Account Management (AC-2)

The organization:

1. Identifies and selects the following types of information system accounts to support organizational missions/business functions: [*Assignment: organization-defined information system account types*];
2. Assigns account managers for information system accounts;
3. Establishes conditions for group and role membership;
4. 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;
5. Requires approvals by [*Assignment: organization-defined personnel or roles*] for requests to create information system accounts;
6. Creates, enables, modifies, disables, and removes information system accounts in accordance with [*Assignment: organization-defined procedures or conditions*];
7. Monitors the use of information system accounts;
8. 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;
9. 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;
10. Reviews accounts for compliance with account management requirements [*FedRAMP Assignment: at least annually*]; and
11. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

| AC-2 | Control Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter AC-2(a): | |
| Parameter AC-2(e): | |
| Parameter AC-2(f): | |
| Parameter AC-2(j) | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| AC-2 What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |
| Part d |  |
| Part e |  |
| Part f |  |
| Part g |  |
| Part h |  |
| Part i |  |
| Part j |  |
| Part k |  |

Control Enhancement AC-2 (1)

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

| AC-2 (1) Control Enhancement Summary Information |
| --- |
| Responsible Role: |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable |
| Control Origination (check all that apply):  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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> |

| AC-2 (1) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement AC-2 (2)

The information system automatically [*Selection: removes; disables*] temporary and emergency accounts after [*FedRAMP Assignment: no more than 30 days for temporary and emergency account types*].

| AC-2 (2) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter AC-2(2)-1: | |
| Parameter AC-2(2)-2: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| AC-2 (2) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement AC-2 (3)

The information system automatically disables inactive accounts after [*FedRAMP Assignment: 90 days for user accounts*].

**AC-2 (3) Parameter Requirement:** The service provider defines the time period for non-user accounts (e.g., accounts associated with devices). The time periods are approved and accepted by the Authorizing Official.

|  |  |
| --- | --- |
| AC-2 (3) | Control Enhancement Summary Information |
| Responsible Role: | |
| Parameter AC-2(3): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Configured by customer  Not applicable | |
| Control Origination (check all that apply):  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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| AC-2 (3) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement AC-2 (4)

The information system automatically audits account creation, modification, enabling, disabling, and removal actions, and notifies [*Assignment: organization-defined personnel or roles*].

| AC-2 (4) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter AC-2(4): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| AC-2 (4) What is the solutions and how is it implemented? |
| --- |
|  |

Control Enhancement AC-2 (5)

The organization requires that users log out when [*Assignment: organization-defined time-period of expected inactivity or description of when to log out*].

| AC-2 (5) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter AC-2(5): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| AC-2 (5) What is the solutions and how is it implemented? |
| --- |
|  |

Control Enhancement AC-2 (7)

The organization:

1. Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles;
2. Monitors privileged role assignments; and
3. Takes [*Assignment: organization-defined actions*] when privileged role assignments are no longer appropriate.

| AC-2 (7) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter AC-2(7)(c): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| AC-2 (7) What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |
| Part c |  |

Control Enhancement AC-2 (9)

The organization only permits the use of shared/group accounts that meet [*Assignment: organization-defined conditions for establishing shared/group accounts*].

**AC-2 (9) Additional FedRAMP Requirements and Guidance:** Required if shared/group accounts are deployed.

| AC-2 (9) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter AC-2(9): | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| AC-2 (9) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement AC-2 (10)

The information system terminates shared/group account credentials when members leave the group.

**AC-2 (10) Additional FedRAMP Requirements and Guidance:** Required if shared/group accounts are deployed.

| AC-2 (10) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| AC-2 (10) What is the solution and how is it implemented? |
| --- |
|  |

Control Enhancement AC-2 (12)

The organization:

1. Monitors information system accounts for [*Assignment: organization-defined atypical use*]; and
2. Reports atypical usage of information system accounts to [*Assignment: organization-defined personnel or roles*].

**AC-2 (12)(a) and AC-2 (12)(b) Additional FedRAMP Requirements and Guidance:** Required for privileged accounts.

| AC-2 (12) | Control Enhancement Summary Information |
| --- | --- |
| Responsible Role: | |
| Parameter AC-2(12)(a) | |
| Parameter AC-2(12)(b) | |
| Implementation Status (check all that apply):  Implemented  Partially implemented  Planned  Alternative implementation  Not applicable | |
| Control Origination (check all that apply):  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 Provisional Authorization (PA) for <**Information System Abbreviation**>, <**Date of PA**> | |

| AC-2 (12) What is the solution and how is it implemented? | |
| --- | --- |
| Part a |  |
| Part b |  |