# System and Communications Protection Procedure

|  |  |  |  |
| --- | --- | --- | --- |
| Procedures Owner |  |  | |
| Procedures Approver(s) |  |
| Effective Date |  | Next Review Date |  |

# Purpose

The purpose of this procedure is to define a consistent approach to manage System and Communications Protection of the IT environment at [COMPANY NAME].

# Scope

This procedure is consistent with CMMC and covers all system and communications protection procedures within [COMPANY NAME] environment. This procedure will be followed by all employees of [COMPANY NAME]. The CMMC System Security Plan (SSP) will be updated to reflect any significant modifications made to this procedure.

# Definitions

**Employees**: All individuals belonging to one or many groups defined below:

1. All individuals associated with [COMPANY NAME] through an employee – employer relationship or contract between [COMPANY NAME] and their employer or [COMPANY NAME] and individual.
2. All individuals possessing equipment issued by [COMPANY NAME]
3. All individuals working on the premises of [COMPANY NAME] and/or utilizing the Internet services provided by [COMPANY NAME].

# Governing Laws, Regulations, and Policies

* NIST SP 800-171, 3.13.1 - 3.13.16
* CMMC SC.L1-3.13.1 – SC.L2-3.13.16
* [COMPANY NAME] – SC – 3.13 - System and Communications Protection Policy

# Procedure Statements

**SC.L1-3.13.1** – **Monitor, control and protect organizational communications (e.g., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.**

1. External Boundaries are defined in the CUI Data Flow Diagram as in Appendix A of the [COMPANY NAME] System Security Plan.
2. Internal Boundaries are defined in the CUI Data Flow Diagram as in Appendix A of the [COMPANY NAME] System Security Plan.
3. [COMPANY NAME]’s System Administrator is to monitor communications (i.e., information transmitted or received by company computer systems) at the external boundaries of company CUI authorized systems on the company Microsoft GCC-H Instance/CUI Secure Enclave environment by using: [Insert Monitoring tools].
4. [COMPANY NAME]’s System Administrator is to monitor communications (i.e., information transmitted or received by company computer systems) at the internal boundaries of company CUI authorized systems on the company Microsoft GCC-H Instance/CUI Secure Enclave environment by [Insert Monitoring tools].
5. [COMPANY NAME]’s System Administrator is to control communications (i.e., information transmitted or received by company computer systems) at the external boundaries of company CUI authorized systems on the company Microsoft GCC-H Instance/CUI Secure Enclave environment by [Insert controlling tools/processes] and controlled such that connections are denied by default and only authorized connections are allowed. The authorization list for such connection can be found in <designated repository>.
6. [COMPANY NAME]’s System Administrator is to control communications (i.e., information transmitted or received by company computer systems) at the internal boundaries of company CUI authorized systems on the company Microsoft GCC-H Instance/CUI Secure Enclave environment by [Insert controlling tools/processes] and controlled such that connections are denied by default and only authorized connections are allowed. The authorization list for such connection can be found in <designated repository>.
7. [COMPANY NAME]’s System Administrator is to protect communications (i.e., information transmitted or received by company computer systems) at the external boundaries of company CUI authorized systems on the company Microsoft GCC-H Instance/CUI Secure Enclave environment by [Insert “protecting” tools/processes], applying encryption when required or prudent, tunneling traffic as needed.
8. [COMPANY NAME]’s System Administrator is to protect communications (i.e., information transmitted or received by company computer systems) at the internal boundaries of company CUI authorized systems on the company Microsoft GCC-H Instance/CUI Secure Enclave environment by [Insert “protecting” tools/processes], applying encryption when required or prudent, tunneling traffic as needed.

* Connections to external networks or systems are allowed only through managed interfaces consisting of the [insert Firewall] by configuring Destination Network Address Translation (DNAT), Azure network rules, application rules on the [COMPANY NAME] Microsoft GCC-H Instance/CUI Secure Enclave environment, encrypted tunnels, and are configured in accordance with the company security architecture.

