**LOGO**

**COMPANY NAME**

**System Security Plan (SSP)**

**CMMC Model 2.0 Level \_\_**

**Date:**

**Organization Name:**

**Organization Street Address:**

**TABLE OF CONTENTS**

**1. Executive summary**

**2. Information System**

* 1. Information System Name/Title
	2. System Function
	3. System Environments of Operation
	4. Network Architecture
	5. System Boundary
	6. System Interconnections

**3.Subjective CMMC Level**

**4. Organization Contacts**

1. Information System Owner
2. Other Designated Contacts

**5. Security Controls**

**Security Controls**

1. ACCESS CONTROL (AC)
2. AWARENESS AND TRAINING (AT)
3. AUDIT AND ACCOUNTABILITY (AU)
4. CONFIGURATION MANAGEMENT (CM)
5. IDENTIFICATION AND AUTHENTICATION (IA)
6. INCIDENT RESPONSE (IR)
7. MAINTENANCE (MA)
8. MEDIA PROTECTION (MP)
9. PERSONNEL SECURITY (PS)
10. PHYSICAL PROTECTION (PE)
11. RISK ASSESSMENT (RA)
12. SECURITY ASSESSMENT (CA)
13. SYSTEM AND COMMUNICATIONS PROTECTION (SC)
14. SYSTEM AND INFORMATION INTEGRITY (SI)

**Appendix:**

Appendix 1 POA&M

Appendix 2 Company Policies

**List of Figures**

Figure 1. Network Diagram page \_\_

Figure 2. System Boundary Diagram page \_\_

**List of Tables**

Table 1. Information System Name and Title page \_\_

Table 2. Environment Name page \_\_

Table 3. System Interconnections page \_\_

 A, B, C, D

Table 4. Subjective CMMC Level page \_\_

Table 5. Information System Owner page \_\_

Table 6. Contact Title page \_\_

Table 7. Leveraged External Organizations and Systems page \_\_

**Executive Summary**

[Company Name] has crafted this System Security Plan (SSP) with the primary objective of establishing robust administrative, technical, electronic, and physical security measures to protect the personal information of our customers and employees, safeguard our proprietary and confidential data, enhance the physical security of our facilities, and ensure the integrity of our electronic systems to facilitate their uninterrupted operation.

Furthermore, this SSP ensures that all company processes uphold adequate security standards to protect covered Department of Defense (DoD) controlled unclassified information (CUI) while it is either within our internal information system or in transit through our network. In addition, it outlines our commitment to promptly report any cyber incidents affecting our system or network to the DoD.

To achieve these security goals, [Company Name] has aligned its security practices with the guidelines established in the following regulatory documents:

* Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting.”
* DFARS provision 252.204-7008, "Compliance with Safeguarding Covered Defense Information Controls.”
* NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations."
* NIST Special Publication 800-172, "Enhanced Security Requirements for Protecting Controlled Unclassified Information.”
* NIST SP 800-171, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations."

[Company Name] is committed to diligently implementing these security measures and adhering to the highest standards of information security to protect sensitive data and fulfill our obligations to the DoD.

**Information System**

This System Security Plan offers an overview of security practices and processes governing the *(Information System Name - Example: Microsoft Office 365 tenant that is in a GCC / GCC High enclave environment*). It outlines the current security controls and those planned for implementation to maintain the requisite level of security for handling Controlled Unclassified Information (CUI) within the system. The security measures in place align with the policy and control requirements delineated in this System Security Plan.

**Information System Name/Title**

*Table 1. Information System Name and Title*

| **<Information System Name>** | **<Information System Abbreviation>** |
| --- | --- |

**System Function**

The function and purpose of the <Information System Abbreviation> system is as follows:

<Describe the purpose of the system>

**System Environments of Operation**

The following environments are used to develop, test or operate the <Information System Abbreviation> system.

*Table 2. Environment*

| *Environment Name* |  |
| --- | --- |
| *Environment Type* |  |
| *Operational Description* |  |

* 1. **Network Architecture**

The following Network Diagram provides a visual depiction of the system network components that constitute the <Information System Abbreviation> system.

|  |
| --- |

*Figure 1. Network Diagram*

* 1. **System Boundary**

The following System Boundary Diagram provides a visual depiction of the System Boundary. The boundary separating in-scope components from out-of-scope components is depicted by a prominent border.

|  |
| --- |

*Figure 2. System Boundary Diagram*

* 1. **System Interconnections**

| **Interconnection** | **Description:** |
| --- | --- |
| SIEM | For user workstations  |
| SOC |  |
| Firewall |  |
| Anti Malware | For anti-malware and anti-exploit protection. |
| Multi Factor Authentication (MFA) |  |
| Network Mapping |  |
| Mobile Device Management  |  |
| Ticketing System |  |

*Table 3A - Primary System Interconnections*

| **Interconnection** | **Identity and Access Management:** |
| --- | --- |
| Azure Multi-Factor Authentication (MFA) | For Office 365 user workstations. |
| Azure Web App Single Sign-On (SSO) | Integration with external cloud services. |
| Microsoft Intune | For workstations and mobile devices |
| Office 365 | Advanced Data Protection |
|  |  |
|  |  |

*Table 3B - System Interconnections - Access Management*

| **Interconnection** | **Data Security and Compliance:** |
| --- | --- |
| Email and Document Classification Labeling  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

*Table 3C - System Interconnections - Data Security and Compliance*

| **Interconnection** | **Endpoint and Device Management:** |
| --- | --- |
| Windows 10  | For user workstations  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

*Table 3D - System Interconnections - Endpoint and Device Management:*

 **2. Subjective CMMC Level**

<Organization Name> has reviewed the security practices in place for the <Information System Abbreviation> information system and believes this system meets or exceeds the requirements of the following CMMC Level.

*Table 4. Subjective CMMC Level*

| CMMC Level |
| --- |
| # |

**Organization Contacts**

* 1. **Information System Owner**

The following individual is identified as the system owner or functional proponent/advocate for this system.

*Table 5. Information System Owner*

| *Name* | <Enter Name> |
| --- | --- |
| *Title* | <Enter Title> |
| *Company / Organization* | <Enter Company/Organization>. |
| *Address* | <Enter Address, City, State and Zip> |
| *Phone Number* | <555-555-5555> |
| *Email Address* | <Enter email address> |

* 1. **Other Designated Contacts**

The following individual(s) possess in-depth knowledge of this system and/or its functions and operation.

*Table 6. Contact Title*

| *Name* | <Enter Name> |
| --- | --- |
| *Title* | <Enter Title> |
| *Company / Organization* | <Enter Company/Organization>. |
| *Address* | <Enter Address, City, State and Zip> |
| *Email Address* | <Enter email address> |

1. **Leveraged Practices and Processes**

<Organization Name> may leverage the practices and processes of external organizations or service providers to operate the <Information System Abbreviation> system. External organizations or service providers, if leveraged by <Organization Name>, are identified in the table that follows and referenced throughout this System Security Plan.

*Table 7. Leveraged External Organizations and Systems*

| *Leveraged Organizational System* | *Contact Information* |
| --- | --- |
| *Leveraged Organization/System* | *Leveraged Organization Contact Details* |

 **5. Security Controls**

Below are the 110 security controls required to meet CMMC Model 2.0, Level \_\_. The control numbering below is consistent with NIST SP 800-171, Revision 2.

##

## **Control 3.1.1**

Control Title:

Implementation Status:

☒ Implemented

**Purpose**: The company utilizes Azure Active Directory services and Microsoft Intune to control access and manage the security of users, devices, and processes within the GCC High environment. This document outlines the controls implemented and the ongoing maintenance practices in place.

#### 1. Access Control:

* **Role-Based Access Control (RBAC):** Access to the system is limited to authorized users and processes, managed via role-based access permissions in Azure.
* **Authentication Methods:** This includes the use of user IDs and passwords, along with multi-factor authentication.
* **Conditional Access:** Access for devices is limited based on conditional access rules implemented in Microsoft Intune.

#### 2. Device Management:

* **Device Enrollment:** Intune enforces restrictions that require devices to be managed or enrolled in Intune before they are allowed to access the GCC High environment.

#### 3. Review and Monitoring:

* **Weekly User Base Review:** The company performs a weekly review of the Azure user base, ensuring that no unauthorized users, processes, accounts, or devices have been added.
* **Setup Review and Maintenance:** Regular review and maintenance of user services and devices within the Azure Active Directory services and Intune environments are conducted.

#### 4. Third-Party Management:

* **Managed IT Service Provider:** The company leverages the expertise of a third-party managed IT service provider to assist in the implementation and maintenance of the above controls.

#### 5. Compliance:

**NIST 800-171:** This plan aligns with the requirements of NIST 800-171, as applicable to the organization’s handling of Controlled Unclassified Information (CUI).

**Defined authorized users:** The personnel with a legitimate business need to access the information system have been determined, and a list of authorized users who have been granted access has been created.

**Established user accounts:** User accounts to access the information system resources, such as computers, servers, and cloud resources, have been ensured to be available only to authorized personnel. Any unnecessary or generic accounts have been removed.

**Associated processes with authorized users:** All automated script updates and other processes have been associated with the specific user who initiated them. The use of generic account names for running scripts, especially for critical processes like backup scripts, has been avoided.

**Controlled device access:** Measures have been implemented to limit which devices can access the information system. Devices are now authenticated and authorized before being granted access to our network.

**Secured VPN access:** Our virtual private network (VPN) has been configured to allow only authorized devices to connect. Authentication mechanisms have been implemented to verify the legitimacy of devices attempting to establish a VPN connection.

**Regularly reviewed and updated access controls:** Access controls have been periodically reviewed and updated to align with changes in personnel, business needs, and technology. Access rights for individuals who no longer require them have been promptly removed.

**Monitored and audited access:** Monitoring and auditing mechanisms have been implemented to track access to the information system. Logs and reports are regularly reviewed to detect any unauthorized access attempts or unusual activity.

**Provided user training and awareness:** Authorized users have been educated about the importance of limiting access and following security protocols. Regular training sessions have been conducted to ensure users are aware of best practices for information system access and the potential risks associated with unauthorized access

## **Control 3.1.2**

Implementation Status:

☒ Implemented

**Purpose**: This System Security Plan (SSP) describes the security protocols and measures utilized by [Company Name] for the protection of its IT resources, including the use of Microsoft Azure Active Directory, Role-Based Access Control (RBAC), and related technologies.

#### 2. Access Control

* **Role-Based Access Control (RBAC):** RBAC is implemented to enforce the types of transactions and functions that authorized users are permitted to execute.
* **Azure Active Directory:** Utilized to manage and secure identities, enabling authorized users to access the required resources.
* **Multi-Factor Authentication (MFA):** Implemented to protect authorized users, using Azure multi-factor authentication.

#### 3. Conditional Access Policies

* **Intune Integration:** Conditional access policies are enabled using Intune to set conditions on what users can access and the devices that can be used to access them.

#### 4. Account Provisioning and Management

* **Provisioning Procedures:** The company adheres to documented procedures for account provisioning and deprovisioning.
* **Access to CMC Environment:** The creation of accounts for accessing the CMC environment is done as per documented procedures.

#### 5. Monitoring and Auditing

* Regular monitoring and auditing of all resources to ensure that the right users have the right access to the right resources.

#### 6. Additional Security Measures

* **Azure Environment Protection:** The Azure environment is protected by Azure multi-factor authentication.
* **Standard Operating Procedures (SOPs):** Depending on the size and structure of the company, SOPs, recurring IT ticketing systems, or direct control may be in place.
* **Policy and Document Writing:** In cases where further documentation is needed, policies are written to guide the controls and assessment procedures.

##

## **Control 3.1.3**

##

Control the flow of Controlled Unclassified Information (CUI) in accordance with approved authorizations.

**Purpose**: The primary goal of this control is to guarantee that the flow of CUI within our organization is systematic, structured, and, above all, secure. To maintain the security and integrity of the CUI we handle, we have taken the necessary measures aligned with the Department of Defense’s compliance standards.

**Implementation**:

1. **CUI Identification and Classification**:
	* We have determined and classified the types of CUI our company handles based on NIST Special Publication 800-171 and other relevant guidelines.
	* Appropriate labels or markings are applied to clearly define the sensitivity and handling requirements for each type of CUI.
2. **Access Authorizations**:
	* We have established and documented the approved authorizations for accessing and handling different CUI categories.
	* This encompasses specific user roles, job responsibilities, or clearance levels.
3. **Access Control Mechanisms**:
	* Measures include the utilization of role-based access control (RBAC), user authentication mechanisms, and encryption.
	* Microsoft Intune is our chosen platform to manage access to our CMMC environment, ensuring devices connecting are compliant with Intune’s policies.
	* Further, our CMMC workstations deter unauthorized copying from the SharePoint environment via security policies on the Edge browser.
4. **Flow of CUI**:
	* Our organization’s policy details CUI’s flow, considering the source, destination, involved parties, and devices that will store or transmit CUI.
	* Copy restrictions are in place on public systems, preventing copy-paste or save functions on the Edge browser.
5. **Protection Measures**:
	* CUI, both in transit and at rest, is protected using strong encryption measures and secure key management practices.
	* Mechanisms are in place to monitor and audit the flow of CUI across our systems and networks, with routine reviews of logs to ensure compliance.
6. **Periodic Reviews**:
	* We regularly reassess approved authorizations to ensure alignment with regulatory demands and contractual obligations.
7. **Training and Awareness**:
	* Our employees undergo training on CUI handling, ensuring they’re well-informed on authorizations, access control measures, and flow procedures.

## **Control 3.1.4**

**1. Control Title**: Separation of Duties using Role-Based Authentication and Control (RBAC)

**2. Purpose**: To ensure that system and data access rights are distributed among personnel in a way that reduces risk and prevents a single individual from executing security-sensitive operations without oversight.

**3. Implementation**:

3.1. **General Approach**: The company has recognized the significance of separating duties to minimize risks associated with fraudulent or unauthorized activities. To achieve this, the company has implemented role-based authentication and control (RBAC).

3.2. **Technological Implementation**:

* **Azure Active Directory (AAD)**: The company uses Azure Active Directory to establish and enforce RBAC assignments. Azure AD’s inherent capabilities allow for fine-grained control, ensuring that users only have the specific access rights necessary for their roles.
* **Group Policy (On-Premise)**: For on-premise systems, Group Policy is employed as an additional means to enforce separation of duties, especially for security-sensitive tasks.

3.3. **Role Review and Maintenance**:

* **Monthly Review**: Every month, the company reviews roles and permissions, leveraging both the company personnel and technology list. This review ensures that access rights remain aligned with each employee’s specific job functions and that no individual has excessive permissions.

3.4. **Separation of Duties Principle**:

* **Risk-Level and Activity Collision**: At its core, the control aims to reduce the risk of a single individual performing security-sensitive activities without oversight. The system is structured to require collaboration (from multiple individuals) for tasks that are deemed highly sensitive.

**4. Roles and Responsibilities**:

4.1. **IT Department**: Ensures the proper configuration of Azure AD and Group Policy, and periodically confirms their effectiveness.

4.2. **Human Resources**: Provides the IT Department with up-to-date personnel lists, job functions, and role changes to ensure accurate role assignments.

4.3. **Management**: Reviews and approves any changes to RBAC settings, ensuring alignment with organizational needs and security best practices.

**5. Periodic Review and Updates**:

The company commits to regularly reviewing and updating this control, at least annually, to adapt to changing organizational needs, technological advances, and emerging threats.

**6. Conclusion**:

By implementing the separation of duties through role-based authentication and control, the company ensures that potential risks associated with unauthorized or malicious activities are significantly reduced. It emphasizes the importance of collaborative oversight, particularly for security-sensitive operations.

**7. Approvals**:

* **CISO**: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_
* **Head of IT**: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_
* **Head of HR**: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_

## **Control 3.1.5**

**Title:** Employing the Principle of Least Privilege

**Purpose:** The intent of this control is to ensure that users and processes within the organization are granted only the permissions and privileges required to perform their specific roles or tasks. This minimizes the potential damage from errors or the misuse of privileges.

**Control Description:**

1. **Definition of Privileged Functions**: The company clearly defines what constitutes privileged functions and documents them in the company’s personnel and technology list.
2. **Assignment of Privileges**: All users, including administrators with privileged access, are granted rights exclusively based on what is necessary for their respective roles. This ensures that they only have the rights required to perform functions aligned with their position.
3. **Implementation & Enforcement**: The company leverages Azure Active Directory and RBAC (Role-Based Access Control) to implement and enforce the principle of least privilege. This ensures that the roles defined come with the minimum set of privileges needed for the job function.
4. **System-Specific Access**: For isolated systems access is restricted solely to individuals whose roles directly involve the use of such systems.
5. **Periodic Review of Privileges**: The company carries out regular assessments to re-evaluate the privileges designated to users, processes, and system accounts. This is to confirm continuous compliance with the principle of least privilege.
6. **Monitoring & Compliance**: Using tools like group policy, active directory, file share permissions, and specific system controls, the company monitors user activities and permissions, ensuring no over-privileged access exists.

**Guidelines & Procedures:**

* **Identification of Privileged Accounts**: Super user accounts, often linked with system administrator roles, are identified and tagged as ‘privileged’.
* **Access Limitation**: Regular users are barred from accessing privileged information or functionalities, reserving this access exclusively for authorized personnel.
* **Lifecycle Application**: The principle of least privilege is enforced throughout the lifecycle of organizational systems. This includes during phases like development, implementation, and regular operation.
* **Continuous Monitoring**: Systems have been implemented to constantly monitor and affirm the application of the least privilege principle, ensuring that access rights remain synchronized with business necessities and imposed restrictions.

## **Control 3.1.6**

 **Tittle:** 3.1.6 Use Non-privileged Accounts

**Purpose:** To ensure that privileged account access is restricted to specific security tasks, facilitating the detection of anomalies or unauthorized access in system logs.

**Assessment Points:**

1. **Identify Non-security Functions:**Verify if non-security functions are meticulously listed and defined, often identifiable through Group Policies and individual system access restrictions. For example, role restrictions might inhibit individuals from executing certain actions or accessing specific records in an application.
2. **Use of Non-privileged Accounts:**Ensure users are obligated to adopt non-privileged accounts or roles when performing non-security tasks. This is verifiable by attempting privileged actions with a standard account and checking for access denials.

**Implementation Details:**

* All privileged account holders are equipped with non-privileged accounts, exclusively used for tasks not demanding elevated permissions.
* Compliance monitoring and anomaly detection of these account usages are executed via our SIEM system.
* All functions or tasks unrelated to security within the organization have been meticulously listed.
* Elevated access privilege roles within systems have been explicitly identified.
* Individuals are allocated non-privileged accounts or roles based on access necessities.
* The organization has distinctly determined non-privileged accounts for accessing non-security functions.
* Access control strategies like role-based access control (RBAC) are established to manage user access to diverse functions and resources.
* Users are trained and educated on the necessity of non-privileged account usage for non-security tasks and informed of the risks of unnecessary elevated access.
* Continuous monitoring of access logs and activities ensures the detection of any unauthorized or inappropriate use of privileged roles.
* Comprehensive documentation related to access policies, role delineations, and relevant updates is consistently maintained.

##

## **Control 3.1.7**

**Prevention of Non-Privileged User Execution of Privileged Functions**

**Purpose:**To prevent non-privileged users from executing privileged functions and ensure the audit of such functions, thereby upholding system integrity and security.

**Assessment Points:**

**Determination of Privileged Functions:**

* **Query:** Are privileged functions distinctly defined within the system?
	+ **Sample Response:** Privileged functions are specifically delineated within each individual system our authorized users have access to. Examples encompass file system permissions, such as granting access to privileged folders containing Controlled Unclassified Information (CUI), security groups, Organizational Units (OU’s), and user permission levels within diverse systems.

**Identification of Non-Privileged Users:**

* **Query:** How are non-privileged users identified and categorized within the system?
	+ **Sample Response:** Non-privileged users are defined based on their role memberships, and by their classification as administrators or standard users, and by their account type.

**Prevention Measures for Non-Privileged Users:**

* **Query:** What mechanisms are in place to prevent non-privileged users from executing privileged functions?
	+ **Sample Response:** Non-privileged users are barred from executing privileged tasks through mechanisms like Group Policy, file system permissions, and user access rights within each distinct system. This extends beyond the foundational OS in our domain, taking into account systems such as accounting or secure engineering platforms.

**Auditing of Privileged Functions Execution:**

* **Query:** How are the executions of privileged functions audited and monitored?
	+ **Sample Response:** Execution activities are logged and tracked in our Security Information and Event Management (SIEM) system. This SIEM system aggregates and analyzes log data from various sources to identify any unauthorized or suspicious activities related to privileged functions.

**SIEM System Effectiveness:**

* **Query:** How effective is the SIEM system in detecting and alerting on unauthorized or suspicious activities related to privileged functions?
	+ **Sample Response:** Our SIEM system is configured with advanced analytics and correlation rules, ensuring a high detection rate of anomalies. Regular reviews and updates of the SIEM configurations are conducted to ensure it remains effective against evolving threat patterns.

**Implementation Strategy:**

* SIEM system to comprehensively capture, log, and monitor the execution of privileged functions.
* Users are granted the minimum privileges required to perform their assigned tasks effectively, avoiding excessive or unnecessary privileges.
* The company conducts regular reviews of user privileges to ensure alignment with their roles and responsibilities. Any unnecessary or outdated privileges are promptly removed.
* Comprehensive auditing and logging mechanisms are enabled in the systems, capturing the execution of privileged functions in audit logs.
* The company regularly monitors and analyzes audit logs to detect any unauthorized or suspicious activities related to privileged functions. Procedures are established for reviewing logs and responding to anomalies.
* Incident response procedures have been developed to promptly investigate potential security incidents or unauthorized access attempts related to privileged functions.
* Appropriate actions are taken to mitigate risks and prevent future occurrences based on the findings of incident investigations.

## **Control 3.1.10**

## **Tittle: Session Locking and User Session Termination**

**Purpose:** To ensure that user sessions are securely managed, preventing unauthorized access during temporary absences or after certain conditions that warrant session termination.

**Assessment Points:**

**Session Lock Properties:**Check the properties of session locks, including their triggering conditions, such as periods of inactivity or user-induced locks. Confirm that the displayed patterns or images during the locked phase don’t display sensitive information.

**Difference Between Session Lock and Logout:**Ensure that users understand the distinction between a session lock and a full logout. Emphasize the importance of logging out at the end of the workday or during extended absences.

**User Session Termination Properties:**Inspect the conditions leading to automatic session termination. These can include user inactivity, certain incident responses, or system usage time restrictions.

**Implementation Details:**

* Sessions are programmed to lock automatically after 15 minutes of user inactivity. A password input is needed for users to regain access.
* For display during session lock, a variety of non-sensitive images or patterns are used.
* Employees receive guidance to lock their screens manually when departing from their workspace temporarily.
* An additional security measure requires users to reauthenticate following an hour of inactivity, upheld by a specific conditional access policy.
* All local computer user sessions are set to lock after 15 minutes of inactivity.
* Session limits within the Office 365 environment are based on [this article](https://docs.microsoft.com/en-us/microsoft-365/enterprise/session-timeouts?view=o365-worldwide).
* After a session termination, users must sign back in to initiate a new session within the network.
* A Conditional Access Policy is also employed to regulate sign-in frequencies.
* Users are educated on the distinction between session locks and logouts, with continuous monitoring of session activities for any discrepancies or unauthorized access attempts.
* Proper documentation detailing session management policies, user guidelines, and any related updates is regularly maintained and reviewed.

## **Control 3.1.11**

##

##

**Control Title:** Session Termination

**Purpose:** This document outlines the existing measures implemented to automatically terminate user-initiated logical sessions after specific conditions. These measures are crucial to protect the organization’s data and to minimize potential unauthorized access risks.

**Control Requirement (NIST 800-171):**Terminate (automatically) user sessions after defined conditions.

**Current Implementation:**

1. **Local Computer Inactivity Lock:**User sessions on local systems have been configured to auto-lock after 15 minutes of inactivity.
2. **Office 365 Session Configuration:**The Office 365 environment strictly adheres to the recommended session timeout configurations, as specified in the Microsoft’s session timeout guidelines: [Session Timeouts in Microsoft 365](https://docs.microsoft.com/en-us/microsoft-365/enterprise/session-timeouts?view=o365-worldwide).
3. **Session Termination Mechanism:**Once users log off their systems or if there’s a system shutdown, the user session is terminated. Subsequent access requires users to re-authenticate and re-establish their session.
4. **Conditional Access Policy:**An active Conditional Access Policy has been applied to manage and regulate sign-in frequencies.
5. **VPN Session Timeout:**The current VPN policy is set to terminate user sessions after 180 minutes of idle time.
6. **Idle Time Termination:**The primary condition determining session termination is the user’s idle time. Local systems are set to measure idle time up to 15 minutes before initiating a session lock and the subsequent termination of user access.

**Compliance and Monitoring:**

1. **User Awareness:**All users have been trained and are fully aware of the session termination policy.
2. **Continuous Monitoring:**Active monitoring mechanisms are in place to ensure that session timeout configurations remain consistent and intact across all platforms.
3. **Regular Policy Review:**The session timeout configurations and associated policies undergo regular reviews to ensure they align with the organization’s evolving security goals and the current cybersecurity environment.

**Responsible Parties:**The IT department and the Network Security team oversee and ensure the strict implementation of this control.

## **Control 3.1.12**

##

## **Title:**

###

1. Purpose: This System Security Plan describes how the organization manages, monitors, and restricts access to Controlled Unclassified Information (CUI). It includes the implementation of a Security Information and Event Management (SEIM) solution, firewalls, Multi-Factor Authentication (MFA), and training procedures.

### 2. Security Measures

#### 2.1 SEIM and Firewall

The SEIM solution, in conjunction with firewall technology, monitors and logs VPN usage. MFA secures the connections, ensuring unauthorized users are restricted.

#### 2.2 Remote Access Control

Remote access is limited to authorized users who need it to complete assigned job duties. Remote support sessions require MFA, and workstations remain locked without proper device-specific credentials and MFA.

#### 2.3 Workstation Security

Access to workstations requires MFA. When not in use, workstations lock with a screensaver, requiring authentication to regain access. Any remote access directly leads to a lock screen.

#### 2.4 Device Management

Devices authorized to store, process, and transmit CUI are always monitored and controlled by trained and authorized users. These measures ensure that access to CUI is only granted to those who have completed the required training and have signed the necessary policies.

### 3. Training and Awareness

All users with access to CUI must undergo training and adhere to signed policies. This ensures that only knowledgeable and compliant personnel have access to sensitive information.

### 4. Compliance

Alignment with relevant standards and the organization’s specific guidelines.

### 5. Review and Updates

Ongoing monitoring, audits, and necessary revisions to ensure compliance and effectiveness.

### 6. Responsibilities

The IT Department, in collaboration with other relevant departments, is responsible for implementing and maintaining these security measures.

### 7. Approval

This SSP is approved by: [Name, Title]

Signature:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## **Control 3.1.13**

##

## System Security Plan (SSP) for [Company Name]

**Date:** [Insert Date]

### 1. Introduction

This SSP outlines the cryptographic mechanisms employed by [Company Name] to secure remote access sessions, focusing on ensuring the confidentiality and integrity of Controlled Unclassified Information (CUI). The plan encompasses the use of modern encryption methods that comply with federal standards.

### 2. Cryptographic Mechanisms

#### 2.1 Wi-Fi Networks

* **WPA2 and WPA3:** Both of these Wi-Fi Protected Access methods utilize FIPS 140-2 encrypted methods, ensuring the security of wireless connections within the organization.

#### 2.2 Remote Access Sessions

* **VPN Connections:** All remote access sessions, including VPNs, are encrypted using FIPS 140-2. There is no non-encrypted method to connect to the network remotely, providing a secure connection environment.

### 3. Cloud Compliance and CUI Storage

#### 3.1 Microsoft GCC High Compliance

* If Microsoft GCC High is utilized for cloud services, compliance with FIPS 140-2 validated encryption is assured.

### 4. Responsibilities

* IT Department: Responsible for implementing and maintaining cryptographic measures.
* Employees: Adhere to the defined policies and use only approved encrypted connections.

### 5. Review and Updates

Ongoing monitoring, audits, and necessary revisions will be conducted to ensure compliance with relevant standards and effectiveness in safeguarding remote access sessions.

### 6. Approval

This SSP is approved by: [Name, Title]

Signature:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## **Control 3.1.14**

## **System Security Plan (SSP) for [Company Name]**

#### **1. Introduction**

This System Security Plan outlines the organization’s approach to securing controlled unclassified information (CUI) by implementing managed access control points, firewalls, authentication methods, monitoring systems, and training programs.

#### **2. Managed Access Control Points**

* **2.1 Designation:** Specific gateways were identified and established for remote access connections, serving as control points for all traffic.
* **2.2 Security Measures:** Strong measures such as firewalls, intrusion detection/prevention systems, and encryption mechanisms are implemented at these control points.
* **2.3 Authentication:** Robust methods, including multi-factor authentication, are employed to verify remote users’ identities.
* **2.4 Monitoring and Logging:** Systems track and log activities routed through the control points, with regular reviews to detect anomalies and investigate suspicious activities.
* **2.5 Training and Awareness:** Remote users are educated about organizational policies and guidelines, emphasizing the proper use of managed access control points.

#### **3. Additional Security Measures**

* **3.1 Role-Based Access Control:** Permissions and role-based access routing are used to manage different areas of the system.
* **3.2 Cloud-Based Strategy:** Integration with cloud solutions like Office 365 GCC High, ensuring secure routing.

#### **4. Compliance**

Alignment with relevant standards, including FIPS 140-2.

#### **5. Responsibilities**

Both the IT Department and Employees share responsibilities in implementing, maintaining, and adhering to these security measures.

#### **6. Review and Updates**

Ongoing monitoring, audits, and necessary revisions to ensure compliance and effectiveness.

#### **7. Approval**

This SSP is approved by:

**[Name, Title]** Signature:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## **Control 3.1.16**

### **System Security Plan (SSP) for ABC Company**

#### **I. Introduction**

This System Security Plan outlines the policies, procedures, and technical controls implemented at ABC Company to ensure secure wireless networking. The plan aligns with recognized standards such as FIPS 140-2, ensuring that the wireless infrastructure of the organization complies with regulatory requirements and security best practices.

#### **II. Wireless Network Security**

1. **Encryption Standards**:
	* **WPA2/WPA3 Implementation**: All wireless networks within ABC Company are secured using WPA2 or WPA3 encryption protocols. This ensures secure transmission of data and prevents unauthorized access.
	* **FIPS 140-2 Compliance**: The encryption methods utilized meet the Federal Information Processing Standards (FIPS) 140-2, ensuring robust cryptographic security.
2. **Access Control**:
	* **Password Requirement**: Strong passwords are enforced within the secure network. Password management policies detail the complexity and rotation requirements.
	* **No Open Wireless Networks**: ABC Company does not operate any open or unprotected wireless networks, ensuring that all connections require proper authentication and authorization.
	* **Unauthorized Access Prevention**: Measures are implemented to detect and prevent unauthorized devices from connecting to the network.
3. **Monitoring and Audit**:
	* Continuous monitoring and periodic auditing ensure that security controls are functioning correctly and that any suspicious activities are promptly detected and addressed.

## **Control 3.1.17**

##

## **System Security Plan (SSP) for wireless access:1. Introduction:** This System Security Plan (SSP) outlines the security measures implemented to protect the wireless network in our organization. The plan adheres to the government-mandated FIPS 140-2 standard and focuses on protecting Controlled Unclassified Information (CUI) through robust encryption and access controls.**2. System Description:**

* + **Name of System:** Secure Wireless Network
	+ **System Functionality:** Provides wireless connectivity to authorized users and devices within the organization.
	+ **Location:** All company facilities
1. **3. Security Measures:**
	* **Authentication and Encryption:**
		+ Utilizes WPA2 encryption to ensure that all wireless traffic is fully encrypted.
		+ Matches the government-mandated FIPS 140-2 for protecting CUI.
		+ Implements authentication to permit access only to authorized users and devices.
	* **Access Controls:**
		+ Only authorized users and company-owned devices are granted access to the wireless network.
		+ Policies are in place to control and monitor access, including regular updates to passwords and access lists.
2. **4. Management Controls:**
	* **Regular Monitoring and Audits:**
		+ Continuous monitoring of the wireless network for unauthorized access or suspicious activities.
		+ Periodic security audits to ensure compliance with the SSP.
	* **Incident Response Plan:**
		+ Procedures for responding to security incidents are well-defined and adhered to.
		+ Reporting mechanisms are in place to ensure timely notification and action if a breach occurs.
	* **Policy Enforcement:**
		+ Users are educated about the policies governing wireless access.
		+ Non-compliance with policies is dealt with promptly through predefined disciplinary actions.

## **Control 3.1.18**

##

## System Security Plan (SSP) for [Organization Name]

#### 1. Introduction

This System Security Plan outlines the organization’s approach to securing its network and the measures taken to protect Controlled Unclassified Information (CUI) within the Cybersecurity Maturity Model Certification NIST 800-171 framework.

#### 2. Wireless Network Access Controls

2.1 **Authorization**: Only authorized users with the wireless password can access the organization’s wireless network. Permissions are granted directly by the IT department.

2.2 **Device Ownership**: All authorized mobile devices must be company-owned. Personal devices are not permitted to access the network.

2.3 **Remote Management**: Authorized mobile devices utilize remote wipe and remote management capability, allowing the IT department to control all aspects of the connection.

2.4 **Conditional Access**: Microsoft Intune is utilized to control the connection of Windows laptops to the secured environment, determining whether a connection should be allowed or denied based on specific criteria.

2.5 **Mobile Device Restrictions**: Mobile phones and other mobile devices are explicitly not authorized to connect to any other environment that holds CUI.

#### 3. Compliance

This SSP is in alignment with the guidelines and standards set forth in the Nist 800-171 framework for the protection of Controlled Unclassified Information.

#### 4. Responsibilities

Both the IT Department and employees have shared responsibilities in implementing, maintaining, and adhering to these security measures.

#### 5. Review and Updates

Ongoing monitoring, audits, and necessary revisions will be carried out to ensure compliance and effectiveness.

#### 6. Approval

This SSP is approved by: [Name, Title]

Signature: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## **Control 3.1.19**

##

## **System Security Plan (SSP)Organization:** [Organization Name]**System Name:** Mobile Device and Computer Encryption System**Date:** [Date]**1. Introduction**This System Security Plan details the encryption measures and policies put in place to ensure that all devices, particularly those within the mobile device organizational unit, are protected against unauthorized access and potential data breaches.**2. System Description**The system encompasses all connected devices, including but not limited to desktop computers, laptops, and mobile devices. It specifies encryption standards and practices for devices that are part of or have access to Controlled Unclassified Information (CUI).**3. Device Encryption Policy**3.1. **BitLocker in FIPS Mode:** All devices within the mobile device organizational unit are mandated to activate BitLocker in FIPS mode. 3.2. **Group Policy Management:** Encryption policies are managed through Group Policy and applied to members of specific organizational units in the Active Directory.3.3. **Device Access to CUI:** All devices that have access permissions to CUI must adhere to the BitLocker Group Policy, ensuring encryption across all devices, not limited to mobile ones.**4. Mobile Device Encryption and Verification**4.1. **IT Verification:** All company-owned mobile devices with clearance to access CUI are subjected to a verification process by the IT department.4.2. **Encryption Standards:** Devices must be encrypted either straight from the factory or using approved aftermarket solutions to gain CUI access clearance.**Signatures:IT Manager:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **Date:** \_\_\_\_\_\_\_**Security Officer:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **Date:** \_\_\_\_\_\_

## **Control 3.1.20**

##

##

**System Security Plan (SSP)
Organization:** [Organization Name]
**System Name:** External Systems Connection Control
**Date:** [Date]

**1. Introduction**This System Security Plan (SSP) delineates the measures taken by the organization to ensure that connections to and use of external systems are verified, controlled, or limited. This is crucial to ensure data integrity, confidentiality, and availability.

**2. Defined System**Every system, software, and hardware component that is owned and administratively controlled by [Company Name] is recognized as our defined system. Any external connection or component not owned or under the administrative purview of our organization is considered outside this defined system.

**3. Connection Management**In our effort to manage and control connections to these external systems, the following measures are detailed:

* **3.1. Firewall Management:**We employ robust firewalls to regulate data traffic that enters or exits the organization’s network. This ensures that only authorized data packets can traverse our network, acting as the first line of defense against potential security threats.
* **3.2. USB Port Restrictions:**To prevent potential threats from external devices, USB port blocking capabilities have been activated across our network. This restricts the connection of unauthorized devices, safeguarding against data breaches or malware intrusion.
* **3.3. Domain Protection:**We use DNS filtering to block access to malicious or unauthorized domains. This limits the potential exposure of our network to harmful content and ensures that users only access secure and approved websites.

**4. Company Policy on External Systems**To ensure clarity and adherence to our security standards:

* All employees are informed that the use of external systems not directly approved by the IT department is prohibited. This includes but is not limited to external drives, software, and unauthorized cloud services.
* Any employee found using an unauthorized external system may face disciplinary action.
* Should any employee require access to an external system for legitimate business purposes, they must first seek and obtain approval from the IT department.

**5. Verification Protocols**

* **5.1. SIEM (Security Information and Event Management):**The SIEM system collects and analyzes security alerts from various network hardware and software.
* **5.2. SOC (Security Operations Center) Solution:**This is the organization’s primary security monitoring unit, ensuring real-time surveillance and immediate response to any security threats or breaches.

**Signatures:
IT Manager:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **Date:** \_\_\_\_\_\_\_
**Security Officer:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **Date:** \_\_\_\_\_\_
**Security Architect:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **Date:** \_\_\_\_\_\_

Note: Remember to fill in the placeholders like [Organization Name] and [Date] with the appropriate details.

## **Control 3.1.21**

##

## System Security Plan (SSP) Section for Control 3.1.21:

**Control**: 3.1.21 – Limit the use of portable storage devices on external information systems.

**Implementation**:

The organization has established a policy that prohibits the use of portable storage media on external systems. This policy is outlined in both our IT use and cyber security documentation. The following measures detail our approach:

1. **Prohibition and Restrictions**:
	* The default stance of our organization is a complete prohibition on the use of organization-controlled portable storage devices on external systems.
	* Exceptions, if any, are limited and clearly outlined in our IT use and cyber security policy. These exceptions consider both the nature of the data being transferred and the security posture of the external system.
2. **Definition of External Systems**:
	* While “external” typically implies systems outside of our organization’s immediate authority and supervision, for the purpose of this control, the term is more expansive.
	* Within our organization’s infrastructure, there exist systems designated for processing Controlled Unclassified Information (CUI) and others that are not. Even among systems that do process CUI, there are delineated access restrictions. As such, any system that isn’t explicitly authorized to access a specific segment of CUI is treated as “external” to that data, regardless of whether it belongs to our organizational infrastructure.
3. **Oversight and Auditing**:
	* Our IT and cybersecurity teams routinely monitor the use of portable storage devices. Any violations of the aforementioned policy result in immediate action, up to and including revocation of system access and disciplinary measures.
	* Audits are conducted periodically to ensure compliance and to identify potential areas of improvement.

## **Control 3.1.22**

##

## **System Security Plan (SSP) for Control 3.1.22: Publicly Accessible Systems and CUI**

**1. Control Title**: Control of CUI Posted or Processed on Publicly Accessible Systems.

**2. Purpose**: This SSP ensures that Controlled Unclassified Information (CUI) is protected from inadvertent exposure and is not posted, processed, or stored on publicly accessible information systems.

**3. Policy & Implementation**:

**3.1. ITU Cyber Security Policy Directive**: Per company’s directive and the ITU Cyber Security Policy, we prohibit the posting or processing of CUI on any system accessible to the general public.

**3.2. Definition of Public Systems**: A publicly accessible system is any platform or medium accessible without restriction to the general public, whether digitally via the internet or physically at a particular location.

**3.3. Protective Measures**: To prevent inadvertent CUI disclosure:

* We have stringent measures for interfaces like public-facing websites or forms to ensure they neither collect nor display CUI.
* Regular audits ensure our public platforms and their supporting backend systems remain CUI-free.
* An established PR review committee evaluates any necessary public communications containing CUI, subjecting them to thorough checks and approvals.

**3.4. Training**: Employees receive comprehensive training on the importance and methods of safeguarding CUI, including the risks associated with public systems. Periodic reminders bolster this training.

**3.5. Incident Management**: In case CUI is unintentionally disclosed on a public platform:

* Procedures are activated for immediate data removal.
* Affected parties are notified.
* A post-incident review identifies and rectifies the cause to prevent recurrence.

**3.6. Exception Management**: All exceptions to this policy must undergo senior management approval and be documented. Before any such exception, the PR review committee ensures the implementation of adequate protection measures.

## **Control 3.2.1**

##

## **System Security Plan (SSP) for Control 03.02.01**

**1. Control Identifier:**Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems

**2. Objective:**Our company has implemented a training system to ensure that our personnel are consistently informed about the security risks associated with their roles, emphasizing the importance of understanding potential threats and vulnerabilities.

**3. Target Group:**

* Managers
* Systems Administrators
* Users of Organizational Systems (ranging from leadership to everyday users)

**4. Purpose:**We aim to solidify our security posture. By ensuring our staff knows what’s at stake and the correct protocols, we minimize potential threats stemming from unawareness or misinformed actions.

**5. Current Implementation:**

a) **Training Program:**Our employees, from entry-level to C-level executives, undergo Security Level I training annually. Our program covers:

* Cybersecurity awareness
* Insider threat nuances
* Counterintelligence dynamics
* Export compliance protocols
* Proper marking of classified information
* The intricacies of derivative classification

b) **Content Calibration:**We’ve tailored our training content and frequency to our specific organizational needs and the systems our personnel access. Core subjects cover:

* Grasping the significance of information security.
* User actions to uphold security standards.
* Proper reactions to suspected security breaches.
* Recognizing the necessity of operational security.

c) **Security Awareness Techniques:**To maintain and enhance our staff’s security consciousness, we employ:

* Scheduled training sessions.
* Stationery and supplies bearing security reminders.
* Regular email advisories and notices from senior officials.
* Security-centric logon screen messages.
* Strategically placed security reminders throughout our facilities.

**6. Measurement & Compliance:**Our evaluation teams carry out post-training checks to measure training effectiveness. Employee understanding and retention are assessed periodically. We also maintain a detailed record of all training interventions, participant details, and performance metrics for internal audits.

**7. Periodic Review:**Our teams review this control annually, updating based on new threat intelligence, technological shifts, and feedback loops from employees.

**8. Role-based Responsibilities:**

* Our IT department oversees technical components, including logon reminders.
* Human Resources helms the orchestration and documentation of training.
* All managers ensure their respective teams understand and follow our security norms.

## **Control 3.2.2**

##

## **Organizational System Security Plan (SSP) – Employee Security Training Protocols**

**Control 03.02.02**

**1. Introduction:**Safeguarding our organizational assets and data is not solely dependent on technological measures but also hinges on the preparedness and knowledge of our team. This document elaborates our systematic approach to employee security training.

**2. Assessment & Policy Framework:**

a. **Organizational Needs Analysis:** Before curating our training approach, we delved into understanding our organizational needs and the access levels of various personnel.

b. **Documented Protocols:** Our assessment led to the formulation of detailed policies and procedures which lay down the foundation for our security training program, including the techniques to be used.

c. **Role-based Responsibilities:** Every stakeholder in our organization, be it managers, system administrators, or general users, has a distinct role to play. Their respective responsibilities towards ensuring organizational security have been clearly defined.

**3. Structured Training Sessions:**

a. **Content Diversity:** Our formal training encompasses a range of topics, highlighting the importance of information security, identification of prevalent threats, adherence to security best practices, and the methodologies for incident response.

b. **Tailored Training:** No two roles in our organization are identical. Acknowledging this, we’ve ensured that the training content is fine-tuned according to the specific needs of different user groups and their respective system access privileges.

**4. Ongoing Annual Mandatory Training:**

* **Training Components:** An annual training mandate exists for all employees, requiring them to undergo sessions on:
	+ Cybersecurity awareness
	+ Insider threat identification
	+ Counterintelligence awareness
	+ Export compliance
	+ Marking of classified information
	+ Derivative classification.

**5. Active Security Awareness Programs:**

a. **Phishing Defense:** Our employees are continually trained to recognize and counteract phishing attempts, equipping them with the knowledge and tools needed to thwart such threats effectively.

b. **DoD Mandatory Training:** All employees that deal with classified data must complete the Department of Defense (DoD) cybersecurity training, ensuring that we consistently meet the high security standards set by the DoD.

**6. System Administrators’ Continuous Learning:**

a. **Vendor-Driven Training:** To ensure our system security remains top-notch, administrators and their backups are encouraged to participate regularly in vendor-specific training sessions. This enhances their familiarity and proficiency with crucial tools and systems.

b. **Specialized Modules:** Our training framework integrates specialized modules to cater to distinct needs, including Microsoft Azure administration and comprehensive comprehension of roles and responsibilities tied to security.

**7. Rigorous Maintenance of Training Records:**

a. **IT Admins’ Training Trail:** Every training session attended is logged in our IT ticketing system. This practice ensures clarity and holds personnel accountable for their training commitments.

b. **Training Records for General Staff:** The Human Resources department is entrusted with the upkeep of training records for the rest of the staff. This ensures that everyone is on the same page and updated with mandatory training modules.

## **Control 3.2.3**

##

## **Control Identifier: 3.2.3**

**Control Title**: Insider Threat Awareness Training

**1. Control Description**: Control 3.2.3 ensures that our organization actively provides security awareness training focusing on recognizing and reporting potential indicators of insider threat.

**2. Implementation Status**: Implemented

**3. Implementation Description**:

a. **Objective**: Our company’s primary goal is to ensure that all our staff members are proficiently educated on identifying signs of insider threats and feel confident in reporting any suspicious activities.

b. **Methodology**:

* + We have instituted an annual review and completion of insider threat training for all our employees.
	+ Our training material derives from the Department of Defense (DoD) insider threat training resources. This choice ensures that the content we provide is up-to-date, relevant, and consistent with government standards.

c. **Supervision**:

* + Our HR manager or an equivalent supervisory role oversees the training’s delivery and completion. This oversight ensures a consistent training experience across our organization and maintains the standards we aim to achieve.

**4. Monitoring & Reporting**:

* + Post-training, our employees are obligated to confirm their understanding. We actively encourage and provide avenues for them to report potential indicators discreetly.
	+ Our internal security or HR team evaluates any reports of suspicious activities, ensuring due diligence and necessary actions.

## **Control 3.3.1**

##

## **System Security Plan (SSP) for Control 3.3.1**

**Control Identifier**: 3.3.1

**Control Title**: System Audit Logs and Records

**1. Control Description**: Control 3.3.1 mandates the creation and retention of system audit logs and records, enabling the monitoring, analysis, investigation, and reporting of any unlawful or unauthorized system activity.

**2. Implementation Status**: Implemented

**3. Implementation Description**:

a. **Objective**: Our primary objective is to continuously monitor, analyze, and report on system activity that may indicate potential security threats or breaches.

b. **Methodology**:

* **SIEM Utilization**: Our SIEM tool (Azure Sentinel) is employed to aggregate and monitor all audit logs, ensuring that even if local event logs are deleted, copies are retained

c. **Event Types and Relevance**:

* We have earmarked specific event types deemed vital for system and operational security, including password changes, failed logons/accesses, administrative privilege usage, and third-party credential applications.
* Event types selected are synchronized with the requirements for each Controlled Unclassified Information (CUI) security provision.

d. **Audit Requirements and Considerations**:

* We determined an appropriate logging level for each event type, ensuring a balance between auditing needs and system performance impacts.
* Explicit content for audit records is determined, capturing essential data such as timestamps, source/destination addresses, user/process identifiers, event details, success/failure status, files involved, and rules invoked.
* We’ve judiciously decided on the necessary detail levels for logs, ensuring clarity while avoiding irrelevant or potentially misleading data.
* Logging requirements encompass distributed transactional processes and activities in cloud architectures.

e. **Retention and Review**:

* Our policy mandates the retention of audit logs for a 6 month period.
* Audit logs undergo routine reviews and analyses, aiding in risk-based decisions and highlighting potential security threats.

f. **Guidance and Best Practices**:

* For effective security log management, we’ve consulted and integrated insights from the NIST Special Publication 800-92.

**4. Monitoring & Reporting**:

* Our SIEM tool and physical premise security system remain pivotal in logging and monitoring all relevant system activities.
* The company has outlined precise audit log requirements for every system within the environment that could produce pertinent security log data. This covers computer endpoints accessing CUI, servers processing CUI, the company firewall, and physical premise security systems.
* Regular analytical reviews of the audit logs pinpoint potential security incidents or abnormalities, promoting timely responses and action.

## **Control 3.3.2**

##

## **System Security Plan (SSP): Control 3.2.2**

#### **Objective**:

Ensure that the actions of individual system users can be uniquely traced to users, so they can be held accountable for their actions.

#### **Implementation**:

1. **User Authentication**:
	* **Active Directory Domain Services (ADDS)**: Our organization uses ADDS to ensure that all users are given unique login credentials. No shared accounts exist within our infrastructure, making it easier to trace activities back to specific users.
2. **Monitoring**:
	* **SIEM Tool Integration**: Our SIEM solution ( Azure Sentinel) is deployed on all company-owned workstations, providing a centralized repository of all system events and user activities.
	* **Privileged-Access Monitoring**: The SIEM tool actively records all privileged-access actions, ensuring that higher-level activities are transparent and traceable.
3. **Physical Tracking**:
	* **Physical Premise Security System**: Our organization has implemented an access badge system to control and monitor access to various parts of our facility. The badge system logs entry and exit times for every user.
	* **Security Cameras**: Strategically placed security cameras capture physical activities within our premises. This provides an additional layer of security and ensures that we can trace physical actions back to individuals.
4. **Event Correlation**:
	* **IP, MAC, & User Correlation**: Every action recorded in our SIEM solution is associated with a specific IP address, MAC address, and user account. This allows for a high level of granularity when tracing actions back to users or devices.
	* **Time-stamped Events**: All logged actions within the SIEM have precise timestamps. This helps in reconstructing events, correlating different activities, and identifying patterns.

## **Control 3.3.3.**

##

## **Control 3.3.3 – Review and Update Logged Events**

**Implementation**:

* **System Integration**: The SIEM tool is deployed across all company endpoints, including Azure AD and Microsoft GGC.
* **Change Control Board (CCB)**: The CCB meets quarterly to discuss all security-related concerns within the organization. The CCB’s responsibilities encompass:
	+ Approving system alterations or upgrades that influence information security.
	+ Setting and refining criteria for Monitorable events.
	+ Recording changes made to the audit criteria.
* **Review Schedule**: The company adheres to a structured review timeline for logged events. Reviews take place quarterly, semi-annually, or annually, contingent upon the associated criticality and risk of particular event types.
	+ **Quarterly Review** (Prioritized due to high criticality or risk):
		- **Failed Login Attempts**: Multiple unsuccessful attempts could signal a brute-force attempt or unauthorized access.
		- **Changes to User Privileges**: Unjustified elevation in user rights might pose significant security threats.
		- **Configuration Changes in Critical Systems**: Alterations to essential system configurations can jeopardize security and operational consistency.
		- **Unusual Data Transfers**: Bulky or atypical data transfers, notably those leaving the company, could indicate data breaches or exfiltration.
		- **Security Patch Failures**: A system becomes susceptible if a crucial security patch isn’t successfully installed.
	+ **Semi-Annual Review** (Moderate frequency, pertaining to medium criticality events):
		- **Inactive User Accounts**: Idle accounts are potential security hazards, especially if they retain access to crucial resources.
		- **Software Installation Logs**: Supervising software installations can pinpoint unauthorized or malicious software.
		- **Database Access Logs**: Periodic assessments can detect anomalous or unauthorized access trends.
		- **VPN Access Logs**: Monitoring access points and timings can reveal potential unsanctioned entries.
	+ **Annual Review** (Less frequent, targeting events of reduced immediate criticality but still vital for extended tracking):
		- **User Training and Awareness Logs**: Confirm completion of obligatory cybersecurity training for all employees.
		- **Hardware Inventory Changes**: Continuously account for all physical devices to ensure none are missing.
		- **Routine System Performance Logs**: Useful in discerning persistent performance patterns or emerging inefficiencies.
		- **Backup and Restoration Logs**: Validate that backups occur at scheduled intervals and that restoration trials are conducted regularly.
* **Incident Analysis**: All logged events undergo thorough examination to gauge their value in incident responses and forensic investigations, ensuring events provide ample data for in-depth analysis and problem-solving.
* **Documentation**: Any modifications to the logged events, whether additions, removals, or other changes, are diligently recorded in our ticketing system.
* **Implementation Solutions**:
	+ SOCs solution oversees and audits security logs.
	+ Endpoint management is executed via a specialized solution, promising complete device coverage.
* **Regular Reviews**: Events and incidents are deliberated during the quarterly risk management meetings. Real-time event monitoring is orchestrated by both IT and facility technical systems, along with the ticketing system, assuring prompt reactions and interventions as scenarios unfold.

## **Control 3.3.4**

##

## **System Security Plan (SSP)**

**Control 3.3.4: Alert in the Event of an Audit Logging Process Failure**

**Implementation:**

**1. Role-Based Alert Configuration at [Company Name]:**

* **Personnel/Roles for Alerts:** At our company, we have configured specific roles, including ‘administrator’ and ‘standard user’, in our SIEM system, Microsoft Sentinel. This ensures that designated personnel receive real-time alerts tailored to their specific roles.
* **Role Demarcation:** Within our organization, only authorized team administrators receive alerts regarding audit logging failures, ensuring a confidential and efficient response.

**2. Alert Triggers & Types at [Company Name]:**

* **Defined Failures:** Our SIEM system is calibrated to recognize and alert for specific audit logging process failures. Examples of these failures include:
	+ Log transmission interruptions from endpoints.
	+ Unauthorized access attempts to the logging system.
	+ Log data corruption or deletion.
	+ Overload or system crashes disrupting logging processes.

**3. System Health & Logging Integrity at [Company Name]:**

* **End-to-End Logging:** Our SIEM system Microsoft Sentinel ensures the integrity of log transmissions from every endpoint. Disruptions or failures in this process immediately trigger alerts.
* **SIEM System Health:** Beyond just external monitoring, our SIEM system is equipped to perform internal diagnostic checks. Any internal malfunctions trigger instantaneous alerts.

**4. Verification & Proof at [Company Name]:**

* **Support Tickets:** In case of an audit process logging failure, a support ticket is automatically generated. Subsequently, our Incident Response Procedures for Audit Logging Failures is activated. (Document attached.).

**5. Configured Alerting Mechanism at [Company Name]:**

* **Notification Channels:** We have established a multi-channel notification system that includes email alerts, SMS messages, and direct notifications, ensuring that any discrepancies in audit logging are promptly communicated.
* **Assigned Responsibility:** We have trained and designated specific teams or personnel as the primary responders to these alerts, reinforcing our commitment to swift and effective countermeasures.
* **Escalation & Incident Response:** Clear escalation procedures are in place at [Company Name]. Furthermore, our documented incident response protocol guides the systematic investigation, troubleshooting, and recovery from any detected audit logging anomalies.
* **Record Maintenance:** Our commitment to transparency and accountability is evident in our meticulous record-keeping. All detected failures, along with their respective investigative actions and resolutions, are diligently documented within our company’s ticketing system.

## **Control 3.3.5**

##

## **Control 3.3.5: Correlation of Audit Record Review, Analysis, and Reporting Processes**

Control Description: The objective is to establish a correlation between audit logs, their review, analysis, and subsequent reporting processes. This mechanism ensures that the system can proactively identify and respond to indicators of potentially unlawful, unauthorized, suspicious, or unusual activities.

**Implementation at [Company Name]:**

Our approach is facilitated by our integrated SIEM and SOC systems:

**SIEM System Purpose:** The SIEM (Security Information and Event Management) system acts as an integrated platform offering real-time analysis of security alerts generated by our hardware and software infrastructures. Its design provides a comprehensive perspective on an organization’s information security by collecting, storing, and analyzing logs and security events from various sources, thus enabling efficient threat detection and compliance reporting.

**SOC’s Role:** Our Security Operations Center (SOC) serves as the nerve center for monitoring, evaluating, and combating cybersecurity threats. Operated by a dedicated team of security experts, the SOC consistently oversees our IT infrastructure to identify, analyze, address, and mitigate potential security incidents. Their expertise is geared towards a proactive approach to security, including advanced threat hunting, forensic analysis, and incident response capabilities.

With the support of our Security Operations Center (SOC) Team, this system guarantees a reduction in false positives and delivers context-rich actionable intelligence.

**Security Operations Center (SOC) Team Responsibilities:**

* Our SOC team excels in identifying and prioritizing Indicators of Compromise (IoCs).
* They systematically assess logs to determine necessary escalation measures and reporting protocols.
* Management receives email notifications for any flagged suspicious activities. Following this, the SOC team liaises with pertinent departments to confirm and mitigate potential threats.

