**Account Management Procedure**

**COMPANY NAME**

**Version #**

**Last Revision Date:**

Document Classification

**Table of Contents**

[1.0 - System Identification 3](#_Toc46816869)

[1.1 - System Name 3](#_Toc46816870)

[1.2 - System Categorization 3](#_Toc46816871)

[1.3 – Responsible Organization 3](#_Toc46816872)

[1.4 – System Roles & Responsibilities 3](#_Toc46816873)

[1.5 - Contracts Containing CUI 4](#_Toc46816874)

[2.0 - System Environment & Boundaries 4](#_Toc46816875)

[2.1 - General Description / Purpose of System 4](#_Toc46816876)

[2.2 - Operating / Hosting Model 4](#_Toc46816877)

[2.3 - System Environment Overview 5](#_Toc46816878)

[2.4 - System Components (Hardware / Software) 5](#_Toc46816879)

[2.5 - System / Network Boundaries 5](#_Toc46816880)

[2.6 - High-Level System Architecture Diagram 5](#_Toc46816881)

[2.7 - System Life Cycle (SDLC) 5](#_Toc46816882)

[3.0 - Security Requirements 6](#_Toc46816883)

[3.1 – Security Requirements 6](#_Toc46816884)

**Procedure Information**

|  |  |
| --- | --- |
| **Prepared By** | |
| **Name:** |  |
| **Department / Title:** |  |
| **Email Address:** |  |
| **Phone #:** |  |

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Revision Date** | **Description** | **Pages Affected** |
| 1.0 | [DATE] | Initial version of procedure | All |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Policy Requirement Reference

|  |  |  |
| --- | --- | --- |
| **Control #** | **Control Description / Requirement** | **NIST 800-53** |
| **3.1.1** | Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). | AC-2 AC-17 |
| **3.1.2** | Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | AC-3 |
| **3.1.4** | Separate the duties of individuals to reduce the risk of malevolent activity without collusion. | AC-5 |
| **3.1.5** | Employ the principle of least privilege, including for specific security functions and privileged accounts. | AC-6 AC-6(1) AC-6(5) |
| **3.1.6** | Use non-privileged accounts or roles when accessing non-security functions. | AC-6(2) |
| **3.3.2** | Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions. | AU-2 AU-3 AU-3(1) Au-6 AU-12 |
| **3.3.8** | Protect audit information and audit tools from unauthorized access, modification, and deletion. | AU-9 |
| **3.4.5** | Define, document, approve, and enforce physical and logical access restrictions associated with changes to the information system. | CM-5 |
| **3.5.1** | Identify information system users, processes acting on behalf of users, or devices. | IA-2 |
| **3.5.2** | Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems. | IA-5 |
| **3.5.3** | Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts. | IA-2(1) IA-2(2) IA-2(3) |
| **3.5.5** | Prevent reuse of identifiers for a defined period. | IA-4 |
| **3.5.6** | Disable identifiers after a defined period of inactivity. | IA-4 |
| **3.5.7** | Enforce a minimum password complexity and change of characters when new passwords are created. | IA-5(1) |
| **3.5.8** | Prohibit password reuse for a specified number of generations. | IA-5(1) |
| **3.5.9** | Allow temporary password use for system logons with an immediate change to a permanent password. | IA-5(1) |
| **3.9.2** | Ensure that CUI and information systems containing CUI are protected during and after personnel actions such as terminations and transfers. | PS-4 PS-5 |

Procedure

The Organization:

1. Identify Systems this is applicable to