# Media Protection Procedure

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

# Purpose

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

# Scope

This procedure is consistent with CMMC and covers all media 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, 3.8.1 - 3.8.9
* CMMC MP.L1-3.8.1 – MP.L2-3.8.9
* [COMPANY NAME] – MP – 3.8 - Media Protection Policy

# Procedure Statements

**MP.L1-3.8.3 – Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse:**

1. Digital and non-digital media containing CUI data is required to be sanitized prior to disposal.
2. Digital and non-digital media containing CUI data is required to be sanitized prior release out of company control, or release for reuse.

* [COMPANY NAME] requires the proper marking of both electric and non-electronic media in accordance with DoDM 5200.01 Vol. 1-4 using techniques and procedures IAW NIST SP 800-88.
* [COMPANY NAME] utilizes the following methods for sanitization or destruction:
  + Destruction of digital media (CDs and DVDs) are to be performed using the NSA approved [Insert shredder name].
  + Destruction of digital media (hard drives) are to be performed using the NSA approved [Insert Degaussing Method].
  + Destruction of non-digital media (documents) are to be performed using the NSA approved [Insert shredder name].
  + Other methods of sanitization include the use of software that performs a wipe pattern to remove data from the device or component (e.g., [insert drive wiping utility software name] ).
* The <role> is responsible for reviewing, approving, and verifying digital media sanitization and disposal actions. The Project Manager (PM), or designee of, is responsible for reviewing, approving, and verifying non-digital media sanitization and disposal actions.

**MP.L2-3.8.1 - Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital:**

1. Access to non-digital media (paper) that contains CUI data is limited by physically controlling media. A CUI document control log is provided in the designated controlled area (GSA rated safe in the FSO office) to allow individuals to check out and return CUI media to maintain accountability for all stored media.
2. Access to digital media (diskettes, magnetic tapes, external and removable hard disk drives, flash drives, compact disks, and digital video disks) that contains CUI data is limited by physically controlling media. A CUI document control log is provided in the designated controlled area (GSA rated safe in the FSO office) to allow individuals to check out and return CUI media to maintain accountability for all stored media.
3. Access to non-digital media that contains CUI data is limited by physically controlling media and storge areas in accordance with the following:

* Storage of non-digital media is physically protected and secured within designated controlled areas (GSA rated safe in the FSO office) to utilizing badge reader technology for access by authorized users only.
* Approved lockable containers within users working spaces are also permitted to be utilized for the protection of non-digital CUI media for active projects.

1. Access to digital media that contains CUI data is limited by physically controlling media and storge areas in accordance with the following:

* Storage of non-digital media is physically protected and secured within designated controlled areas (GSA rated safe in the FSO office) to utilizing badge reader technology for access by authorized users only.
* Approved lockable containers within users working spaces are also permitted to be utilized for the protection of digital CUI media for active projects.
* For employees who are work from home and manage Digital and/or Non-digital CUI data, storage of CUI media is physically protected and secured within designated controlled area in a room that can be locked. An approved lockable container within users’ working spaces are also permitted to be utilized for the protection of digital and non-digital CUI media for active projects. A CUI document control log is provided for the remote employee to allow employees to keep track of the use of the CUI media to maintain accountability for all stored media.

**MP.L2-3.8.2** **- Limit access to CUI on system media to authorized users**:

1. Access to media containing CUI data is limited using Role-Based Access Control (RBAC) at the discretion of the <System Administrator> and <FSO>. The <FSO> will maintain a list of Roles and/or personnel with access to CUI data within the company. A CUI document control log is provided in the designated controlled area (FSO Office) to allow individuals to check out and return CUI media to maintain accountability for all stored media.

**MP.L2-3.8.4** **- Mark media with necessary CUI markings and distribution limitations:**

1. [COMPANY NAME] requires the proper marking of both electric and non-electronic media. Organizational personnel mark media in accordance with Section Marking and Labeling Requirements of the DoDI 5200.01 DoD Information Security Program and Protection of Sensitive Compartmented Information, DoD Manual (DoDM) 5200.01 Vol 1-4 and DoDI Instruction 5200.48 – Controlled Unclassified Information (CUI). For additional reference review <https://www.archives.gov/cui/registry/category-marking-list>.
2. [COMPANY NAME] requires the proper Distribution limitations marking of both electric and non-electronic media. Organizational personnel mark media in accordance with Section Marking and Labeling Requirements of the DoDI 5200.01 DoD Information Security Program and Protection of Sensitive Compartmented Information, DoD Manual (DoDM) 5200.01 Vol 1-4 and DoDI Instruction 5200.48 – Controlled Unclassified Information (CUI). For additional reference review <https://www.archives.gov/cui/registry/limited-dissemination>.

**MP.L2-3.8.5** **- Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas:**

1. [COMPANY NAME] Security Group ensures the [COMPANY NAME] defined security measures includes a requirement to develop and maintain a list of personnel authorized to transport information system media outside of controlled areas, IAW DoDM 5200.01 M Vol. 1-4 and DoDD 5015.2. A chain-of-custody is also kept at all times.
2. In the event the [COMPANY NAME] has a need to ship components the primary means of shipping is through FedEx. The choice of a specific vendor is determined by several factors including the size and weight of the material, how fast it needs to be on site, distance, classification, etc. (Note: Movement Tracking System (MTS) is authorized to ship material up to and including Secret). All material that is moved thru the MTS is insured and tracked by the vendor and the MTS. A transportation control number (TCN) is provided to MTS once the material is processed for movement followed by the vendor’s tracking number once it is on the delivery vehicle. Most vendors have websites available to the public to track the shipment in transit. Confirmation of delivery can be obtained from the vendor website and can be requested directly if required. No equipment is shipped with sensitive organizational information.

**MP.L2-3.8.6** **- Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards:**

1. All media to include external USB drives and external hard drives authorized for use within the [COMPANY NAME] are FIPS 140-2 encrypted to ensure security safeguards are in place when [COMPANY NAME] personnel transport these items. These items are to be maintained in the possession of <IT personnel> assigned the equipment. The use of external storage devices must be explicitly authorized by the <IT Team>. No unauthorized external storage devices are permitted for use at [COMPANY NAME]. In the event that a non-encrypted storage device is connected to [COMPANY NAME] media stations, logs of the event will be collected and forwarded to the [COMPANY NAME] Microsoft Sentinel SIEM. The <role>, with the assistance of the <MSP, SecureStrux> will investigate the occurrence.

**MP.L2-3.8.7** **- Control the use of removable media on system components:**

1. [COMPANY NAME] Media includes both digital and non-digital media containing information not cleared for public release such as: Compact Disks/Digital Video Disks (CD/DVD), portable hard drives, removable hard disks, magnetic tapes, flash drives, paper, and microfilm. Authorization to Burn CD or connect external USB storage device requires authorization and a specific PC exemption to grant permissions to do so. Certain components may contain internal hard disks or flash drives which are considered non-removal (i.e. the system needs to be disassembled to remove the drive hence no external direct access to storage drive). [COMPANY NAME] does disseminate portable hard drives to organizational personnel for backup purposes, etc. The determination for this dissemination is based on need and not role. These drives include FIPS 140-2 compliant encryption which prevents unauthorized access. CDs/DVDs are also permitted for use by all organizational personnel. [COMPANY NAME] personnel are trained and held accountable for protecting organizational information that is not cleared for public release. [COMPANY NAME] obtains and examines the documented personnel or roles to restrict access to media to ensure the access is granted.

**MP.L2-3.8.8** **- Prohibit the use of portable storage devices when such devices have no identifiable owner.**

1. The [COMPANY NAME] prohibits the use of portable storage devices in organization information systems when such devices have no identifiable owner. To further prevent the unauthorized use of media, [COMPANY NAME] deploys Microsoft Sentinel to restrict the use of portable USB storage devices (except for those that are assigned by the [COMPANY NAME] to organizational personnel, and which are registered in the Microsoft Sentinel for that specific user through group policy).
   * Any attempts to use unauthorized portable storage devices will be blocked and an alert sent to the <IT Team>. The <IT Team> will receive an automatic alert that an attempt to use an unauthorized removeable media has been attempted. Only authorized users have the ability to use removeable media. Any attempt to transfer data to portable storage devices is logged and monitored by the <IT Team>. Any unauthorized user that attempts to store sensitive data on removeable media will cause an alert in the Microsoft Sentinel.

**MP.L2-3.8.9** **- Protect the confidentiality of backup CUI at storage locations.**

1. Backups of [COMPANY NAME] data are controlled and managed by <the MSP>. All Backups are encrypted by Microsoft Bitlocker FDE which is FIPs 140-2 validated.

**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 | 12/5/2022 | Securestrux | Initial draft |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |