRamp Control Origination.

* Service provider Corporate
* Service provider System Specific
* Service Provider Hybrid (Corporate and System Specific)
* Configured by Customer (Customer System Specific)
* Provided by Customer (Customer System Specific)
* Shared (Service Provider and Customer Responsibility)
* Inherited from pre-existing FedRAMP Authorization [Enter text here], Date of Authorization

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

Add control implementation description here for control ac-2.1

## System and Communications Protection (SC)

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

#### Control Statement

The organization:

* [a] Develops, documents, and disseminates to organization-defined personnel or roles:
  + [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 organization-defined frequency; and
  + [2] System and communications protection procedures organization-defined frequency.

#### SC-1 Summary information

| Parameter ID | Value |
| --- | --- |
| sc-1\_prm\_1 | organization-defined personnel or roles |
| sc-1\_prm\_2 | organization-defined frequency |
| sc-1\_prm\_3 | organization-defined frequency |

##### FedRamp Implementation Status.

* Implemented
* Partially implemented
* Planned
* Alternative implementation
* Not Applicable

##### FedRamp Control Origination.

* Service provider Corporate
* Service provider System Specific
* Service Provider Hybrid (Corporate and System Specific)
* Configured by Customer (Customer System Specific)
* Provided by Customer (Customer System Specific)
* Shared (Service Provider and Customer Responsibility)
* Inherited from pre-existing FedRAMP Authorization [Enter text here], Date of Authorization

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

##### Part a.

Add control implementation description here for item sc-1\_smt.a

##### Part b.

Add control implementation description here for item sc-1\_smt.b

### 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

##### FedRamp Implementation Status.

* Implemented
* Partially implemented
* Planned
* Alternative implementation
* Not Applicable

##### FedRamp Control Origination.

* Service provider Corporate
* Service provider System Specific
* Service Provider Hybrid (Corporate and System Specific)
* Configured by Customer (Customer System Specific)
* Provided by Customer (Customer System Specific)
* Shared (Service Provider and Customer Responsibility)
* Inherited from pre-existing FedRAMP Authorization [Enter text here], Date of Authorization

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

Add control implementation description here for control sc-2

## Custom Controls (CC)

### CC-1 - Energy consumption

#### Control Statement

All services should report energy consumed by their service.

#### Summary information

##### FedRamp Implementation Status.

* Implemented
* Partially implemented
* Planned
* Alternative implementation
* Not Applicable

##### FedRamp Control Origination.

* Service provider Corporate
* Service provider System Specific
* Service Provider Hybrid (Corporate and System Specific)
* Configured by Customer (Customer System Specific)
* Provided by Customer (Customer System Specific)
* Shared (Service Provider and Customer Responsibility)
* Inherited from pre-existing FedRAMP Authorization [Enter text here], Date of Authorization

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

Add control implementation description here for control cc-1

### CC-2 - Carbon reporting

#### Control Statement

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

#### Summary information

##### FedRamp Implementation Status.

* Implemented
* Partially implemented
* Planned
* Alternative implementation
* Not Applicable

##### FedRamp Control Origination.

* Service provider Corporate
* Service provider System Specific
* Service Provider Hybrid (Corporate and System Specific)
* Configured by Customer (Customer System Specific)
* Provided by Customer (Customer System Specific)
* Shared (Service Provider and Customer Responsibility)
* Inherited from pre-existing FedRAMP Authorization [Enter text here], Date of Authorization

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

Add control implementation description here for control cc-2

## 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

##### FedRamp Implementation Status.

* Implemented
* Partially implemented
* Planned
* Alternative implementation
* Not Applicable

##### FedRamp Control Origination.

* Service provider Corporate
* Service provider System Specific
* Service Provider Hybrid (Corporate and System Specific)
* Configured by Customer (Customer System Specific)
* Provided by Customer (Customer System Specific)
* Shared (Service Provider and Customer Responsibility)
* Inherited from pre-existing FedRAMP Authorization [Enter text here], Date of Authorization

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

##### Part a

Add control implementation description here for item pr-1\_smt.a

##### Part b

Add control implementation description here for item pr-1\_smt.b

##### Part c

Add control implementation description here for item pr-1\_smt.c

##### Part d

Add control implementation description here for item pr-1\_smt.d

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

#### Control Statement

#### Summary information

##### FedRamp Implementation Status.

* Implemented
* Partially implemented
* Planned
* Alternative implementation
* Not Applicable

##### FedRamp Control Origination.

* Service provider Corporate
* Service provider System Specific
* Service Provider Hybrid (Corporate and System Specific)
* Configured by Customer (Customer System Specific)
* Provided by Customer (Customer System Specific)
* Shared (Service Provider and Customer Responsibility)
* Inherited from pre-existing FedRAMP Authorization [Enter text here], Date of Authorization

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

Add control implementation description here for control pr-2