**Response & Remediation Procedures:**

The severity of any detected anomaly dictates our course of remediation. In situations that demand heightened responses, we activate our incident response plan protocol, which is tailored to tackle indicators of unlawful, unauthorized, suspicious, or unusual activities.

**Company Name]’s Protocol for Handling Security Events Pertaining to CUI**:

1. **Immediate Reporting to DC3**:
	* Upon identifying a security event related to CUI, our first step is to promptly report the incident to the Defense Industrial Base (DIB) Cyber Incident Reporting and Response program.
	* As a partner working with DoD data, we acknowledge the DoD Cyber Crime Center (DC3) as the focal point for addressing reports of technological vulnerabilities and cyber incidents.
2. **Internal Notification**:
	* Concurrently, the incident is escalated internally to our designated Security Officer or the respective department responsible for handling such security breaches. Their guidance steers our subsequent actions and ensures we adhere to established protocols.
3. **Engagement with Security Agencies**:
	* Depending on the breach’s scope and implications, we might engage with local or federal law enforcement bodies, including but not limited to the FBI, to ensure a comprehensive response.
4. **Adherence to NIST Guidelines**:
	* Being compliant with NIST SP 800-171 standards, our organization has embedded the guidelines’ mandates into our operations. As such, any CUI-related incident automatically invokes the specific incident response and reporting procedures set forth by these guidelines.
5. **Meticulous Documentation**:
	* We believe in the utmost transparency and accountability during incident handling. Therefore, a comprehensive record is maintained, capturing all relevant details about the event, actions undertaken, and communications made. This rigorous documentation not only aids investigations but establishes a basis for any future references or legal inquiries.
6. **Prompt Mitigation Actions**:
	* Recognizing the criticality of immediate response, our teams initiate mitigation measures to contain and reduce the impact of the breach. These actions could range from isolating compromised systems and changing access credentials to enhancing surveillance on potential data exit nodes.

This protocol underscores [Company Name]’s commitment to safeguarding CUI and underscores our proactive and structured approach to potential security threats.

## **Control 3.3.6**

##

## **System Security Plan (SSP) for [Company Name]Control Number:** 3.3.6

**Control Title:** Provide audit record reduction and report generation to support on-demand analysis and reporting.

**I. Control Overview:**

The objective of this control is to ensure that audit records are efficiently reduced and organized such that on-demand analysis and reporting can be promptly and accurately conducted.

**II. Implementation at [Company Name]:**

**A. SIEM Tool Deployment:**

* The SIEM tool is deployed across all company-owned workstations. This centralized system automatically aggregates logs from all integrated workstations.
* Alerts of a serious or critical nature are immediately sent to both our Security Operations Center (SOC) and IT department, thereby streamlining the incident detection process.
* This automation eliminates the need for IT support staff to comb through event logs manually, ensuring more timely responses to potential threats.

**B. Reporting Capabilities:**

* The SIEM tool allows for the generation of diverse reports, such as logon failures and the detection of anomalous user logins. This not only helps in identifying potential threats but also enables the organization to discern broader cybersecurity trends.

**C. Assessed Audit Record Collection:**

* The responsibility for collecting audit records has been delegated to specific individuals or teams within the company. This ensures accountability and clarity in the audit process.
* Audit information structure and format have been standardized to facilitate consistent data analysis.

**D. Time Stamp Granularity:**

* Adjustments have been made to the time stamp granularity within the SIEM tool to enhance the precision of event logging.

**E. Defined Report Templates:**

* Based on prior identified reporting needs, customizable report templates have been crafted. These templates ensure that reports are consistently structured while still allowing for flexibility based on specific analysis requirements.

**F. Established On-Demand Procedures:**

* A clear procedure has been defined for on-demand access and analysis of audit records. This ensures that when real-time or impromptu reports are needed, there’s a standardized method to generate and deliver them.

**III. Solution Overview:**

* + Together, the SIEM tool and Siemens SOC solution create a robust and integrated system that aligns with the organization’s commitment to cybersecurity and compliance with the defined control objectives.

## **Control 3.3.7**

##

## **System Security Plan (SSP) for [Company Name]**

**Control Number**: 3.3.7

**Control Title**: Provide a system capability that compares and synchronizes internal system clocks with an authoritative source to generate timestamps for audit records.

**II. Implementation at [Company Name]**:

A. **SIEM Tool Time Synchronization**: Our SIEM tool synchronizes its time with public time servers. This ensures that the timestamps provided are consistent with universally accepted time standards.

B. **Azure-Joined Computers**: Computers integrated with Azure synchronize automatically with public time servers. This adds a layer of consistency and accuracy to our timestamp recording.

C. **Domain Controller as the Authoritative Time Source**: Group policies designate the domain controller as the authoritative time source for the domain. This controller sources its time from internal Microsoft time servers, which in turn derive their time from Microsoft’s Stratum 1 devices equipped with GPS antennas.

D. **Time Synchronization Service**: Every host computer boasts a time synchronization service. This service, familiar with the designated time servers, checks periodically if computer clocks need adjustment. Should discrepancies arise, the service makes the necessary corrections. This meticulous synchronization process ensures that our audit logs bear consistent timestamps.

E. **Time Measurement & Granularity**: Internal system clocks generate timestamps, capturing both date and time. These timestamps are presented in Coordinated Universal Time (UTC)—a contemporary iteration of Greenwich Mean Time (GMT)—or as local time adjusted from UTC. The granularity of our time measurement synchronizes our system clocks with reference clocks. Different granularities are set for different system components to guarantee timestamp precision.

**IV. Compliance with IETF Standards**: Our dedication to time synchronization complies with the standards delineated by the IETF, as outlined in IETF 5905. This ensures our synchronization methods align with globally accepted best practices.

## **Control 3.3.8**

##

## **System Security Plan (SSP) – Control 3.3.8**

**Control Identifier:** 3.3.8

**Control Title:** Protect audit information and audit logging tools from unauthorized access, modification, and deletion.

**Control Description:**

This control focuses on safeguarding audit information and audit logging tools from unauthorized access, alterations, and deletions. Our organization takes comprehensive measures to achieve this control requirement, as detailed below:

**Security Information and Event Management (SIEM):**

* Our organization employs a Security Information and Event Management (SIEM) system to manage and retain audit logs effectively. This SIEM system operates independently, ensuring the integrity and security of audit data.
* The SIEM solution may be either cloud-based or on-premises, but it is always implemented as a separate and isolated system.
* Access to the SIEM system is protected by its own secure login system, independent of other authentication mechanisms like Active Directory.

**Immutable Audit Logs:**

* Audit logs and records are configured to be immutable for a minimum period of one year. Once data is written into the system, it cannot be erased or modified within this timeframe.

**Limited Access:**

* Only authorized users with explicit permissions have access to the SIEM solution. Unauthorized access to the SIEM system is not possible, as it is entirely isolated and air-gapped from other systems.

**Protection of Audit Information:**

* Audit information encompasses all relevant data, including audit records, audit log settings, and audit reports, necessary for conducting system activity audits.

**Technical Protections:**

* Technical safeguards are implemented to prevent unauthorized access to audit information. These safeguards include robust authentication mechanisms, encryption, and access controls.

**Limitations on Audit Logging Tools:**

* Access to and execution of audit logging tools are restricted to authorized individuals with the appropriate permissions. Unauthorized use or execution of these tools is not allowed.

**Physical and Environmental Protections:**

* Physical protection of audit information is addressed through media protection measures and compliance with physical and environmental protection requirements.

##

## **Control 3.4.2**

##

## **System Security Plan (SSP) – Control 3.4.2: Security Configuration Settings****Purpose**: Ensure the establishment and enforcement of security configuration settings for all IT products used within the organization.**Scope**: This SSP encompasses all IT products, both hardware and software, utilized within our organization, including servers, workstations, mobile devices, and networking equipment.**1. Definition and Documentation**:

* + A documented annual baseline configuration is maintained. This baseline provides a standardized set of security configuration settings for all IT products.
	+ Whenever significant changes to the system are made, this documentation will be updated to reflect the new baseline configuration.
	+ Any departures from the baseline must be documented with a rationale and approved by the IT Security Manager.
1. **2. Configuration Implementation and Enforcement**:
	* **Group Policy**: All group policies are set as per the annual baseline configuration. Ability exists to link, unlink, enforce, and not enforce these policies as required.
	* **Firewall**: Firewall configurations are standardized to block all unauthorized inbound and outbound traffic and only allow necessary ports, services, and applications to function.
	* **VPN**: A VPN solution is in place to ensure encrypted and secure remote access to the organization’s network resources.
	* **Endpoint Management Solution**: Devices are managed to ensure they adhere to the required security configurations.
	* **Security Information and Event Management (SIEM)**: SIEM solutions are in place to monitor and alert on any deviations from the baseline configuration in real-time.
2. **3. Conditional Access and Device Configurations with InTune**:
	* All devices, whether mobile or desktop/laptops, have InTune configurations implemented.
	* InTune conditional access policies serve as the baseline security configuration for all user devices.
	* Regular checks are done to ensure all devices remain compliant with these configurations.
3. **4. Review and Update**:
	* Periodic reviews of the security configuration settings will be conducted to ensure they remain effective and relevant.
	* Any updates or changes to the baseline configuration will be communicated to all relevant stakeholders.
4. **5. Responsibilities**:
	* **IT Security Manager**: Overall responsibility for the establishment and maintenance of the security configuration settings and the annual baseline configuration documentation.
	* **System Administrators**: Ensure that all systems are configured according to the established settings. Responsible for implementing, managing, and monitoring group policies, firewall configurations, VPN settings, and endpoint management solutions.
	* **Device Managers**: Ensure that all devices are compliant with the InTune conditional access policies and device configurations.
5. **6. Training & Awareness**:
	* All staff members will be made aware of the importance of adhering to the security configuration settings.
	* Periodic training sessions will be conducted to keep staff informed about any changes to the baseline configuration and how to maintain compliance.
6. **7. Reporting & Auditing**:
	* Regular audits will be conducted to ensure compliance with the established security configuration settings.
	* Any deviations or violations will be reported, and corrective actions will be taken.

## **Control 3.4.5**

##

## **System Security Plan (SSP) – Control 3.4.5: Define/Document/Approve/Enforce Physical/Logical Access Restrictions****Purpose:** To ensure that all changes, both physical and logical, to organizational systems are properly defined, documented, approved, and enforced.**Scope:** This procedure covers any changes to the hardware, software, and other related components of the company’s IT infrastructure.

* 1. **Authorization for Changes:**
		+ The [INSERT NAME/POSITION] is the sole individual empowered to authorize changes to the company’s hardware and software infrastructure.
		+ All proposed changes must be presented and approved by this individual before any alterations commence.
	2. **Execution of Changes:**
		+ [INSERT ENTITY/DEPARTMENT NAME] holds exclusive rights to conduct approved changes to the infrastructure.
		+ All changes, once approved, are conducted strictly under the purview and oversight of this entity.
	3. **Documentation and Record-keeping:**
		+ All approved changes are meticulously recorded in the central ticketing system maintained by [INSERT ENTITY/DEPARTMENT NAME].
		+ This record retention ensures traceability and accountability for all changes made to the system.
		+ On a monthly basis, a summarized report of all changes made to the system will be provided to the company by [INSERT ENTITY/DEPARTMENT NAME].
	4. **Physical Access Restrictions:**
		+ **Secure Area for CUI & Sensitive Assets:**
			- All Controlled Unclassified Information (CUI), servers, backup systems, network appliances, and other sensitive technological assets are housed in a specially designated secure area of the building.
			- This area has been structurally fortified and equipped with additional security measures to deter unauthorized access, tampering, or compromise.
		+ **Access Control to Secure Area:**
			- The IT closet or office within this secure area, which houses these crucial components, is kept securely locked at all times.
			- Access to this secured zone is strictly regulated. Only personnel explicitly authorized by [INSERT NAME/POSITION] and who have a demonstrated need-to-know are granted permission to access this space.
			- A biometric or card-based access control system, combined with CCTV surveillance, ensures that entry and exit are logged and can be audited if necessary.
		+ **Escorted Access:**
			- Any other individual requiring access to the secured area for professional purposes must be escorted at all times while inside. An entry and exit log will be maintained, noting the reason for the visit and the duration of the stay.
	5. **Roles and Responsibilities:**
		+ [INSERT NAME/POSITION]: Holds the authority to grant and authorize changes to the system’s hardware and software components.
		+ [INSERT ENTITY/DEPARTMENT NAME]: Executes approved changes and maintains a record of all such changes in the central ticketing system.
		+ IT Security Team: Ensures that the process laid out in this SSP is adhered to and may assist [INSERT NAME/POSITION] in the evaluation of proposed changes for potential security risks.
	6. **Implementation Procedure:**
		+ All changes to the system, both physical and logical, are documented within this System Security Plan (SSP).
		+ Steps leading to the implementation of approved changes are articulated in the accompanying Plan of Action and Milestones (POA&M).
	7. **Review and Updates:**
		+ This SSP, along with its associated processes, will undergo periodic review to ensure it meets the evolving needs and challenges of the organization.
		+ Adjustments, when necessary, will be made following the same procedure of approval and documentation laid out in this plan.

## **Control 3.4.6**

##

## **System Security Plan (SSP) – Control 3.4.6Control Title**: Employ the Principle of Least Functionality**Control Requirement**: Configure organizational systems to provide only essential capabilities.**Implementation Status**: Implemented**Implementation Details**:

* 1. **Service-Level Controls**:
		+ All services within the organization operate without admin-level credentials. This ensures that even if a service is compromised, the potential damage is contained within the bounds of that service’s permissions.
		+ Services are strictly designed and monitored to ensure they only offer required functionalities, reducing potential avenues of attack.
	2. **Endpoint Management**:
		+ The organization leverages Active Directory with Group Policy to ensure granular control over system functionalities.
		+ Controls are in place to dictate which applications can be installed, executed, and which internet destinations are accessible.
		+ The endpoint management system effectively manages file system permissions, ensuring that users can only access the files they need for their respective duties.
	3. **Access Based on Role**:
		+ Permissions are granted based solely on job requirements. If a role doesn’t necessitate access to specific data or functionality, that access is not granted.
		+ Continuous auditing and review processes are in place to ensure access permissions align with job duties and to revoke unnecessary access promptly.
	4. **Physical Premise Access Control**:
		+ The organization employs a stringent physical premise access control system.
		+ Access to specific zones, like IT closets or server rooms, is limited only to personnel whose roles necessitate it.
		+ Unauthorized access to sensitive areas is detected and promptly acted upon to ensure the physical security of IT resources.

## **Control 3.4.7**

##

**System Security Plan (SSP) – Control 3.4.7**

**Control Title:** Restrict/Disable/Prevent the Use of Non-Essential Programs, Functions, and Protocols

**Control Requirement:** The organization must limit the access and execution of non-essential software and protocols to mitigate potential security risks.

**Implementation Status:** Implemented

**Implementation Details:**

1. **Firewall Restrictions:**
	* Limited inbound access points via the corporate firewall, providing a strong front against cyber threats.
	* Configured to specifically limit the services, protocols, and functions accessible, serving as the primary defense layer against potential intrusions.
2. **Software Control & Execution Restrictions:**
	* Non-critical software execution necessitates explicit role-based approval, ensuring a controlled environment.
	* Auto-execute features are disabled, reducing the risk of unintended software actions.
	* A combined approach of both program blacklisting and whitelisting guarantees that only essential software is operational.
	* Simultaneous execution of identical program instances is controlled, ensuring software processes don’t overrun system capacities.
3. **Protocol Restrictions:**
	* Protocols, including but not limited to Bluetooth, FTP, and peer-to-peer networking, undergo rigorous scrutiny. Based on their security implications, they are either restricted, limited, or outright disabled.
4. **Group Policy Management:**
	* Serving as the cornerstone of our security strategy, the group policy management solution dictates the permissible software landscape:
		+ Dictates the allowed program executions.
		+ Restricts the spontaneous installation of unapproved software.
		+ When combined with the firewall, it provides a layered defense mechanism ensuring the sanctity of organizational endpoints.

**Notes:** The organization commits to a dynamic security strategy, continuously evaluating and configuring what protocols, ports, and functions are permissible. This proactive approach ensures that as the cyber threat landscape evolves, our defenses remain robust and adaptive.

## **Control 3.4.8**

##

**System Security Plan (SSP) – Control 3.4.8**

**Control Title:** Apply Blacklist or Whitelist Policy to Prevent/Permit the Use of Software

**Control Requirement:** The organization must establish and rigorously enforce a policy that delineates software permissions, blocking or allowing specific software installations based on comprehensive organizational needs and meticulous security assessments.

**Implementation Status:** Fully Implemented

**Implementation Overview:**

**1. Group Policy and Active Directory Configuration:**

* **Software Restriction via Group Policy:** Through meticulous configuration of our Group Policy, we ensure that installation of software is contingent upon express authorization from a designated IT administrator.
* **Dynamic Behavior Regulations:** The Group Policy has been further fortified to encompass various behaviors, most notably the initiation of non-sanctioned software. These restrictions are modulated based on specific Organizational Unit (OU) affiliations.
* **Active Directory Organizational Units (OU) Configurations:** Our Active Directory structure allows for nuanced software permissions across OUs. This granularity ensures that departments are provisioned software access pertinent to their operational necessities.

**2. User Permissions & Approvals:**

* **Restricted Installation Capabilities:** To safeguard against potential vulnerabilities, software installations are contingent upon involvement and oversight by a certified IT administrator.
* **Senior Management Approval:** Prior to the integration of new software into our operational ecosystem, it mandates approval from our senior management, ascertaining its relevance and safety for business operations.
* **Whitelisting Requests & Trouble Tickets:** For access to non-preapproved software or websites, users must formally submit a comprehensive request to the IT department, ensuring centralized oversight and stringent security checks.

**3. Continuous Monitoring & Policy Management:**

* **Regular Policy Updates:** Our IT team perpetually refines and amends our software policies, ensuring alignment with evolving business requirements and emergent security threats.

**4. Specific Implementations and Processes:**

* **Blacklisting Policy:** A meticulously curated policy is in place that proscribes specific undesired software. This list undergoes periodic reviews and updates based on the latest security intelligence.
* **Whitelisting Policy:** Concurrently, a roster of sanctioned software has been delineated, underpinned by rigorous verification mechanisms such as cryptographic checksums and digital signatures.
* **Technical Controls:** Advanced technological tools are deployed to assert that only whitelisted software operates within our infrastructure.
* **Periodic Audits and Assessments:** Regular assessments are conducted to corroborate adherence to our blacklisting and whitelisting policies, and to promptly rectify any aberrations.
* **Documentation & Compliance:** A comprehensive record detailing our software-related policies has been archived, including the rationale for each directive and the verification mechanisms employed.

**Review Date:** [Quarterly/Bi-annually/Annually]

**Reviewer:** [Senior Security Officer/ CISO]

## **Control 3.4.9**

**System Security Plan (SSP) – Control 3.4.9**

**Control Title:** Control and Monitor User-Installed Software

**Objective:**To control and monitor the installation and execution of software on company machines, ensuring the safety and integrity of the IT environment.

**Implementation Status:** Implemented

**Implementation Details:**

**1. No Local Administrator Accounts:**To ensure the secure management of software, the company has abolished local administrator accounts on all machines belonging to non-administrator level employees. This ensures that only a standard user access is granted, thereby preventing unauthorized software installations.

**2. Software Installation Requires Admin Access:**Any software installation mandates administrator-level access, reinforcing our security posture against potential threats. This elevated access is exclusively provisioned via Active Directory and is reserved for IT administrators or those with explicit authorization.

**3. Request Protocol for Software Changes:**All software alteration requests are to be channeled through the company’s IT ticketing system. This structured approach ensures a traceable record of every software change request, ensuring transparency and accountability.

**4. Approval and Implementation Mechanism:**If a software request is approved, it is executed by the System Security Administrator or another designated authority in the organization. Each software request undergoes a thorough evaluation process, and an impact analysis is conducted before the actual installation.

**5. Monitoring Software Execution:**Software execution within the organization is continually observed through our SEIM (Security Information and Event Management) SOC (Security Operations Center) system. Additionally, we employ an Endpoint Management System for granular monitoring. These systems are equipped to:

* Analyze log files from critical devices, checking for any unusual or unauthorized activities.
* Detect malicious activities, restricting their execution, and alerting the relevant authorities.

**6. Endpoint Management Solution:**Beyond the SEIM SOC system, our Endpoint Management solution, comprising antivirus software and other security tools, is strategically positioned to control, detect, and mitigate risks on individual endpoints. If malicious activity is detected, the system is designed to instantly suppress it and raise an alert.

**7. User Permissions and Installation Protocol:**Our policy strictly prohibits users from installing any software without the necessary administrative clearance. All software installation requests must be routed through the Change Control Board (CCB), and an impact analysis is mandatorily performed before the green light is given for the software’s installation.

**Review and Audit:**

Routine audits and assessments will be conducted to ensure the effectiveness of the implemented controls and monitor unauthorized software installations. These evaluations will ensure our system remains robust as the organization’s needs evolve and new software threats surface.

**Review Date:** [Quarterly/Bi-annually/Annually]

**Reviewer:** [Senior Security Officer/ CISO]

## **Control 3.5.2**

####

#### **1. Introduction**

[Company Name] is committed to maintaining robust and secure authentication protocols to protect organizational systems and Controlled Unclassified Information (CUI). This SSP outlines our practices, mechanisms, and measures to authenticate and verify the identities of users, processes, and devices.

#### **2. Authentication Mechanisms**

* **User Authentication:** Users must provide individual authenticators, such as passwords, key cards, or cryptographic devices, to gain access.
* **Multi-Factor Authentication (MFA):** Combines two or more different types of authenticators, ensuring a stronger authentication process.
* **Device and Process Verification:** Implemented mechanisms to verify the identities of devices and processes, including those that interact with organizational systems.
* **Initial Authenticator Content:** Ensured the organization’s security standards are met, such as minimum password length.
* **Avoidance of Factory Default Credentials:** Avoided easily discoverable default credentials that may pose security risks.

#### **3. Authenticator Management**

* **Configuration and Management:** Configured system components to support organization-defined settings and restrictions for authenticator characteristics.
* **Managing Issued Authenticators:** Managed authenticators securely, revoking and removing them when no longer needed.
* **Compliance with SP 800-63-3:** Followed best practices on digital identities for authenticator management and identity verification.
* **Reviews and Assessments:** Conducted regular assessments to ensure effectiveness and alignment with industry practices.
* **User Education:** Educated users on strong authentication practices, including the protection of passwords.

#### **4. Monitoring and Logging**

* **Monitoring and Logging of Events:** Captured relevant information on authentication events, supporting incident response, auditing, and investigations.
* **Integration with Other Security Controls:** Integrated with access control systems, enhancing overall system protection.

#### **5. Access Control and Verification Philosophy**

Access control at [Company Name] is more than just implementing technical measures. It’s about understanding who needs access to what information and ensuring that the right people have the right access. This approach is evidenced by:

* **Controlled Access:** No open access to CUI, with verification required for access to ensure authorized interaction.
* **Physical Access Control:** Measures like security badges and camera verification at entrances for physical areas where CUI is handled.
* **Layered Security:** Collaborative integration of IT security controls, including passwords and multi-factor authentication.

#### **6. Conclusion**

The authentication and verification practices outlined in this SSP underscore [Company Name]’s commitment to security and compliance. As we continue to evolve and adapt to new threats, we remain steadfast in our dedication to ensuring that our systems, users, and information are protected.

## **Control 3.5.3**

##

1. **System Security Plan (SSP) – Example
I. Introduction**This System Security Plan (SSP) details the measures implemented by our organization to comply with the requirements of NIST SP800-171, focusing on Control 3.5.3 concerning multifactor authentication (MFA). The following sections explain how we have deployed MFA and related security measures to ensure secure access to our systems.
**II. MFA Implementation for Privileged and Non-Privileged Accounts**
	1. **Privileged Accounts:**
		* **Implementation:** Implemented MFA for local and network access to privileged accounts, requiring at least two different factors to authenticate users.
		* **Authentication Factors:** Utilized various factors such as passwords, cryptographic devices, tokens, or biometrics to establish robust authentication.
		* **MFA Solutions:** Deployed MFA solutions involving hardware tokens, smart cards, or commercial MFA solutions with replay resistance.
	2. **Non-Privileged Accounts:**
		* **Extension of MFA:** Extended MFA to network access for non-privileged accounts, requiring multiple authentication factors for users or processes accessing the systems through network connections.
		* **Network Access:** Implemented MFA across various networks including LANs, WANs, and the Internet.
		* **Remote Access:** Identified and implemented MFA for remote access connections, using additional security measures like encrypted VPNs.
	3. **Tokens and Credentials:**
		* **Hard and Soft Tokens:** Utilized both hard (e.g., smart cards) and soft tokens to securely store user credentials.
	4. **Integration at System and Application Levels:**
		* **Integration Points:** Integrated MFA mechanisms at both system (e.g., at logon) and application levels when necessary to enhance information security and prevent unauthorized access.
	5. **Compliance and Best Practices:**
		* **Guidance and Standards:** Followed guidance provided in SP 800-63-3 for digital identity best practices, including MFA.
		* **Regular Review:** Regularly reviewed and updated MFA mechanisms and processes to align with evolving threats, industry best practices, and organizational needs.

## **Control 3.5.6**

##

**System Security Plan (SSP) for Account Inactivity Management**

**1. Overview**

This document outlines the policy and procedures for managing accounts that are no longer in use within our system. The primary focus is on disabling user accounts that have been inactive for more than 180 days. This process is automated through PowerShell scripts and task scheduling, as part of our ongoing commitment to maintaining a secure and efficient operating environment.

**2. Purpose**

The purpose of this policy is to reduce the potential security risks associated with inactive user accounts. By regularly monitoring and disabling accounts that are no longer in use, we minimize the chance of unauthorized access and ensure that only active users have access to our system resources.

**3. Scope**

This policy applies to all user accounts within our system, regardless of their roles or permissions. It encompasses both regular user accounts and privileged administrative accounts.

**4. Policy**

* **4.1 Inactivity Monitoring:** An annual service ticket is created to check for accounts that have not been logged in for more than 180 days.
* **4.2 Account Disabling:** If an account meets the inactivity threshold, it will be disabled automatically.
* **4.3 Automation:** This activity is implemented through PowerShell scripts and task scheduling, providing an efficient and consistent approach to inactivity management.

**5. Technology Description**

PowerShell, a task automation and configuration management framework developed by Microsoft, is utilized for this process. It includes a command-line shell and scripting language built on the .NET Framework, allowing for robust and flexible automation solutions.

**6. Responsibilities**

* **System Administrators:** Responsible for maintaining the PowerShell scripts, task scheduling, and monitoring the annual service tickets.
* **Security Team:** Responsible for overseeing the policy and ensuring that it aligns with organizational security requirements.
* **Users:** Responsible for informing the IT department if they anticipate their accounts will be inactive for extended periods.

**7. Review and Updates**

This policy will be reviewed annually or as needed to ensure that it continues to meet our organizational goals and regulatory requirements.

## **Control 3.5.7**

##

#### **1. Overview:**

This document outlines the policy, controls, and audit procedures for managing password complexity within our organization. This is essential for safeguarding information integrity and is implemented in alignment with the compliance standard.

#### **2. Scope:**

The policy applies to all organizational units within the company and covers all user accounts that require password authentication.

#### **3. Policy Statement:**

##### **3.1 Password Complexity:**

* **Minimum Length**: Passwords must be at least 12 characters in length.
* **Complexity Requirements**: Passwords must meet complexity requirements, including the use of upper and lowercase letters, numbers, and special characters.

##### **32 Group Policy:**

* **Application**: Group policy will enforce these requirements and be applied to all organizational units.
* **Enforcement**: This policy ensures that all systems are configured with the necessary settings, in line with our compliance requirements.

#### **4. Auditing:**

* **Annual Audits**: This policy will be audited yearly to ensure that the controls are effective and aligned with the compliance standard.
* **Audit Records**: All audit records, including findings and corrective actions, will be properly documented and retained as per the organization’s retention policy.

#### **5. Responsibilities:**

* **IT Security Team**: Responsible for implementing, maintaining, and auditing the policy.
* **Employees**: Responsible for complying with the policy and reporting any inconsistencies or breaches.
* **Management**: Responsible for the overall oversight and support of this policy’s implementation.

## **Control 3.5.8**

##

Example SSP – System Security Plan

1. **Policy Statement**: The organization has implemented a policy to prohibit password reuse for a specified number of generations.
2. **Password Generation and Management**:
	1. Temporary passwords are generated and provided to users upon registration or password reset requests.
	2. Users are prompted to change their temporary passwords to permanent ones immediately after system logon.
	3. Password complexity requirements are enforced, including minimum length, character types, and expiration period.
3. **Password History**:
	1. The system tracks the specified number of generations (e.g., N generations) based on organizational security requirements.
4. **Password Reuse Prohibition**:
	1. When users attempt to change their passwords, the system checks against the password history log to ensure the new password has not been used within the specified number of generations.
	2. If the new password matches any of the previously used passwords, the system rejects the change request and prompts the user to choose a different, unused password.
5. **Configuration Settings**:
	1. The system is configured to enforce password reuse restrictions for N generations, as specified by the organizational security policy.
	2. Password history log size is set to retain the required number of previous passwords for each user.
6. **User Notifications**:
	1. Users are informed about the password reuse policy during account creation, password reset, or password change processes.
	2. Users are advised to choose strong, unique passwords that have not been used within the specified number of generations.
7. **Monitoring and Auditing**:
	1. The IT security team regularly monitors the system logs to ensure compliance with the password reuse policy.
	2. Detected violations are reported and addressed promptly.
8. **Exceptions**:
	1. Exceptions to the password reuse policy may be granted on a case-by-case basis, subject to approval by the appropriate authority (e.g., IT security manager).
	2. All exceptions are documented, justified, and periodically reviewed.

## **Control 3.5.9**

##

Example SSP – System Security Plan

1. **Policy Statement**: The organization has implemented a policy to prohibit password reuse for a specified number of generations.
2. **Password Generation and Management**:
	1. Temporary passwords are generated and provided to users upon registration or password reset requests.
	2. Users are prompted to change their temporary passwords to permanent ones immediately after system logon.
	3. Password complexity requirements are enforced, including minimum length, character types, and expiration period.
3. **Password History**:
	1. The system tracks the specified number of generations (e.g., N generations) based on organizational security requirements.
4. **Password Reuse Prohibition**:
	1. When users attempt to change their passwords, the system checks against the password history log to ensure the new password has not been used within the specified number of generations.
	2. If the new password matches any of the previously used passwords, the system rejects the change request and prompts the user to choose a different, unused password.
5. **Configuration Settings**:
	1. The system is configured to enforce password reuse restrictions for N generations, as specified by the organizational security policy.
	2. Password history log size is set to retain the required number of previous passwords for each user.
6. **User Notifications**:
	1. Users are informed about the password reuse policy during account creation, password reset, or password change processes.
	2. Users are advised to choose strong, unique passwords that have not been used within the specified number of generations.
7. **Monitoring and Auditing**:
	1. The IT security team regularly monitors the system logs to ensure compliance with the password reuse policy.
	2. Detected violations are reported and addressed promptly.
8. **Exceptions**:
	1. Exceptions to the password reuse policy may be granted on a case-by-case basis, subject to approval by the appropriate authority (e.g., IT security manager).
	2. All exceptions are documented, justified, and periodically reviewed.

## **Control 3.6.1**

**System Security Plan (SSP) – Control 3.6.1**

**Control Title:** Operational Incident-Handling Capability

**Control Requirement:** Establish an operational incident-handling capability for organizational systems that encompasses the following activities: preparation, detection, analysis, containment, recovery, and user response.

**Implementation Status:** Implemented

**Implementation Details:**

**Incident Response Plan (IRP) Integration:**

1. **Preparation:**
	* The organization has defined and documented its approach to incident response within the Incident Response Plan (IRP).
	* All personnel undergo regular training and awareness sessions on the IRP, ensuring readiness to respond to potential incidents.
	* The organization maintains a dedicated Incident Response Team (IRT) equipped with the necessary tools and resources to handle incidents.
2. **Detection:**
	* Using advanced monitoring solutions, potential security threats are detected in real-time.
	* Alerts are configured to notify the IRT of any anomalies or potential security breaches, ensuring swift detection.
3. **Analysis:**
	* Upon receiving an alert, the IRT performs a comprehensive analysis to ascertain the nature, scope, and impact of the incident.
	* Correlation tools and threat intelligence platforms aid in understanding the threat context and the potential risk to organizational assets.
4. **Containment:**
	* Immediate steps are taken to isolate the affected systems or components to prevent further compromise or spread of the incident.
	* Both short-term (immediate) and long-term (permanent) containment strategies are employed, as defined in the IRP.
5. **Recovery:**
	* The IRT works diligently to restore and validate system functionality for business operations to resume.
	* Necessary patches, updates, or configuration changes are applied to ensure the vulnerability or entry point of the incident is addressed.
6. **User Response Activities:**
	* The organization maintains open channels of communication to keep users informed during and after an incident.
	* Affected users receive guidance on protective and remedial measures they should take in the aftermath of an incident.

The entirety of these activities and procedures is implemented via the organization’s Incident Response Plan (IRP) and its associated procedures. Regular audits and reviews ensure the IRP’s efficacy and alignment with evolving threat landscapes and organizational requirements.

**Review Date:** [Quarterly/Bi-annually/Annually]

**Reviewer:** [Incident Response Team Lead/ CISO]

## **Control 3.6.3**

**System Security Plan (SSP) for Control 3.6.3: Test the Organizational Incident Response Capability**

**Policy Statement:**Our organization is committed to conducting regular testing of its incident response capability to assess its effectiveness, identify weaknesses, and address potential deficiencies.

**Purpose of Incident Response Testing:**The primary objective of incident response testing is to evaluate the effectiveness of our organization’s incident response capabilities in handling security incidents. Through testing, we aim to identify and address any weaknesses or deficiencies in our incident response procedures and protocols.

**Testing Mechanism:**

1. **Routine Testing:**For every IT and security-related event, as well as physical premises incidents, the organizational incident response procedures are immediately activated and executed. This ensures the incident response mechanism is continuously tested and improved upon.
2. **Permissions Request Testing:**Any permissions request change is also an opportunity to test the incident response mechanism by cycling through its procedures.

**Testing Methods:**Incident response testing encompasses various methods, including:

* Use of checklists to ensure adherence to all necessary steps during incident response.
* Walk-through or tabletop exercises involving scenario discussions and evaluation of incident response strategies.
* Simulations, such as parallel exercises, to simulate incident scenarios without actual interruption, and full interrupt exercises with real-time responses to simulated incidents.
* Comprehensive exercises covering multiple aspects of incident response testing.

**Determining Effects on Organizational Operations:**During incident response testing, we assess the impact of security incidents on our organizational operations, including potential reductions in mission capabilities. We also consider the effects of incident response on organizational assets and individuals.

**Performance Review:**

1. **Quarterly Risk Management Meetings:**During these meetings, there is a thorough review of past incident response actions to gauge the response capability and effectiveness of the organization.
2. **Feedback Loop:**Lessons learned and areas of improvement identified in these meetings are communicated back to the relevant departments for implementation.

**Guidance and Standards:**Our incident response testing aligns with the guidance provided in [SP 800-84], ensuring compliance with testing programs for information technology capabilities.

**Testing Frequency:**Incident response testing is conducted on a regular basis in accordance with our incident response plan and risk management strategies. The frequency of testing is determined based on our risk profile and operational requirements and may occur annually, semi-annually, or at defined intervals.

**Incident Response Improvement:**Findings and lessons learned from incident response testing serve as valuable inputs to enhance our incident response procedures and update the incident response plan. We take corrective actions to address identified weaknesses and deficiencies, improving our incident response capabilities.

**Involvement of Incident Response Teams:**Our dedicated incident response teams actively participate in incident response testing exercises, providing valuable feedback and insights for continuous improvement.

**Annual Testing:**Managers, in collaboration with department heads, conduct an annual test to simulate a likely event that the organization might face. The chosen scenario is briefed to the participants. The test is then executed, and results are compiled and discussed among all participants.

**Responsibilities:**

* **Managers:** Facilitate the annual test, review quarterly performance, and ensure the effectiveness of the incident response mechanism.
* **Department Heads:** Participate in the annual tests and contribute to the review and improvement processes.
* **Incident Response Teams:** Participate in testing exercises and provide feedback for improvement.
* **FSO:** Maintain all test results, documentation, and oversee the implementation of improvements to the incident response procedures.

**Continuous Improvement:**Our organization fosters a culture of continuous improvement, regularly evaluating and enhancing our incident response capability by incorporating best practices and industry standards.

**Approval:**This plan is subject to the approval of the senior management of the organization. Upon approval, it will be communicated to all relevant departments for implementation.

## **Control 3.7.1**

##

**System Security Plan (SSP) – Control Identifier: 3.7.1**

**Control Title: Maintenance of Organizational Systems**

**Control Description:**

This control focuses on ensuring the effective maintenance of organizational systems, including user computers, servers, physical premise security systems, and network components. The organization follows industry best practices to ensure that system maintenance is conducted efficiently and securely. Most maintenance is automated, but manual updates are performed when necessary.

**Implementation:**

1. **Automated Workstation/OS Updates:**
	* Our organization automatically performs updates on user computers as they are released by Microsoft. These updates are scheduled to run on a weekly basis through Lansweeper. This automated process ensures that workstations and operating systems are kept up to date with the latest security patches and improvements.
2. **SonicWall Updates:**
	* SonicWall, a critical component of our network security, is updated through the cloud console. This ensures that our firewall system is continuously updated with the latest threat protections and firmware releases.
3. **Manual Switch Updates:**
	* Network switches are manually updated as required. Although most maintenance is automated, manual intervention is performed when necessary to ensure the reliability and performance of our network infrastructure.
4. **Utilization of Windows Server Update Service (WSUS):**
	* For operating system updates, our organization utilizes a Windows Server Update Service (WSUS) server. This server is used to deploy and verify the installation of operating system updates in accordance with Microsoft best practices. This ensures that all servers in our environment are consistently patched and secure.
5. **Physical Premise Security Systems:**
	* Physical premise security systems, including alarm systems and other security components, are maintained in accordance with best practices and procedures specified by the respective vendors. This includes updating alarm systems as required by the vendor to ensure effective security monitoring.
6. **Endpoint Security:**
	* All endpoints, including user computers and servers, are equipped with antivirus and other endpoint protection mechanisms. These mechanisms are updated periodically through automatic updates and are verified by IT administrators to ensure their effectiveness in safeguarding our systems.

## **Control 3.7.2**

**System Security Plan (SSP) – Control Identifier: 3.7.2**

**Control Title: Controls on System Maintenance Tools and Personnel**

**Control Description:**

This control addresses security-related issues with maintenance tools used for diagnostic and repair actions on organizational systems that process, store, or transmit Controlled Unclassified Information (CUI). It emphasizes the need for controls on tools, techniques, mechanisms, and personnel involved in system maintenance to prevent unauthorized or malicious usage.

**Policy Statement:**

Our organization is committed to implementing controls on the tools, techniques, mechanisms, and personnel involved in system maintenance, with a specific focus on those used for diagnostic and repair actions on systems processing, storing, or transmitting CUI.

**Scope of Controls:**

These controls apply to maintenance tools used for diagnostic and repair actions on organizational systems containing CUI, including both hardware and software tools, techniques, and mechanisms.

**Approving, Controlling, and Monitoring Tools:**

* Maintenance tools are subject to approval, control, and monitoring to prevent unauthorized or malicious usage.
* The organization determines specific controls based on risk assessments and security requirements.

**Security Risks with Maintenance Tools:**

Maintenance tools are recognized as potential vectors for malicious code, either intentionally or unintentionally, into organizational systems. To mitigate these risks and maintain system integrity and confidentiality, controls are established for their secure usage.

**Personnel Access Controls:**

* Access to maintenance tools is limited to authorized personnel possessing the necessary skills and training.
* Access is granted based on job roles and responsibilities and is regularly reviewed and updated.

**Tool Inventory and Accountability:**

* An inventory of maintenance tools, including hardware, software, and firmware items, is maintained.
* Accountability for tool possession and usage is ensured through periodic audits.

**Secure Use of Maintenance Tools:**

* Guidelines and procedures for secure tool usage are established to ensure legitimate diagnostic and repair purposes.
* Controls may include secure storage, physical access restrictions, and logging of tool usage.

**Monitoring and Incident Reporting:**

* Tool usage is continuously monitored for unusual or unauthorized activities.
* Incidents related to tool usage are promptly reported and investigated to prevent further damage.

**Training and Awareness:**

* Authorized personnel receive specific training on proper tool usage and security implications.
* Regular security awareness training emphasizes the risks associated with maintenance tools and responsible tool usage.

**Continuous Improvement:**

* The organization regularly reviews and updates controls on maintenance tools to adapt to evolving threats and technology, ensuring ongoing effectiveness.

## **Control 3.7.3**

##

**System Security Plan (SSP) – Control Identifier: 3.7.3**

**Control Title: Equipment Sanitization for Off-Site Maintenance**

**Control Description:**

Control 3.7.3 focuses on ensuring that equipment containing Controlled Unclassified Information (CUI) is properly sanitized when removed for off-site maintenance. This control addresses the security considerations associated with maintenance activities conducted by local or non-local entities, including contractors, warranty services, or in-house software maintenance agreements. The control requires adherence to guidelines provided in [SP 800-88] for media sanitization.

**Policy Statement:**

Our organization is dedicated to safeguarding Controlled Unclassified Information (CUI) throughout its lifecycle, including during off-site maintenance activities. This System Security Plan (SSP) outlines our commitment to ensuring that all equipment removed for off-site maintenance is appropriately sanitized to prevent unauthorized access or disclosure of CUI.

**Scope of Controls:**

These controls apply to all equipment that may contain CUI and requires off-site maintenance, whether the maintenance is conducted by internal or external parties. Equipment includes but is not limited to servers, workstations, storage devices, and other hardware or software components.

**Sanitization Process:**

To ensure the secure handling of CUI during off-site maintenance, the following process will be followed:

1. **Identification of CUI-Containing Equipment:** All equipment containing or potentially containing CUI must be identified before removal for off-site maintenance.
2. **Data Destruction Policy:** Equipment identified as containing CUI must undergo sanitization following the organization’s Data Destruction Policy. This policy includes methods such as secure wiping or physical destruction.
3. **Sanitization Prior to Removal:** CUI-containing equipment must be sanitized in accordance with the Data Destruction Policy before it is removed from the secure facility. This may involve securely wiping data, removing and retaining storage media, or taking other approved measures to prevent data exposure.
4. **Documentation:** Records of the sanitization process, including dates, methods used, and personnel involved, must be maintained and included in the equipment’s maintenance documentation.

**Off-Site Maintenance Security Measures:**

When CUI-containing equipment is removed for off-site maintenance, the following security measures will be implemented:

1. **Authorization and Waivers:** External maintenance providers, including contractors and warranty services, must be authorized to perform maintenance on equipment containing CUI. They must sign waivers acknowledging their understanding of the presence of CUI and their commitment to not make unauthorized copies or access CUI.
2. **Escorted Access:** Personnel authorized to handle equipment containing CUI during off-site maintenance must be escorted by an organization-approved IT administrator or designated personnel at all times.

**Training and Awareness:**

All employees and authorized personnel involved in the off-site maintenance process will receive training on the organization’s Data Destruction Policy, equipment sanitization procedures, and the handling of CUI during maintenance activities. Regular security awareness training will emphasize the importance of safeguarding CUI during off-site maintenance.

## **Control 3.8.2**

##

**System Security Plan (SSP) for Control of Access to CUI on System Media**

**1. Access Control and Management:**

* Control over access to CUI on system media is managed by the IT department under directives from the administration.
* Program managers are responsible for initiating access requests on behalf of employees who need access for their specific job duties.
* All access requests are approved by the IT department and, when necessary, by the administration.
* For physical media containing CUI, the facilities department is involved.
* A complete record of all access requests is maintained in the IT ticketing system, ensuring full chain of custody for CUI data access.

**2. CUI Training and Authorization:**

* Only personnel who have successfully completed CUI training are permitted to access system media containing CUI.
* CUI data is stored electronically, with strict access controls in place to limit its access only to those who are authorized.

**3. Removable Media Control:**

* Employees wishing to transfer information to removable media must submit a formal request through their immediate supervisor to the COO for consideration.
* Upon approval, only devices procured by the company will be issued for such purposes.
* To facilitate this, the IT administrator forwards a written request detailing the requirement to activate the authorized individual’s USB port. This documentation contains specifics such as the user’s name, the time window for which the USB port will be open, and the date of its deactivation.

**4. Device Management:**

* The Facility Security Officer (FSO) is responsible for issuing these devices and maintaining an inventory control log.
* Once its use is concluded, the device is returned to the FSO. It is then cleansed of all stored data and reset to its factory settings.

All the above procedures and protocols have been successfully implemented to ensure that access to CUI on system media is controlled, monitored, and maintained securely.

## **Control 3.8.3**

##

**Organization’s Data Destruction Policy and Implementation SSP**

**Objective:** Our primary objective was to implement guidelines for data destruction that strictly align with DoD standards, thus ensuring the security, confidentiality, and integrity of CUI throughout the organization.

**Scope:** The policy and its subsequent implementation covered all employees, contractors, and third parties responsible for handling, processing, storing, or disposing of organizational data.

**Implemented Standards for Data Destruction:**

1. **NIST 800-88 Compliance:** All sanitization processes were executed In Accordance With (IAW) NIST 800-88 Guidelines for Media Sanitization. This ensured data was thoroughly sanitized before media disposal or reuse.
2. **Non-Digital Media:** Non-digital media no longer in use was destroyed using a paper shredder, ensuring data was rendered irrecoverable.
3. **Digital Media:** a. All digital media containing sensitive data was appropriately erased. b. Outdated devices, post-erasure, were not returned to use. Instead, they were physically destroyed to prevent any potential data breaches. c. CUI data retention on digital devices, particularly laptops, was strictly prohibited.
4. **Laptop Hard Drives:** All laptop hard drives were re-imaged upon the departure of company personnel. This ensured no residual data, especially CUI, remained on the device.

**Post-Implementation Measures & Responsibilities:**

1. **Awareness and Training:** We trained all personnel on the data destruction procedures. Regular training sessions have been scheduled to keep the workforce updated.
2. **Monitoring:** Our IT and Security teams have been actively monitoring the data destruction processes. This includes regular audits, checks, and reviews.
3. **Reporting:** Protocols have been set for immediate reporting of any instances of non-compliance or potential breaches to the IT and Security departments.

**Review:** We have scheduled an annual review of our Data Destruction Policy Implementation to ensure its continued relevance and effectiveness.

## **Control 3.8.4**

**Control 3.8.4: Marking Media Containing CUI**

**Objective:** Our primary aim is to ensure all media containing CUI are properly marked, handled, and controlled to prevent unauthorized access, distribution, or compromise.

**Scope:** This policy applies to all employees, contractors, and third parties who may come into contact with or handle media containing CUI within the organization.

**Definition of System Media:** System media encompasses both digital and non-digital platforms used for the storage, processing, or transmission of CUI. This includes digital files, paper documents, microfilm, and any other medium where CUI might be found.

**Implemented Measures and CUI Marking Guidance:**

* We strictly follow the government-provided CUI marking guidelines.
* Portable storage media containing CUI are identified with a “CUI Notice” sticker.
* Filing cabinets housing CUI are marked “Contains CUI” using designated stickers.
* Systems housing CUI exhibit interactive logon messages at login, informing users of the CUI’s security and privacy norms.
* We’ve activated specialized email filters that pinpoint, notify, and label emails potentially containing CUI within our secure system.

**Security Marking Requirements:** Security marking incorporates human-readable security attributes on system media, signaling the sensitivity and management requirements of the information. By marking system media correctly, personnel recognize the protection degree required for the CUI inside.

**CUI Markings and Distribution Limitations:** Media with CUI are adorned with suitable CUI labels and distribution restrictions according to guidance in [32 CFR 2002] and [NARA CUI]. These markings categorize the information based on sensitivity and clarify any access and distribution limitations.

**Compliance with Federal Guidelines:** Our commitment is in line with the marking guidance stipulated in [NARA MARK], guaranteeing conformity with federal rules and regulations regarding CUI management. Adherence to these guidelines is paramount to maintain a standardized and potent CUI protection approach.

**Training and Awareness:** Personnel handling system media undergo rigorous training on correct CUI markings and distribution limitations application. This training accentuates the importance of sticking to marking guidelines to effectively safeguard sensitive data.

**Incident Reporting and Response:** Should any incidents related to CUI improper marking or distribution arise, we adhere to a proactive incident reporting and resolution procedure. Quick reporting and rectification of such incidents curtail potential threats and ensure the implementation of corrective measures.

**Continuous Improvement:** Reflecting our commitment, we periodically reassess and enhance our marking procedures to coincide with federal guideline updates and industry best practices. This recurrent initiative assures our marking system media approach remains current and robust in securing CUI.

**Policy Statement:** Our organization is unwavering in its dedication to the appropriate handling and safeguarding of Controlled Unclassified Information (CUI). We’ve put into action a thorough policy for the marking of system media that houses CUI with the requisite security attributes and distribution constraints. This policy is in sync with pertinent federal laws, Executive Orders, policies, directives, and regulations, preserving the confidentiality and integrity of CUI.

## **Control 3.8.5**

##

**Transportation and Control of Controlled Unclassified Information (CUI)**

1. **Objective:**To ensure the secure handling, transportation, and management of CUI data within and outside company-controlled areas, in alignment with company security policies to protect sensitive information.
2. **Scope:**This protocol covers all employees who access CUI data and the stipulations governing its transport.
3. **Authorization:**a. Only select employees, as identified by the Facility Security Officer (FSO), are authorized to transport CUI data outside of company-controlled areas.
b. All employees with access to CUI receive a briefing detailing the requirements for controlling CUI data.
c. CUI data is not removed from designated areas unless the FSO grants explicit authorization.
4. **Data Protection:**a. All electronic CUI data is password protected.
b. Authorization for transport of electronic CUI data must be secured from the FSO prior to transport.
5. **Transportation of Physical Media:**For physical media such as blueprints and technical drawings:
a. A transport log is created prior to the movement of such materials.
b. During transportation, all physical CUI documents are kept in a locked briefcase to ensure maximum security.
c. The transport log captures the following information:
i. Content of the data
ii. Name of the person transporting the data
iii. Duration of the event (how long the data is outside the designated area)
iv. Final disposition of the data (where it ends up and its secured state)
6. **Log Maintenance:**a. The FSO maintains and oversees the transport log.
b. The log is electronically maintained and stored within the FSO’s designated corporate files.
c. Access to this log is limited to authorized personnel, providing an extra layer of security for the movement records of CUI data.
7. **Breaches & Non-Compliance:**Any violations of this protocol are considered serious security breaches and are subjected to appropriate disciplinary actions.
8. **Review & Updates:**This protocol is reviewed annually by the FSO and the security team to ensure its effectiveness and to incorporate any updates in regulations or company policies.

## **Control 3.8.6**

##

**Control Title:** Protection of CUI during Transport

**Control Number:** 3.8.6

**Purpose:** To ensure the confidentiality of CUI stored on digital media during transport and safeguard against unauthorized access.

**Control Description:** The organization protects the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.

**Implementation Details:**

1. **Encryption Protocols:**
	* All digital CUI is encrypted at all times. Specifically, mobile computing platforms use FIPS mode in BitLocker. Wireless connections leverage WPA2 FIPS compliant encryption. VPNs employ 256-bit AES FIPS validated cryptography.
2. **Storage:**
	* Company policy dictates that all CUI data is stored on a secure cloud, with access limited strictly to authorized employees.
3. **Device Restrictions:**
	* All systems have been configured to disallow the use of external devices, effectively preventing direct data transfers to such devices.
4. **Removable Media Protocol:**
	* Employees desiring to transfer information to removable media must formally request authorization from the Change Control Board (CCB).
	* Once authorized, only company-approved USB drives will be provided for use.
	* The Facility Security Officer (FSO) manages the issuance of these devices and maintains a meticulous inventory control log for each.
	* Post-use, devices are to be returned to the FSO, where all data will be erased, restoring the device to its factory state.

**Policy Statement:**Our organization firmly commits to ensuring the confidentiality of Controlled Unclassified Information (CUI) when transported on digital media. By integrating cryptographic mechanisms, we achieve robust protection for sensitive data, especially when alternative physical safeguards aren’t present.

**Scope of Requirement:**The reach of this policy encompasses all portable storage mediums used for CUI storage and transport, including but not limited to USB memory sticks, DVDs, CDs, and external/removable hard drives.

**Cryptographic Protection:**We rely on cryptographic tools to shield the confidentiality of CUI on digital media during its transport. By encrypting the data, the risk posed by potential media loss or theft is significantly reduced, preventing unauthorized data access.

**Alternative Physical Safeguards:**For instances where encryption might not be applicable, alternative physical safeguards take precedence. These methods have been curated to ensure CUI’s integrity and confidentiality during transit.

**Guidance on Cryptographic Mechanisms:**Our organization strictly aligns with the guidance detailed in [NIST CRYPTO]. This alignment ensures our cryptographic choices are in tandem with the industry’s best practices and standards.

**Training and Awareness:**All staff members engaged in the transport of CUI on digital media undergo intensive training. This training focuses on cryptographic tool usage, reinforces the paramount importance of transit data protection, and promotes responsible digital media handling.

## **Control 3.8.7**

**System Security Plan (SSP) for Control 3.8.7**

### **Control the use of removable media on system components.**

**2. Control Description:** This control actively governs the management and use of mobile media within our organization. It reinforces the antivirus measures in place, provides guidelines for different types of portable storage, and ensures the ongoing confidentiality and integrity of Controlled Unclassified Information (CUI).

**3. Purpose:** We’ve established a comprehensive cybersecurity infrastructure that incorporates proactive antivirus protocols, removable media restrictions, and distinct processes for mobile media usage, ensuring the unwavering protection of sensitive data.

**4. Implemented Measures:**

* **Antivirus Measures:**
	+ Any removable media, such as USB sticks inserted into our machines, instantly undergoes an antivirus scan.
	+ Our IT department consistently sanitizes all removable media using a dedicated air-gapped machine equipped with the latest antivirus software.
* **Mobile Media Usage Protocols:**
	+ **Specific Media Restrictions:** Certain removable media types, especially flash drives, face restrictions or are entirely prohibited.
	+ **Physical Measures:** Our workstations are equipped with physical barriers like cages, preventing access to specific external ports, limiting the use of portable storage devices.
	+ **Capability Limitations:** We’ve deactivated or entirely removed the ability to read, write, or insert particular removable media.
	+ **Approved Devices Only:** We permit only organization-sanctioned devices. Personal device use is minimized to deter security risks.
	+ **Writable Device Restrictions:** We’ve controlled writing to portable storage devices, either disabling or removing the capability.
	+ We mandate clearance from our IT department for any removable media usage. Each approved medium bears a CUI sticker, indicating its sanitized status and rightful ownership.
	+ Our company’s cybersecurity policy meticulously documents these processes and media usage records.
* **CCB Oversight and Device Management:**
	+ Our employees must secure approval from the Change Control Board (CCB) to use removable media.
	+ The Facility Security Officer (FSO) is actively managing the issuance of organization-approved USB drives.
	+ Our FSO meticulously maintains an inventory control log, recording device issuance, return dates, and unique identifiers.
	+ After usage, devices are returned to the FSO, sanitized, and reset.
* **Training and Awareness:**
	+ Our team undergoes regular training sessions on the established policies and procedures. This reinforces understanding and emphasizes the importance of security risks.

## **Control 3.8.8**

**System Security Plan (SSP) for Control 3.8.8
Prohibition of Unidentifiable Portable Storage Devices**

**1. Control Overview:**Control 3.8.8 is dedicated to prohibiting the use of portable storage devices that lack identifiable ownership. Such a measure is crucial for preventing unauthorized data transfer, mitigating potential security risks, and ensuring the confidentiality and integrity of our systems.

**2. Purpose:**To establish a stringent security boundary by disallowing the use of unmarked or unidentified portable storage devices within our infrastructure.

**3. Implementation:**

**3.1 Device Identification:**All organization-issued portable storage devices are distinctly marked or labeled, indicating both organizational ownership and the user assigned, if applicable.

**3.2 Strict Prohibition:**No employee or affiliated individual is permitted to insert or use unmarked or personal portable storage devices on the company’s systems or devices.

**3.3 Unidentified Device Protocol:**Upon discovery of any unidentifiable portable storage device within our premises, it should be immediately handed to the IT department. The IT department is then responsible for its secure and immediate destruction to avert potential security risks.

**3.4 Device Management:**

* The Facility Security Officer (FSO) exclusively oversees the issuance of organization-approved portable storage devices.
* An inventory control log, managed by the FSO, tracks device issuance, return dates, and unique identifiers.
* Post-usage, all devices are returned to the FSO for sanitation and a reset to a factory state.

**3.5 Personal Device Policy:**Only organization-procured and issued portable storage devices are permitted for use, thereby entirely disallowing personal devices.

**4. Training and Awareness:**Employees undergo regular training sessions concerning this control, ensuring comprehensive understanding and compliance. The emphasis is on the potential security risks associated with unidentifiable devices.

**5. Monitoring and Review:**This control will be evaluated and reviewed annually by the IT and cybersecurity teams to confirm its continued relevance and effectiveness against emerging threats.

Document Approved by:
[Name, Title, Date]

## **Control 3.8.9**

**System Security Plan (SSP) for Data Backup and Encryption**

**1. Control Identifier:** 3.8.9

This control is implemented. All cloud-based digital CUI is read-protected, allowing access only to those who are authorized on a need to know basis.

**2. Purpose:**To ensure the confidentiality, integrity, and availability of all backup data, particularly containing Controlled Unclassified Information (CUI), by using secure, compliant, and encrypted backup methods and practices.

**3. Control Description:**Our organization has adopted strict measures to guarantee that backup data, particularly CUI, remains protected at all times. This encompasses encryption during transit and at rest, naming conventions that obscure the nature of the content, and stringent access controls.

**4. Implemented Measures:**

**4.1 Secure Backup Processes:**

* All data is backed up via secure, compliant methods, ensuring data availability and integrity.
* Backup data, including system and user-level information, is stored in alternative physical locations to provide redundancy and protection against localized incidents.

**4.2 Encryption Measures:**

* All backup data is fully encrypted during both transit and storage phases.
* Encryption methods adhere to industry best practices and utilize private key encryption, ensuring the highest level of security.

**4.3 Naming Conventions:**

* We employ non-specific naming conventions for backup files to obfuscate the content and purpose of the backups.
* This approach ensures that names like “super secret department of defense project backup” are avoided.

**4.4 Access Control:**

* All backup data is password protected, ensuring that unauthorized access is prevented.
* All cloud-based digital CUI backups are read-protected and limited to individuals who have a justified need for access.

**4.5 Cryptographic and Physical Security:**

* Cryptographic mechanisms are in place for backup information at designated storage locations.
* In situations where cryptographic solutions might not be feasible, alternative physical controls are employed to secure backup data.

**4.6 Data Types in Backup:**Backup data encompasses:

* **System-level information:** System state, operating system software, application software, licenses.
* **User-level information:** All data other than the system-level information, ensuring comprehensive backup of all necessary data.

**5. Policy Review:**This SSP will be reviewed annually or as deemed necessary by the organization’s management. Feedback from IT and cybersecurity teams will inform updates to ensure compliance and optimal security.

## **Control 3.9.1**

##

**System Security Plan (SSP) – Control Identifier: 3.9.1**

**Control Title:** Personnel Security Screening for CUI Access

**Control Description:** All employees must undergo personnel security screening, including federal background checks, prior to being granted access to organizational systems containing Controlled Unclassified Information (CUI). Additional screening takes place during our interview process to further assess the individual’s conduct, integrity, judgment, loyalty, reliability, and stability to determine their trustworthiness for accessing CUI.

**Implementation:**

1. **Personnel Screening Process:**
	* All prospective employees must undergo a thorough personnel security screening process before being considered for access to CUI.
	* The screening process, which includes federal background checks, evaluates various factors, including conduct, integrity, judgment, loyalty, reliability, and stability, in accordance with applicable federal laws, Executive Orders, directives, policies, and regulations.
2. **Access Determination:**
	* Only individuals who have successfully passed the personnel security screening, including federal background checks, will be considered for access to organizational systems containing CUI.
	* The level of access granted will align with the specific criteria established for their assigned positions and the requirements of the CUI they will be handling.
3. **Mandatory Training:**
	* Individuals granted access to CUI are required to undergo the following mandatory training:
		+ Information Technology (IT) and Cybersecurity Policy Training.
		+ Department of Defense (DoD) CUI Training.
		+ Other applicable training, such as insider threat awareness and anti-phishing training.
		+ Job-specific training as relevant to their assigned duties.
4. **Continuous Monitoring:**
	* Individuals with access to CUI will be subject to continuous monitoring to ensure their ongoing trustworthiness and adherence to security policies and practices.
	* Any deviations or concerns regarding an individual’s trustworthiness will be promptly addressed through appropriate security measures.

## **Control 3.9.2**

##

**System Security Plan (SSP) – Control 3.9.2**

**Control Identifier:** 3.9.2

**Control Title:** Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.

**Control Description:** This control focuses on safeguarding Controlled Unclassified Information (CUI) during and after personnel actions such as terminations and transfers. The organization ensures that thorough out-processing steps are taken to prevent departing employees from having unauthorized access to CUI. This includes HR notifications, disabling system accounts, collecting system-related property, conducting exit interviews, and updating security systems as necessary.

**Current Implementation:**

* The organization has established a comprehensive process for protecting CUI during and after personnel actions. The process involves collaboration between various departments, including HR, Facility Security Officer (FSO), Equipment Custodian, and other company representatives.
* Key aspects of the current implementation include HR notifications, immediate termination of system access, password resets, updating physical security systems, and escorting departing employees out of the building.
* All access, including computer systems and physical building access, is promptly removed upon personnel actions, such as terminations. Departing employees are escorted out of the building, and personal items are collected by security officers and managers.
* Notably, departing individuals are not permitted to clean out their computer systems, mobile devices, or offices. All these tasks are carried out by authorized staff members to ensure the security and integrity of CUI.
* The procedures and policies governing these actions are documented in the organization’s Employee Handbook, ensuring that all employees are aware of the strict security protocols in place during personnel actions.

**Protection of CUI During Personnel Actions:**

* The organization recognizes the importance of protecting CUI during personnel actions, including terminations and transfers. This includes returning system-related property, conducting exit interviews, and reminding departing individuals of nondisclosure agreements.

##

## **Control 3.10.1**

**System Security Plan (SSP) for Control 3.10.3**

**Title**: Visitor Management, Escort Protocol, and Incident Reporting

**Purpose**: To ensure the security and integrity of the facility by strictly monitoring and controlling the movements and activities of visitors within the premises.

**Implementation Details**:

1. **Visitor Registration and Identification**:
	* All visitors are required to register their presence upon arrival at the facility.
	* Identification verification is a must to confirm the visitor’s identity and establish the purpose of their visit.
2. **Visitor Logging**:
	* Upon registration, visitors are also required to sign a designated logbook.
	* The logbook captures details like the visitor’s full name, organization (if applicable), purpose of visit, and contact details.
	* The system further provides:
		+ Proper visitor identification
		+ U.S. person status verification (if applicable)
		+ Entry and exit time stamping
3. **Visitor Access Restrictions**:
	* Visitor access is strictly limited based on the purpose of their visit.
	* The principle of need-to-know governs access restrictions, ensuring visitors only access areas pertinent to their stated purpose.
4. **Escort Protocol**:
	* All visitors are required to be escorted during their entire time in the facility.
	* Trained personnel are designated for this task to ensure adherence to access restrictions and security protocols.
	* Every visitor is assigned a single point of contact or person for their visit’s duration.
5. **Visitor Badge**:
	* Visitors are provided with badges that detail both their name and their escort’s name.
	* This ensures visitors can be immediately questioned if found unaccompanied.
6. **Training and Awareness**:
	* Personnel responsible for escorting and monitoring visitors undergo rigorous training on proper procedures and protocols.
	* This training ensures all security protocols are understood and followed meticulously.
7. **Incident Reporting and Response**:
	* Any security concerns stemming from visitor activities are to be promptly reported.
	* The organization has a set incident response procedure in place to address and rectify any such issues.

## **Control 3.10.2**

##

**Control 3.10.2 System Security Plan (SSP)**

**Title**: Protect and Monitor Physical Facilities and Support Infrastructures

**Purpose**: To ensure the safety and security of organizational systems, equipment, and assets, by guarding against unauthorized access, damage, and theft.

**Implementation Details**:

1. **Alarm System**:
	* The building is equipped with a alarm system.
	* Monitored 24/7 by ADT to immediately respond to any alerts or breaches.
2. **IT Infrastructure**:
	* The IT closet, which houses critical organizational systems, is locked at all times to prevent unauthorized access.
3. **Monitoring**:
	* Camera Systems: Integrated camera systems have been installed throughout the facility.
4. **Protection**:
	* Access Control: Advanced door access systems have been set up, requiring key fobs or codes for entry, ensuring only authorized personnel can access restricted areas.
	* Personnel Training: Employees are trained to recognize and report any suspicious activities or individuals. This training promotes a culture of awareness and vigilance, reinforcing the “if you see something, say something” mantra.
5. **Support Infrastructure**:
	* Besides the IT closets, the facility also has power generators, power meters, and other infrastructure essentials. These too are safeguarded against unauthorized access or tampering.
6. **Additional Measures**:
	* Fire Safety: The building is equipped with a comprehensive fire alarm and safety system.
	* Security Personnel: Trained security personnel monitor and guard the facility. If a location doesn’t have dedicated security staff, the existing personnel are trained with basic security measures.
	* Personnel Awareness Training: Regular training sessions are conducted to keep staff updated about security protocols and to foster a proactive security culture.
	* Monitoring Systems: The facility employs a closed-loop camera system, along with the alarm and fire system. These tools work in conjunction with trained personnel to offer robust protection.

## **Control 3.10.3**

**System Security Plan: Escorting Visitors and Monitoring Visitor Activity**

1. **Policy Statement**: The organization employs procedures to escort visitors and monitor their activity within the facility. Individuals with permanent physical access authorization credentials are exempt from visitor status. The organization uses audit logs to monitor visitor activity to ensure security and accountability.
2. **Visitor Escort Procedures**:
3. Visitors are escorted while within the facility to ensure they are accompanied by authorized personnel at all times.
4. **Exemption for Authorized Personnel**:
5. Individuals with permanent physical access authorization credentials, who are not considered visitors, are allowed unrestricted access to designated areas.
6. **Monitoring Visitor Activity**:
7. Visitor activity within the facility is monitored to track their movements and actions while on-site.
8. **Use of Audit Logs**:
9. Audit logs are utilized to record and track visitor activities, providing a comprehensive record for security and accountability purposes.
10. **Visitor Registration and Identification**:
11. Visitors are required to register their presence at the facility and provide identification to verify their identity and purpose of visit.
12. **Visitor Access Restrictions**:
13. Visitor access is limited to specific areas based on the purpose of their visit and the need-to-know principle.
14. **Training and Awareness**:
15. Personnel responsible for escorting visitors and monitoring their activities receive training on proper procedures and protocols.
16. **Incident Reporting and Response**:
17. Any incidents related to visitor activities that raise security concerns are promptly reported and addressed through the organization’s incident response procedures.
18. **Continuous Improvement**:
19. The organization periodically reviews and enhances its visitor escort and monitoring procedures to adapt to changing security needs and improve overall effectiveness.

## **Control 3.10.4**

###

### **System Security Plan (SSP) for Control 3.10.4**

### Maintain audit logs of physical access

**Purpose**: To maintain comprehensive audit logs of physical access to the facility and ensure security through systematic monitoring, timely reporting, and continuous enhancement of protocols.

**Implementation Details**:

1. **Visitor Management**:
	* All visitors are required to register their presence in a designated logbook upon entering the facility.
	* Visitors are continuously escorted throughout their stay in the building, ensuring adherence to security protocols.
2. **Employee Access Monitoring**:
	* All employees are issued unique key fobs, facilitating the electronic tracking of their entries and exits from the building.
	* These fobs ensure that only authorized personnel gain access to the premises.
3. **Video Surveillance**:
	* Video cameras are strategically placed to capture and record activities within the facility, acting as an additional layer of security and monitoring.
4. **Coverage of Physical Access Points**:
	* Comprehensive audit logs are kept for all physical access points, both external and internal.
	* This includes key facility entry and exit points, as well as specific areas housing critical system components.
5. **Monitoring Publicly Accessible Areas**:
	* System components placed in publicly accessible areas, such as workstations and notebook computers, are also audited.
	* Strict access controls are implemented to safeguard these components.
6. **Training and Awareness**:
	* Dedicated personnel assigned the duty of maintaining and reviewing audit logs undergo systematic training.
	* This ensures they are equipped with the latest procedures and protocols for access record management.
7. **Retention and Protection of Audit Logs**:
	* Audit logs are retained in accordance with the organization’s established policies.
8. **Incident Reporting and Response**:
	* Incidents highlighting unauthorized physical access or any security concerns originating from the audit logs are immediately reported.
	* These concerns are swiftly addressed following the organization’s incident response procedures.
9. **Continuous Improvement**:
	* Periodic reviews of the audit log management procedures are carried out.

## **Control 3.10.5**

##

**System Security Plan (SSP) for Control 3.10.5**

**Title**: Control and Management of Physical Access Devices

**Purpose**: To ensure the integrity, confidentiality, and availability of the organization’s physical resources by implementing strict controls and management measures for physical access devices.

**Policy Statement**: The organization is committed to maintaining robust controls over physical access devices, including but not limited to keys, locks, combinations, and card readers. These devices safeguard the organization’s assets and prevent unauthorized access to sensitive areas.

**1. Inventory and Tracking**:

* **Description**: All physical access devices are logged and tracked. This inventory assists in maintaining a clear record of all devices, their locations, and authorized users.
* **Implementation**: A centralized inventory system, managed by the Facility Security Officer (FSO), logs all physical access devices, their associated access points, and designated users.

**2. Issuance and Authorization**:

* **Description**: Physical access devices are issued following strict authorization procedures.
* **Implementation**: Human Resources (HR) provides directives on personnel authorized to receive physical access devices, which the FSO implements.

**3. Key Management**:

* **Description**: A comprehensive key management system ensures keys’ secure storage, issuance, and duplication prevention.
* **Implementation**: Keys are stored in a secured key cabinet. Their issuance and return are logged. Duplication is strictly prohibited without the FSO’s authorization.

**4. Locks and Combinations**:

* **Description**: Locks and combination systems are essential components of the physical security framework.
* **Implementation**: Regular inspections ensure their operational effectiveness. Combinations are changed periodically and after any security incidents.

**5. Card Reader Access**:

* **Description**: Electronic access controls, like card readers, provide enhanced security measures.
* **Implementation**: Access logs from card readers are periodically reviewed. Unauthorized access attempts trigger alerts to the security team.

**6. Monitoring and Auditing**:

* **Description**: Monitoring ensures that physical access devices function as intended and that anomalies are detected promptly.
* **Implementation**: Routine audits, spearheaded by the Audit Team, analyze access logs, device conditions, and user behaviors to identify potential security risks.

**7. Replacement and Decommissioning**:

* **Description**: The life cycle of physical access devices is managed to ensure security at all stages.
* **Implementation**: Lost, compromised, or outdated devices are promptly reported to the FSO and replaced. Decommissioned devices undergo secure disposal procedures.

**8. Training and Awareness**:

* **Description**: Continuous training ensures that all personnel are aware of their roles and responsibilities concerning physical access devices.
* **Implementation**: Regular training sessions, led by the Training Coordinator, cover device usage, security protocols, and incident reporting procedures.

**9. Incident Reporting and Response**:

* **Description**: Rapid response to incidents prevents potential security breaches.
* **Implementation**: Incidents related to physical access devices are reported to the Incident Response Team, which follows established response protocols to address and mitigate risks.

**10. Continuous Improvement**:

* **Description**: The organization is committed to adapting and enhancing its security measures over time.
* **Implementation**: Feedback loops, periodic reviews, and security assessments ensure that the control and management of physical access devices evolve with changing security landscapes.

## **Control 3.10.6**

**System Security Plan: Safeguarding CUI at Alternate Work Sites and During Transit**

**Policy Statement:**Our company is unwavering in its commitment to the integrity, confidentiality, and availability of Controlled Unclassified Information (CUI) regardless of its location, be it at an alternate work site, in transit, or at home.

**Implementation Details:**

**1. Identification of Alternate Work Sites:**We have mapped out all alternate work sites, including private residences, temporary setups at partner facilities, or transit locations, where CUI is accessed or managed.

**2. Risk Assessment for Each Site:**We conduct a comprehensive risk assessment for every alternate work site to address the unique challenges and risks pertinent to different environments.

**3. Safeguarding Measures Enforced:**

* **Blueprints at Construction Sites:**
	+ We ensure secure storage in lockable containers when not in active use.
	+ Access is strictly confined to authorized personnel.
	+ Electronic versions are accessed strictly through our encrypted devices.
* **Traveling Employees with CUI:**
	+ Documents are always securely stored in our approved locked containers/bags.
	+ All electronic data is encrypted and necessitates multi-factor authentication for access.
	+ Our employees are well-trained to circumvent accessing CUI in public settings.
* **Home-Based Safeguards:**
	+ We mandate a dedicated and secure network connection for all work-related activities. Secondary backup connections are established where feasible.
	+ All CUI data transmissions utilize our encrypted channels.
	+ Our devices accessing CUI receive regular software and security updates.
	+ We’ve disseminated guidelines to ensure physical security at homes, which include lockable storage solutions and privacy protocols.
	+ Our clear desk policy and screen-locking procedures are non-negotiable, minimizing any exposure risks.

**4. Training and Awareness Programs:**Our continual training modules focus on safeguarding CUI and underscore unique scenarios such as home-based work, traveling with CUI materials, and challenges at construction sites.

**5. Continuous Monitoring:**We actively monitor for compliance and promptly detect any anomalies, irrespective of the work site.

**6. Teleworking Protocols:**By adopting the guidelines from [SP 800-46] and [SP 800-114], we ensure that our teleworking protocols address the multifaceted challenges of various environments.

**7. Incident Response:**Our tailored response plans are ever-ready to tackle potential security breaches at any location, ensuring immediate action and mitigation.

**8. Physical Security Protocols:**Our guidelines span a variety of setups, from ensuring the sanctity of CUI at homes to its security at construction sites.

**9. Clear Desk & Screen Protocols:**We actively enforce best practices to curtail exposure risks, no matter the working environment.

**10. Regular Policy Reviews:**We periodically revisit our SSP, adjusting for evolving scenarios and integrating new best practices.

## **Control 3.11.1**

**System Security Plan (SSP) – Risk Assessment and Management**

**1. Introduction:**

This SSP details the steps and protocols our organization has put in place to periodically assess the risk to our operations, assets, and individuals. This stems from the operation of our system and the associated processing, storage, or transmission of CUI (Controlled Unclassified Information).

**2. Periodic Risk Assessment:**

* **Frequency**: Quarterly risk management meetings are held.
* **Scope**: All facets of organizational risk are evaluated, which includes operations, mission, functions, reputation, assets, and associated individuals.
* **Procedure**: The exact methodologies employed during these meetings are outlined in our ‘Standard Operating Procedure for Risk Management’. [Attachment: **SOP RISK standard operating procedure document**]
* **Outcome**: Risks are consistently reviewed, evaluated, and adjusted as needed, with the ultimate goal of proactively managing and minimizing threats throughout the organization.

**3. Annual Review:**

* **Frequency**: An annual review of the Cybersecurity & CUI Plan and this System Security Plan is conducted.
* **Participants**: Spearheaded by our COO, FSO, and department heads.
* **Agenda**: This review critically evaluates potential risks and our incident response strategies. Changes in mission, assets, people, or systems that could compromise the secure management of CUI are discussed in detail.
* **Outcome**: Necessary modifications are made to the Cybersecurity & CUI Plan and this SSP to maintain alignment with NIST SP 800-171 and other relevant government regulations.

**4. System Boundaries:**

* **Definition**: Our organization emphasizes the clear delineation of system boundaries to conduct efficient risk assessments.
* **Scope**: Risks associated with threats, vulnerabilities, likelihood, and impact to our operations, assets, and individuals are assessed. This encompasses risks from external parties such as service providers, contractors, and entities we outsource to.
* **Levels of Assessment**: Be it formal or informal; risk assessments are conducted at different tiers: organization-wide, mission/business process-focused, or system-centric. These can be initiated at any juncture of the system development life cycle.
* **Guidance**: Our protocols are in alignment with the [SP 800-30] guidelines for conducting risk assessments.

## **Control 3.11.2**

**System Security Plan (SSP) for Control 3.11.2**

1. **Purpose**: To establish a robust procedure to identify, assess, and manage vulnerabilities within the organization using top-tier software available within the Microsoft GCC High and Azure ecosystems.
2. **Scope**: This plan encompasses all organizational systems and components, such as network devices, software applications, databases, and connected infrastructure.
3. **Responsibilities**:
	* **IT Department**: We conduct routine vulnerability scans using Azure Security Center and ensure we implement the necessary patches.
	* **Security Team**: We monitor vulnerability databases within Microsoft GCC High and ensure our scanning tools are current.
	* **Department Heads**: Ensure compliance with this SSP in their respective domains.
4. **Vulnerability Scanning Procedures**:
	* **Endpoint Management**: We utilize Microsoft Defender for Endpoint integrated within GCC High for continuous vulnerability scans.
	* **Firewall Management**: We use Azure Firewall for continuous scanning of incoming and outgoing traffic.
	* **SIEM/SOAR Solutions**: Azure Sentinel serves as our go-to solution for identifying and alerting on detected vulnerabilities.
5. **Additional Scanning Considerations**:
	* **Custom Software**: For in-house applications, we use Azure DevOps for static, dynamic, binary analysis, and source code reviews.
	* **SCAP-Validation**: Within Microsoft GCC High, we utilize built-in SCAP tools that employ the OVAL and express vulnerabilities in the CVE naming convention.
	* **Vulnerability Information Sources**: We routinely review the CWE listing and the National Vulnerability Database (NVD) using Azure Policy.
6. **Vulnerability Scanning Depth**:
	* **Patch Levels**: With the help of Azure Update Management, we ensure our systems are current and patched.
	* **Unnecessary Functions**: We use Azure Network Watcher to scrutinize for unnecessary ports, protocols, services, and functions.
	* **Flow Control Mechanisms**: We leverage Azure Firewall Policies to verify our data flow controls are properly operational.
7. **Advanced Vulnerability Assessments**:
	* **Red Team Exercises**: We sporadically employ red team exercises using Azure Red Team Tool.
	* **CVSS**: We utilize Azure Security Benchmark to gauge the impact of identified vulnerabilities using the Common Vulnerability Scoring System.
8. **Privileged Access**: For certain situations demanding in-depth vulnerability scanning or involving highly confidential data, we grant elevated access to selected system components, ensuring thorough scanning while safeguarding the data’s confidentiality.
9. **Documentation & Reporting**:
	* We document all discoveries, patches applied, and open vulnerabilities using Azure Security Center.
	* We craft monthly reports for the leadership, detailing vulnerability status, trends, and tasks using Azure Monitor Logs.
10. **Continuous Improvement**: This SSP is reviewed and updated annually or when there are significant changes to our organization’s infrastructure, software, or relevant regulations.

## **Control 3.11.3**

##

**System Security Plan (SSP) for Control 3.11.3**

### Title: Remediation of Vulnerabilities in Accordance with Risk Assessments

1. **Purpose:**
	* This SSP ensures that we appropriately address vulnerabilities identified within the organization based on their assessed risk. By following this plan, we ensure the security of our digital assets, maintain the confidentiality of our customer data, and protect our brand reputation.
2. **Scope:**
	* The plan encompasses all organizational systems, applications, databases, network devices, and related infrastructures susceptible to vulnerabilities.
3. **Responsibilities:**
	* **IT Department:** We execute regular vulnerability scans and work closely with the security team during incident responses.
	* **Internal Risk Management Team:** We conduct risk assessments quarterly, provide risk scoring for identified vulnerabilities, and suggest remediation prioritization.
	* **Security Team:** We activate the incident response plan when vulnerabilities are detected, oversee remediation efforts, and ensure policy adherence.
	* **Department Heads:** We ensure compliance with remediation directives and that department-specific applications or systems are available for scanning.
4. **Vulnerability Management Procedures:**
	* **Periodic Scanning:** We utilize vulnerability scanning tools to detect potential security weaknesses in organizational assets.
	* **Incident Response:** When we detect a vulnerability, we invoke the Incident Response Plan to address the issue swiftly and effectively.
	* **Risk Assessments:** We conduct risk assessments quarterly, considering factors like potential business impact, likelihood of exploitation, and data sensitivity.
5. **Plan of Action (PoA):**
	* When identifying vulnerabilities, we formulate a PoA that outlines the remediation steps, required resources, and targeted completion dates.
	* **Milestones:** We define milestones within the PoA to ensure trackable remediation activities and accomplish them within stipulated time frames.
6. **Remediation:**
	* We prioritize remediation efforts based on risk scores derived from assessments.
	* While we aim to remediate all vulnerabilities, we focus on those posing the highest risk to the organization.
7. **Review and Update:**
	* We review this SSP annually or after any significant infrastructural or procedural changes to ensure its continued relevance and effectiveness.
8. **Documentation:**
	* We document all risk assessment findings, remediation activities, and PoA milestones for transparency and future reference.
9. **Continuous Improvement:**
	* We encourage feedback from all departments and regularly update the SSP to align with the evolving threat landscape and business requirements.
10. **Training:**
* We ensure that all staff, especially those in IT and Security, undergo regular training on vulnerability management and remediation processes.

## **Control 3.12.1**

**Cybersecurity & CUI System Security Plan (SSP) – Control 3.12.1 – Assess Security Controls to Determine Effectiveness**

**1. Introduction**

This SSP was established to present an organized approach to assess the effectiveness of security controls under the Cybersecurity & CUI Plan in line with Control 3.12.1. The document underscored the importance of proactive security measures and continuous improvement in the face of ever-evolving cyber threats.

**2. Change Control Board (CCB)**

A CCB board has been put in place with the critical responsibilities of:

* Conducting annual reviews to assess the effectiveness of all security controls.
* Implementing new controls based on the findings of the reviews.
* Updating the SSP as necessary to reflect changes in controls and security procedures.

**3. Quarterly Risk Management Meetings**

Implementation of Control 3.12.1 was realized through quarterly risk management meetings. During these sessions:

* Security controls were thoroughly reviewed.
* Root Cause Analyses (RCAs) were carried out to pinpoint the core issues behind security lapses or breaches.
* The organization deliberated on whether the security controls in place were effective or if there were superior alternatives that should have been adopted.

**4. Incident Response Plan & Procedures**

As part of the broader risk management strategy, and especially during the quarterly risk management meetings:

* The organization consistently aimed to refine its security posture.
* Emerging cybersecurity threats were acknowledged and addressed.
* Staying abreast of the dynamic nature of security threats was deemed crucial, as the threats faced then differed from those encountered previously.

**5. Expert-Run Risk Management Meetings**

In a commitment to uphold high security standards:

* Expert-led risk management meetings were organized.
* These meetings, helmed by seasoned professionals, ensured a comprehensive analysis of current risks and the formulation of effective strategies.

## **Control 3.12.2**

**Control 3.12.2 – Develop and Implement Plans of Action**

**Introduction:**In alignment with the guidelines set forth by the NIST 800-171 and CMMC protocols, our company has proactively written and established a System Security Plan (SSP). Furthermore, we’ve initiated a Plan of Action and Milestones (POA&M) to ensure that any potential discrepancies are effectively addressed. This document outlines the strategies, practices, and management framework for Control 3.12.2.

**Scope:**Our procedures span the entirety of our organization, capturing all areas where potential discrepancies in security controls may manifest. Whenever such discrepancies arise, the creation and implementation of remedial plans of action and milestones are mandated.

**Procedure:**

1. **Identification of Discrepancies:**Discrepancies are consistently identified during our periodic SSP reviews and evaluations performed by independent auditors.
2. **Development of POA&M:**Any identified discrepancy triggers the creation of a Plan of Action and Milestones (POA&M). This plan methodically details:
	* The nature of the recognized discrepancy.
	* The proposed corrective action.
	* The projected timeline for its resolution.
	* The individual or department responsible for its completion.
3. **Oversight and Meetings:**Emphasizing our commitment to robust cybersecurity practices, our Chief Operating Officer (COO) holds regular meetings with the relevant staff members. These sessions:
	* Monitor progress against the POA&M.
	* Address any emerging challenges.
	* If necessary, adjust action plans or timelines to better match the evolving landscape.
4. **Tracking and Logging via Ticketing System:**A ticketing system is in place to ensure efficient and systematic tracking of all identified discrepancies. Each discrepancy ticket provides:
	* A clear description of the discrepancy.
	* The party responsible for its resolution.
	* The prescribed corrective measure.
	* The estimated date of completion.
5. Additionally, this ticketing system provides automated notifications, facilitates follow-ups, and possesses robust reporting capabilities to bolster our oversight and future audit activities.
6. **Roles and Responsibilities:**Our Facility Security Officer (FSO) plays a pivotal role, overseeing the internal SSP reviews, managing corrections as dictated by the POA&M, and liaising with independent auditors when reviews are necessary.

## **Control 3.14.1**

* + **Policy Statement:**Our organization commits to the diligent identification, reporting, and correction of system flaws. We understand that safeguarding Controlled Unclassified Information (CUI) demands prompt action and adherence to best practices, as defined by our Service Level Agreement (SLA) and guidance from industry standards.

	**Implementation Details:
	Implementation Details:
	1. SLA for Remediation Efforts:**Any system flaw which may affect CUI will have a service level agreement of 60 minutes or less to initiate remediation efforts.
	**2. Identification of System Flaws:**
		- **Procedure:** System flaws are determined within the specified timeframe through our proactive monitoring processes.
		- **Implementation:** During information intake, IT ticket creation is triggered in our IT ticketing system. This ensures that flaws are logged and queued for immediate attention.
	+ **3. Reporting of System Flaws:**
		- **Procedure:** A specified timeframe is set for reporting system flaws to ensure timely resolution.
		- **Implementation:** Our Incident Response Plan dictates the mechanisms and timelines for flaw reporting. The IT service ticket system facilitates the reporting process, and the ticket review audit process, in conjunction with the risk management standard operating procedure, ensures compliance with reporting timelines.
	+ **4. Correction of System Flaws:**
		- **Procedure:** Identified system flaws must be corrected within a specified timeframe to reduce vulnerabilities.
		- **Implementation:** The IT service ticketing system, the ticket review audit process, and the risk management SOP oversee and guide the flaw correction process. Each of these mechanisms ensures that flaws are addressed promptly and according to organizational standards. **5. Security-Relevant Updates:**
	+ We prioritize and apply security-relevant updates like patches, service packs, hot fixes, and anti-virus signatures promptly.
	+ Such updates are vital for addressing known vulnerabilities and deterring potential exploitation.
* **6. Flaw Correction Process:**
	+ Our organization swiftly addresses and rectifies flaws detected during security assessments, continuous monitoring, incident response activities, and system error handling.
* **7. Use of Available Resources:**
	+ In rectifying flaws found in our systems, we refer to the Common Weakness Enumeration (CWE) database and Common Vulnerabilities and Exposures (CVE) database.
	+ These databases facilitate comprehension of the flaws’ nature and the suggested remediation steps.
* **8. Organization-Defined Time Periods:**
	+ Timeframes for updating security-relevant software and firmware take into account factors like the update’s urgency and the vulnerability’s severity linked to the discovered flaw.
* **9. Flaw Remediation Testing:**
	+ Our organization undertakes testing to ascertain the efficacy of flaw remediation steps before their comprehensive deployment. This ensures that the implemented solutions don’t cause further disruptions.
* **10. Guidance from [SP 800-40]:**
	+ Our organization aligns with the guidance from [SP 800-40] for efficient and secure patch management, bolstering our defense against vulnerabilities.
* **11. Continuous Improvement:**
	+ Drawing from lessons of incident response activities and security assessments, we are committed to refining our approach to flaw management. This ensures we are aptly fortified against emerging threats.

##

## **Control 3.14.2**

* Organizational System Security Plan (SSP) – Protecting Against Malicious Code
* 1. Introduction:
The main objective of this document is to lay out a clear plan ensuring that the organization remains shielded from malicious code at critical and designated locations within our systems. We integrate several Microsoft Azure products and services into our strategy to provide comprehensive protection against potential threats.
* a. **Primary Measures:**– Managed Endpoint Solution for real-time scanning. ( name of solution here )
– Firewalls to filter and block potential threats. ( name of solution here )
– Advanced Email Protection Solutions for safeguarding against malicious emails. ( name of solution here )
* b. **Definitions:**– Managed Endpoint Solution: Integrated system for managing security across devices, inclusive of antivirus capabilities.
– Firewalls: Systems to regulate network traffic.
– Advanced Email Protection Solution: Detect and deter malicious email content.
* 4. **Continuous Monitoring and Incident Prevention:**Constant surveillance of all designated protection locations to detect potential threats. Monitoring is enhanced by threat intelligence and guidelines from [SP 800-83].
* 5. **Threat Intelligence Integration:**Utilizing our security measures and continuous monitoring, our threat intelligence is incorporated into security operations. This aims to broaden our understanding of potential threats, enabling us to refine our response strategies.
* 6. **Regular Review and Updates:**In light of the ever-evolving cyber threats, our defense mechanisms and tools are consistently assessed and updated. This proactive approach ensures we remain ahead of potential threats.
* 7. **Continuous Improvement:**Driven by feedback from reviews, monitoring, and threat intelligence, we are dedicated to constantly improving our strategies and technologies to effectively combat the changing landscape of malicious code threats.

## **Control 3.14.3**

Organizational System Security Plan (SSP) – Monitoring System Alerts and Advisories

1. **Introduction:**

The primary goal of this document is to outline our organization’s strategy to proactively monitor and respond to system security alerts and advisories, safeguarding our infrastructure from potential threats.

1. **System Integration for Monitoring:**

a. **Our SIEM (Security Information and Event Management):**

Purpose: Acts as the frontline defense by serving as our primary threat sensor. Integration: Regularly captures and processes system security alerts. This system operates in conjunction with our internal Security Operations Center (SOC) which performs analysis, detection, and response functions.

1. **Sources of Security Alerts and Advisories:**

a. **Internal System Alerts:** These are alerts generated from within our system infrastructure, signifying potential security anomalies or risks.

b. **External Advisories:** We maintain subscriptions and liaisons with trusted external agencies, notably CISA, which provide timely warnings and advisories on emerging threats and vulnerabilities.

1. **Response Strategy:**

a. **Internal Notification via Ticketing System:** Once an alert or advisory is detected and verified by our SOC, it’s logged into our ticketing system. This system ensures that relevant stakeholders, including the internal IT department, are immediately notified and can track the response to completion.

b. **Action Response:** The nature and severity of the alert dictate the response. Our Incident Response Plan, integrated with the ticketing system, offers a structured and hierarchical response mechanism ensuring every threat is addressed efficiently and effectively.

c. **External Communication:** For alerts that have wider implications, especially those that might impact our partners or stakeholders, we activate a communication protocol ensuring transparency and collaboration.

## **Control 3.14.4**

##

**Organizational System Security Plan (SSP) – Control 3.14.4: Updating Malicious Code Protection Mechanisms**

**1. Introduction:**

This document articulates our organization’s strategy for ensuring that malicious code protection mechanisms are consistently updated, ensuring the highest degree of protection against potential threats.

**2. Implementation of Malicious Code Protection:**

All our malicious code protection systems are set to automatically update directly from their respective vendors. As soon as new protection definitions and versions are released, they’re instantly applied across our infrastructure.

**3. Integration with Windows Update Service Server:**

Beyond individual malicious code protection mechanisms, we also utilize a Windows Update Service Server. This ensures that all operating system updates are consistently current. Furthermore, any instance of update failure triggers an alert, which ensures we maintain the security of our systems at all times.

**4. IT Administration and Management:**

Our IT administrators play a critical role in this process. They make use of the IT ticketing system to diligently track and update critical system versions. This not only guarantees that updates are applied but also provides a structured record of all updates, ensuring transparency and traceability.

**5. Addressing Custom-built Software:**

We do not operate or maintain any custom-built software. As a result, our malicious code protection mechanisms are tailored to widely recognized software, optimizing their efficiency.

**6. Monitoring Practices:**

We uphold robust monitoring practices, which involve real-time surveillance and analysis of system activity. This ensures immediate detection of unusual behavior or indications of potential malicious threats.

**7. Prompt Update Deployment:**

As part of our commitment to security, whenever new releases or updates for malicious code protection mechanisms become available, these updates are automatically deployed across our infrastructure. This proactive approach ensures that our systems remain fortified with the most recent security defenses.

**8. Continuous Improvement:**

In the ever-evolving realm of cybersecurity, our organization remains dedicated to consistently updating and improving our security mechanisms, ensuring we’re always a step ahead of potential threats.

## **Control 3.14.5**

##

* **Control 3.14.5**
* **Organizational System Security Plan (SSP) – Active Periodic and Real-time Scanning Protocols**
* **1. Introduction:**This document outlines our established practices for conducting systematic scans on our organizational systems, complemented by real-time scans on external files, ensuring continuous threat detection and mitigation.**2. Established Scanning Infrastructure:**a. **Endpoint Protection Solution:**
	+ - Purpose: Our antivirus protection is integrated into our current endpoint protection solution.
* b. **Operational Corporate Firewall:**
	+ - All traffic passing through is scanned in real time, detecting and blocking potential threats promptly.
* **3. Routine Organizational System Scans:**Our systems are scanned daily. This established practice utilizes industry-leading tools, proficient in detecting a myriad of malicious code formats, including those in compressed, hidden, or uniquely concealed files.
**4. Ongoing Real-time Scans of External Source Files:**As part of our operational protocols, every file from external sources is instantly scanned before interaction, safeguarding our systems from potential malicious codes.
**5. Our Dual Scan Methodology:**Beyond our automated scanning, our seasoned security team conducts manual inspections and analysis, ensuring a deeper scrutiny of potentially suspect files or activities.
**6. Logging and Immediate Response:**Upon detection of any anomalies, details are promptly logged in our ticketing system, triggering our IT department’s immediate investigation.
**7. Ongoing User Training and Awareness Initiatives:**We regularly conduct training sessions. These programs underscore the significance of safely handling external files and emphasize threat recognition and adherence to best practices in file management.
Our active and comprehensive scanning approach ensures that we remain at the forefront of threat detection, maintaining the highest level of security and data integrity for our systems.

* .