**SC.L1-3.13.5** – **Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.**

1. Any publicly accessible systems are currently accessible in the information system are place on separate VLANs that cannot access information systems that store, process, and transmit CUI. For example, the guest network. The [COMPANY NAME] website is hosted offsite. Any future publicly accessible systems will be placed into similar VLANs or DMZs.
2. Boundary control devices and techniques on the Firewall are utilized to prevent public access to the [COMPANY NAME] secure enclave. All VLAN and DMZ management will be conducted by the <role>, with the assistance of the <IT Team>.

**SC.L2-3.13.2** - **Employ architectural designs, software development techniques and systems engineering principles that promote effective information security within organizational systems.**

1. [COMPANY NAME] applies system architecture security engineering principles in the specification, design, development, implementation, and modification of the system and system components designed to promote information security within the company systems.
2. [COMPANY NAME] applies software development security engineering principles in the specification, design, development, implementation, and modification of the system and system components designed to promote information security within the company systems.
3. [COMPANY NAME] applies system engineering security principles in the specification, design, development, implementation, and modification of the system and system components designed to promote information security within the company systems.
4. The systems Architecture security engineering discipline applies to each stage of the systems life cycle and provides security considerations in the following types:
   * New Systems: Includes activities such as concept exploration, alternatives and technologies employed in the new system.
   * Modifications to Systems: Includes reactive modifications due to incidents, accidents, and component failures; and planned modifications for system upgrades to enhance system capability.
   * Retirement of Systems: Includes the removal of the entire system functions or services from operation and/or the transition of system functions and services to another system.

Systems Architecture security engineering efforts include, but are not limited to:

* + System security requirements and verification methods.
  + Identification of vulnerabilities, hazards, and threats.
  + Proactive and reactive security strategies to control asset loss.
  + Engineering efforts to reduce errors, flaws and weakness that may cause a security vulnerability.
  + Evaluates the cost verses benefits of the security functions and consideration of alternatives or risk treatment decisions.
  + Performs security review in support of decision making and risk management.

System life cycle processes are employed to produce Architectural security outcomes that are necessary to achieve trustworthy secure systems. System life cycle processes include, but are not limited to:

* + Project Planning: The project is formally requested, and resources are committed.
  + System Requirements Definition: Security requirements and constraints are defined.
  + Architecture Definition: Secure functions for the system architecture is defined.
  + Acquisition: Security considerations are included when selecting a supplier.
  + Configuration Management: Security aspects are identified, managed, and included in the configuration baselines.
  + Risk Assessment: Security risks are identified and analyzed.
  + Maintenance: Systems or services necessary to support the security aspect of the system maintenance.
  + Disposal: Systems are securely removed from service, destroyed, reclaimed, or recycled.

1. The software development security engineering discipline applies to each stage of the systems life cycle and provides security considerations in the following types:
   * New Software: Includes activities such as concept exploration, alternatives and technologies employed in the new system.
   * Modifications to Software: Includes reactive modifications due to incidents, accidents, and component failures; and planned modifications for system upgrades to enhance system capability.
   * Retirement of Software: Includes the removal of the entire system functions or services from operation and/or the transition of system functions and services to another system.

Systems Software Development security engineering efforts include, but are not limited to:

* + System security requirements and verification methods.
  + Identification of vulnerabilities, hazards, and threats.
  + Proactive and reactive security strategies to control asset loss.
  + Engineering efforts to reduce errors, flaws and weakness that may cause a security vulnerability.
  + Evaluates the cost verses benefits of the security functions and consideration of alternatives or risk treatment decisions.
  + Performs security review in support of decision making and risk management.

System life cycle processes are employed to produce software development security outcomes that are necessary to achieve trustworthy secure systems. System life cycle processes include, but are not limited to:

* + Project Planning: Project is formally requested, and resources are committed.
  + System Requirements Definition: Security requirements and constraints are defined.
  + Architecture Definition: Secure functions for the system architecture is defined.
  + Acquisition: Security considerations are included when selecting a supplier.
  + Configuration Management: Security aspects are identified, managed, and included in the configuration baselines.
  + Risk Assessment: Security risks are identified and analyzed.
  + Maintenance: Systems or services necessary to support the security aspect of the system maintenance.
  + Disposal: Systems are securely removed from service, destroyed, reclaimed, or recycled.

1. The systems security engineering discipline applies to each stage of the systems life cycle and provides security considerations in the following types:
   * New Systems: Includes activities such as concept exploration, alternatives and technologies employed in the new system.
   * Modifications to Systems: Includes reactive modifications due to incidents, accidents, and component failures; and planned modifications for system upgrades to enhance system capability.
   * Retirement of Systems: Includes the removal of the entire system functions or services from operation and/or the transition of system functions and services to another system.

Systems security engineering efforts include, but are not limited to:

* + System security requirements and verification methods.
  + Identification of vulnerabilities, hazards, and threats.
  + Proactive and reactive security strategies to control asset loss.
  + Engineering efforts to reduce errors, flaws and weakness that may cause a security vulnerability.
  + Evaluates the cost verses benefits of the security functions and consideration of alternatives or risk treatment decisions.
  + Performs security review in support of decision making and risk management.

System life cycle processes are employed to produce security outcomes that are necessary to achieve trustworthy secure systems. System life cycle processes include, but are not limited to:

* + Project Planning: The project is formally requested, and resources are committed.
  + System Requirements Definition: Security requirements and constraints are defined.
  + Architecture Definition: Secure functions for the system architecture is defined.
  + Acquisition: Security considerations are included when selecting a supplier.
  + Configuration Management: Security aspects are identified, managed, and included in the configuration baselines.
  + Risk Assessment: Security risks are identified and analyzed.
  + Maintenance: Systems or services necessary to support the security aspect of the system maintenance.
  + Disposal: Systems are securely removed from service, destroyed, reclaimed, or recycled.
* [COMPANY NAME] requires that all organizational system, system components, and services meet at a minimum security and privacy requirements to maintain the confidentiality, integrity, and availability of [COMPANY NAME]’s systems, system components, and services. Architectural diagrams will be included in this document’s appendix. All system engineering/configurations are based on NIST SP 800-171/ CMMC 2.0 requirements.
* Configuration information is maintained by the <role>, in conjunction with the <IT Team>, and enforced through configuration mechanisms. Any deviation from required configurations that affect security must be approved by the <role> before putting into operation.

**SC.L2-3.13.3 - Separate user functionality from system management functionality.**

1. [COMPANY NAME]’s general users are not provided with the permissions necessary to perform any system administration functions. Permissions are only given by <role> to perform their role in the organization.
2. [COMPANY NAME]’s <role> can perform system administration functions. However, such function must include using their privileged account.
3. The Information System and components are configured to logically separate user functionality from management functionality. Management (e.g., system configuration) of desktop Information System and components and management (e.g., system configuration) of network servers is restricted to the <role>. Roles for user and administrator accounts are determined at the time of creation. User accounts are created by the <role> and the <IT Team>. Administrator accounts are created by the <role>, or by the <role>, with the approval of the <role>.

**SC.L2-3.13.4** **- Prevent unauthorized and unintended information transfer via shared system resources.**

1. [COMPANY NAME] configures the information system to prevent unauthorized and unintended information transfer via shared system resources using available system settings. For example:
   * By default, all [COMPANY NAME] user accounts have user-specific profile storage that is not accessible by other user accounts; users may not grant themselves elevated access rights; and may not grant other user accounts elevated access rights.
   * When necessary, and upon approval from the <role>, [COMPANY NAME] may establish storage containers on systems to enable sharing of information between users’ accounts, such as file share.
   * All [COMPANY NAME] organizational physical systems are wiped in accordance with DoD best practices prior to being re-issued to another [COMPANY NAME] user. Systems that may have had access to sensitive information conduct, at minimum, a DoD level three pass wipe, or equivalent, to ensure there is no data remanence that can be accessed by the new assigned user once the image is applied.

**SC.L2-3.13.6** **-** **Deny network communications traffic by default and allow network communications traffic by exception (e.g., deny all, permit by exception).**

1. The [insert Firewall] utilizes the default rule set which blocks all inbound connections unless specific exceptions are created. The firewall is configured to block outbound connections through Content Filtering (CF), filtering and blacklisting of domains.
2. Outbound connections and their associated responses are allowed through the firewall based on the organization’s business requirements. Firewall rules are reviewed semi-annually to ensure no unauthorized changes were made. Each application that requires traffic to be passed through the system firewall is reviewed by the <IT Team>, and appropriate traffic exceptions are placed into the firewall configuration, tested, and documented.

**SC.L2-3.13.7 – Prevent remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (e.g., split tunneling).**

1. The [insert Firewall] l has been configured to disable split-tunneling for remote devices which prevents the possibility of simultaneously establishing a non-remote connection with a system and communicating via other connections to resources in external networks. Computer systems have no Internet connectivity during the VPN session, except through the company firewall. Technical controls and configurations are established by the <role>, to prohibit any remote connection from making connections with any other systems or networks while connected to the [COMPANY NAME] information system.

**SC.L2-3.13.8** **- Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.**

1. The Information Systems employ cryptography that is validated through the NIST Cryptographic Module Validation Program (CMVP) to protect the confidentiality of CUI during transmission. The following safeguards are used for the protection of CUI data:
   * + Microsoft Windows Cryptographic Modules (Windows and Windows Server), CMVP certificate numbers 3300, 3527, 3544, 3630.
     + Microsoft Bitlocker Cryptographic Module (Windows and Windows Server), CMVP certificate numbers 3501. 3502.
     + (add any other systems used by the organization to protect CUI on the CMVP list)
2. [COMPANY NAME] defines the alternative physical safeguards to be employed when cryptographic mechanisms are not implemented to protect information during transmission. Refer to the [COMPANY NAME] Physical Protection Procedure.
3. [COMPANY NAME] utilizes the company GCC-H tenet space for transmission of CUI of which Microsoft protects CUI, at all times, via FIPS 140-2 compliant end-to-end encryption.

**SC.L2-3.13.9** **- Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.**

1. The period of inactivity to terminate network connections associated with communications sessions with the [COMPANY NAME] information system is defined as 15 minutes of inactivity. Users are required to terminate their session at the end of the workday, or after fifteen (15) minutes of inactivity, whichever comes first. Additionally, all [COMPANY NAME] systems are configured to restart at 20:00 PST automatically. This automated restart is configured via Group Policy. These automated configurations are configured and implemented by the <role>.
2. [COMPANY NAME] Information Systems are configured to terminate the internal and external network connections associated with communication sessions at the end of the session by deallocating TCP/IP addresses or ports at the operating system level, and/or deallocating assignments at the application system level to prevent malicious actors from taking advantage of an open network session.
3. [COMPANY NAME] Information Systems are configured to terminate the internal and external network connections associated with communication sessions at the defined period of inactivity by deallocating TCP/IP addresses or ports at the operating system level, and/or deallocating assignments at the application system level to prevent malicious actors from taking advantage of an open network session.
   * External (VPN) connections are configured in The Firewall to terminate network connections after a period of 60 minutes of inactivity.

**SC.L2-3.13.10** **- Establish and manage cryptographic keys for cryptography employed in organizational systems.**

1. Cryptographic keys are established whenever cryptography is employed by leveraging the practices and processes that Microsoft utilizes to protect the confidentiality of CUI to include Azure Key Vault. All cryptographic keys are retained in the information system Domain Controller.
2. [COMPANY NAME] <System Administrators> retain full administrative and cryptographic control of the user certificates. The key logs are managed through Azure Key Vault and monitored with [Insert Monitoring Tool].

**SC.L2-3.13.11** **- Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.**

1. The Information Systems and components that store and transfer CUI data for the organization employ FIPS-validated cryptography, utilizing Microsoft Bitlocker Whole Disk Encryption, [insert Firewall name] and Microsoft GCC-H, which is validated through the NIST, to protect the confidentiality of CUI in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

**SC.L2-3.13.12** **- Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.**

1. Collaborative computing devices are identified as webcams, headsets, or microphones and a log is stored on the <designated Repository>.
2. Collaborative computing devices provide indication to users of devices in use in the form of activation indicator lights to notify the user when the device is in use. Users are trained to be cognizant of the indicator light, to monitor and prevent remote activation. Any collaborative computing devices which are not provided with an activation indicator light (headsets) are required to be physically disconnected from the computer systems when not in use to prevent remote activation. Users are trained to physically disconnect these devices when not in use. Company provided laptops and tablets include built-in cameras and microphones with activation indicator lights to identify when the device is in use.
3. The default configuration for these devices is disabled in the protected system BIOS, preventing any activation, remote or locally. Enabling of the collaboration devices requires the approval of the <role>.

**SC.L2-3.13.13** **- Control and monitor the use of mobile code.**

1. Mobile code technology is currently not authorized for deployment by any components of [COMPANY NAME]. However, execution of code is monitored by [monitoring/malicious code tool] and any unauthorized mobile code installed on a user device will alert the <IT Team> through the [monitoring/malicious code tool portal]. Any user requesting authorization for the use of mobile code must obtain explicit authorization from [COMPANY NAME] administrators.
2. [COMPANY NAME] will not develop mobile code technologies without the authorization of the Information System (IS) Change Configuration Board (CCB). The CCB makes decisions regarding whether or not proposed changes to an information system should be implemented

**SC.L2-3.13.14 - Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.**

1. [COMPANY NAME] does not include voice-over Internet protocol (VoIP) equipment nor does the CCB authorize the use of any desktop VoIP products. The [COMPANY NAME] PPSM spreadsheet does not list VoIP protocols and therefore, those protocols should be blocked. Should [COMPANY NAME] in the future authorize VoIP technologies for the information system, the System Administrator authorizes any appropriate usage of VoIP within the information system.
2. [COMPANY NAME] then documents and implements a process to monitor and control the use of VoIP within the information system. The organization must maintain an audit trail of monitoring. [COMPANY NAME] will establish usage restrictions for VoIP technologies based on the potential to cause damage to the information system if used maliciously.

**SC.L2-3.13.15** **- Protect the authenticity of communications sessions.**

1. The organization provides mechanisms to protect the authenticity of communications sessions and protects against man-in-the-middle attacks, session hijacking and the insertion of false information into communications sessions. Controls and technologies are implemented to validate the identification and protect the session from attacks, utilizing Microsoft Multi-Factor Authentication (MFA) and one or more of the following:

* Virtual Private Network (VPN).
* Transport Layer Security (TLS).
* Secure Shell (SSH).
* Secure Socket Layers (SSL).
* Digital Signatures.
* Digital Certificates.
* Digital Time Stamping.
* FIPS-Validates Encryption.

**SC.L2-3.13.16** **- Protect the confidentiality of CUI at rest.**

1. [COMPANY NAME] Information Systems are configured to protect the confidentiality of CUI data at rest. To accomplish this the following methods are employed:
   * Access to the facility boundaries and information systems are limited to approved individuals with verified access authorizations.
   * Information Systems and components are configured to leverage data-at-rest protection utilizing Microsoft Bitlocker Full Disk Encryption (FDE) that meets the FIPS-Validated encryption requirement to protect the confidentiality and integrity of all related information.
   * Offline data (e.g., digital, and non-digital media) that requires secure protections are stored within secured areas or locked containers. Reference Physical Protection Procedures and Media Protection procedures for more details.
   * [Include any other methods]

# Roles and Responsibilities

|  |  |  |
| --- | --- | --- |
| **Role** | **Responsibilities** | **Contact Information** |
|  |  |  |
|  |  |  |

# Non-Compliance

Violations of this policy will be treated like other allegations of wrongdoing at [COMPANY NAME]. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for non-compliance may include, but are not limited to, one or more of the following:

1. Disciplinary action according to applicable [COMPANY NAME] policies;
2. Termination of employment; and/or
3. Legal action according to applicable laws and contractual agreements.

# Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Version ID** | **Date of Change** | **Author** | **Rationale** |
| V.01 | 11/28/2022 | Securestrux | Initial draft |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |