**Network Configuration 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** |
| **3.1.3** | Control the flow of CUI in accordance with approved authorizations. | AC-4 |
| **3.1.13** | Employ cryptographic mechanisms to protect the confidentiality of remote access sessions. | AC-17(2) |
| **3.1.14** | Route remote access via managed access control points. | AC-17(3) |
| **3.13.1** | Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems. | SC-7 |
| **3.13.3** | Separate user functionality from information system management functionality. | SC-2 |
| **3.13.4** | Prevent unauthorized and unintended information transfer via shared system resources. | SC-4 |
| **3.13.5** | Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks. | SC-7 |
| **3.13.6** | Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception). | SC-7(5) |
| **3.13.7** | Prevent remote devices from simultaneously establishing non-remote connections with the information system and communicating via some other connection to resources in external networks. | SC-7(7) |
| **3.13.8** | Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards. | SC-8 Sc-8(1) |
| **3.13.9** | Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity. | SC-10 |
| **3.13.10** | Establish and manage cryptographic keys for cryptography employed in the information system. | SC-12 |
| **3.13.11** | Employ FIPS-validated cryptography when used to protect the confidentiality of CUI. | SC-13 |
| **3.13.12** | Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device. | SC-15 |
| **3.13.14** | Control and monitor the use of Voice over Internet Protocol (VoIP) technologies. | SC-19 |

Procedure

The Organization: