**Risk 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** |
| **3.11.1** | Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of CUI. | RA-3 |
| **3.12.1** | Periodically assess the security controls in organizational information systems to determine if the controls are effective in their application. | CA-2 |
| **3.12.2** | Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems. | CA-5 |
| **3.12.3** | Monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls. | CA-7 |
| **3.12.4** | Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems. | PL-2 |
| **3.13.2** | Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems. | SA-8 |

Procedure

The Organization: