**System Security Plan (SSP)**

**COMPANY NAME**

**Information System Name**

**Version #**

**Plan Date**

Document Classification

**Table of Contents**

[1.0 - System Identification 3](#_Toc58097144)

[1.1 - System Name 3](#_Toc58097145)

[1.2 - System Categorization 3](#_Toc58097146)

[1.3 – Responsible Organization 3](#_Toc58097147)

[1.4 – System Roles & Responsibilities 3](#_Toc58097148)

[1.5 - Contracts Containing CUI 4](#_Toc58097149)

[2.0 - System Environment & Boundaries 4](#_Toc58097150)

[2.1 - General Description / Purpose of System 4](#_Toc58097151)

[2.2 - Operating / Hosting Model 4](#_Toc58097152)

[2.3 - System Environment Overview 5](#_Toc58097153)

[2.4 - System Components (Hardware / Software) 5](#_Toc58097154)

[2.5 - System / Network Boundaries 5](#_Toc58097155)

[2.6 - High-Level System Architecture Diagram 5](#_Toc58097156)

[2.7 - System Life Cycle (SDLC) 5](#_Toc58097157)

[2.6 – Applicable Procedures 6](#_Toc58097158)

[3.0 - Security Requirements 6](#_Toc58097159)

[3.1 – Security Requirements 6](#_Toc58097160)

**SSP Information**

|  |  |
| --- | --- |
| **Prepared By / SSP Point-of-Contact** | |
| **Name:** |  |
| **Department / Title:** |  |
| **Email Address:** |  |
| **Phone #:** |  |

**Revision History**

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

1.0 - System Identification

1.1 - System Name

*Name of the information system, or environment described in this plan.*

|  |
| --- |
| **System Name / Title** |
|  |

1.2 - System Categorization

*List the impact level for each security objective, and include the rationale for categorization. The three levels (Low, Moderate, High) relate to the potential impact on organizations or individuals should there be a breach of security (i.e. a loss of confidentiality, integrity, or availability). Reference FIPS 199, NIST 800-600 for additional information on system categorization.*

|  |  |  |
| --- | --- | --- |
| **Security Objective** | **Impact Level** | **Rationale for Categorization** |
| **Confidentiality** |  |  |
| **Integrity** |  |  |
| **Availability** |  |  |

1.3 – Responsible Organization

*Owning and/or installation organization*

|  |  |
| --- | --- |
| **Responsible Organization** | |
| **Name:** |  |
| **Address:** |  |
| **Phone:** |  |
| **CAGE Code(s):** |  |
| **DUNS #:** |  |

1.4 – System Roles & Responsibilities

|  |  |
| --- | --- |
| **System Owner -** *Subject-matter-expert of the information system and data contained therein* | |
| **Name:** |  |
| **Department / Title:** |  |
| **Email Address:** |  |
| **Phone #:** |  |
| **System Security Officer -** *Owner of overall system security program, and is responsible for overseeing the development, implementation, and maintenance of controls.* | |
| **Name:** |  |
| **Department / Title:** |  |
| **Email Address:** |  |
| **Phone #:** |  |

1.5 - Contracts Containing CUI

*List all applicable contracts that contain CUI safeguarding requirements under DFARS 252.204-7012. CUI requirements are found in Sections I and J of government contracts (DODI 5230.24)*

|  |  |  |  |
| --- | --- | --- | --- |
| **Contract Title / Number** | **Award Date** | **Information Owner** | **Address & Phone** |
| *<Enter contract title and identification number>* | *<Enter contract award date>* | *<Enter the government point-of-contact / organization responsible for providing and/or receiving CUI>* | *<Enter address and phone number for Information Owner / Government organization>* |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

2.0 - System Environment & Boundaries

2.1 - General Description / Purpose of System

*Describe the function and business purpose(s) of the system. Include a description of the type of data being processed and the business processes / programs supported.*

2.2 - Operating / Hosting Model

|  |  |  |
| --- | --- | --- |
| **Operating Environment Where CUI Exists (check all that apply)** | | |
|  | Data Center | Company-owned and operated data center on-premise |
|  | Public Cloud | Cloud services and infrastructure supporting multiple organizations and customers |
|  | Private Cloud | Cloud services and infrastructure dedicated to a specific organization and internal users, vs. the general public |
|  | Hybrid Cloud | Combination of public and private cloud (explain) |
|  | Distributed Endpoints | Workstations and other mobile / portable computing devices |
|  | Other | Explain: |

|  |  |  |
| --- | --- | --- |
| **Overview of Where CUI is Stored, Transmitted, Processed (check all that apply)** | | |
|  | Internal Application / System | Internal applications (i.e. ERPs, financial systems, machine shop applications) |
|  | Distributed File Servers | File servers, SAN storage |
|  | End-User Devices | Desktops, workstations, and laptops |
|  | Mobile Computing Devices | Smartphones, tablets, and other portable computing devices |
|  | Infrastructure-as-a-Service (IaaS) | Cloud environments (i.e. AWS, Azure) |
|  | Platform-as-a-Service (PaaS) | Cloud based, major applications (i.e. Azure Cloud Services, Amazon Web Services)s |
|  | Software-as-a-Service (SaaS) | Cloud based, externally hosted applications |
|  | Other | Explain: |

2.3 - System Environment Overview

*Provide a detailed topology narrative and graphic that clearly depicts the system environment, including system boundaries, system interconnections, and key components. (Note: It is not necessary to depict every workstation, server, or network device, but include a general description of each operating system in use, a description of portable components (if applicable), the virtual and physical server landscape, as well as a description of the firewalls, routers, switches, printers, etc. in use.*

2.4 - System Components (Hardware / Software)

*Populate the tables below or attach a complete listing of all hardware and software components installed on the system, or reference to the organizational component inventory database (i.e. configuration management database). Indicate whether hardware and software is maintained and owned by the organization (i.e. COTS, purchased and customized, or developed in-house).*

**Hardware Components**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Device / System Name** | **Type** | **Manufacturer / Model** | **Serial Number (s)** | **Memory / Media (Size & Type)** |
| *<ERP System 1>*  *<ERP System 2>*  *<File Server 1>* | *<Hard Drive>* | *<HP SSD>* | *<############>*  *<############>*  *<############>* | *<5 TB>* |
| *<ERP system>* | *<Printer>* | *<HP Laserjet Pro>* | *<############>* | *<None>* |
|  |  |  |  |  |

* *List the size/capacity of any memory or media that retains CUI when all power is removed.*
* *If the device has all volatile memory, specify “Power Off” in this column. If more lengthy sanitization or write-protection methods are used, reference the artifact that includes the sanitization or write-protection procedures.*

**Software Components**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Software Name** | **Manufacturer** | **Version** | **Purpose** | **Type / Ownership** |
| *<Windows 10>* | *<Microsoft>* | *<1909>* | *<Operating System>* | *<COTS>* |
|  |  |  |  |  |

*Note: The software list must include all security relevant software.*

2.5 - System / Network Boundaries

*Describe the network topography and system boundaries or attach a high-level network diagram. The description or diagram should portray the system boundaries and all applicable connections and major components (i.e. firewalls, routers, switches), including the mechanisms for monitoring and controlling communications at the external boundary and at key internal boundaries within the system environment.*

2.6 - High-Level System Architecture Diagram

*Attach a system architectural diagram. Describe major inbound and outbound data flows and connecting systems or attach a diagram.*

2.7 - System Life Cycle (SDLC)

Describe the operational phase of the information system.

|  |  |  |
| --- | --- | --- |
| **Operational Phase** | | |
|  | Operational / Production | System is in a production environment |
|  | Development / Testing | System is in a development or testing phase (non-production) |
|  | Major Modification | System environment is undergoing a major change, modification, or transition |
|  | Other | Explain: |

2.6 – Applicable Procedures

*Identify procedures used to govern the system:*

* *Account Management Procedures*
* *Endpoint configuration procedures*
* *Incident Detection & Response Plan*
* *Information Marking / Data Classification Procedures*
* *Maintenance procedures*
* *Mobile Configuration Procedures*
* *Network Configuration Procedures*
* *Awareness Procedures*
* *Physical and Environmental Protection Procedures*
* *Risk Management Procedures*
* *Server Configuration Procedures*

3.0 - Security Requirements

3.1 – Security Requirements

*Provide a thorough description of how all the security requirements are being implemented or planned to be implemented. The description for each security requirement contains:*

1. *The security requirement number and description (from NIST 800-171)*
2. *A brief description of how the security requirement is being implemented or planned to be implemented.*
3. *Any scoping guidance that has been applied (i.e. compensating controls or mitigations in place due to implementation constrains in lieu of the stated requirement.*

*If the requirement is not applicable to the system, provide rationale.*

**Security Control Identifiers and Family Names**

*Source: NIST 800-171*

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Family** | **ID** | **Family** |
| **3.1** | Access Control (AC) | **3.8** | Media Protection (MP) |
| **3.2** | Awareness and Training (AT) | **3.9** | Personnel Security (PS) |
| **3.3** | Audit and Accountability (AU) | **3.10** | Physical Protection (PE) |
| **3.4** | Configuration Management (CM) | **3.11** | Risk Assessment (RA) |
| **3.5** | Identification and Authentication (IA) | **3.12** | Security Assessment (SA) |
| **3.6** | Incident Response (IR) | **3.13** | System and Communications Protection (SC) |
| **3.7** | Maintenance (MA) | **3.14** | System and Information Integrity (SI) |