# Access control procedure

|  |  |  |  |
| --- | --- | --- | --- |
| Procedure owner |  | Signature: **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** | |
| Procedure approver(s) |  |
| Effective date |  | Next review date |  |

# Purpose

The purpose of this procedure is to define a consistent approach to manage access control of the it environment at Matt's Company.

# Scope

This procedure is consistent with CMMC and covers all network and system access 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, 3.1.1 - 3.1.21
* CMMC AC.l1-3.1.1 – AC.l2-3.1.21
* [COMPANY NAME] – AC – 3.1 - access control policy

# Procedure statements

**AC.L1-3.1.1** – **Authorized Access Control: Limit Information System Access To Authorized Users, Processes Acting On Behalf Of Authorized Users, Or Devices**

1. [COMPANY NAME] manages all IT onboarding processes through the IT department. This department uses email distribution lists to route approved appointment letters to the account managers for the account creation process. All accounts, including users and administrators that will be created in the Azure Active Directory.
2. To monitor the use of the IS and IS accounts, auditing of all is components has been implemented. All audit records of is components are sent to the [SIEM Solution]. All account logon and logoff events are audited. In addition to logon events, all privileged access events generate audit records. This assists the <Role> in determining if account holders are violating the terms of use and aids in potentially identifying insider threats. Please refer to the audit policy for more detailed information regarding auditing.
3. All devices added secure enclave will be identified by their (Static IP/MAC Address/Unique Identifier) and monitored and audited.
4. All [COMPANY NAME] devices are restricted by Microsoft Endpoint Manager conditional access policies. Only authorized devices have the ability to access the [COMPANY NAME] secure enclave.
5. Immediately upon notification that an employee no longer requires access to the is, account managers are notified via email (a specific distribution list is used). Each account manager will respond to all individuals in the email distribution with a notification that the account has been disabled or deleted. Additionally, the following actions are completed:

* Retrieve keys, smart cards, tokens, badges, etc.
* Remove all access permissions to critical/sensitive areas, such as telephone closets, computer rooms, and areas containing sensitive information
* Disabled the employee’s account and password from all systems and networks; to include any external communication user ids
* Retrieve all hardware, software, and documentation.

**AC.L1-3.1.2** – **Transaction & Function Control:** **Limit Information System Access To The Types Of Transactions And Functions That Authorized Users Are Permitted To Execute**:

1. <Role> adhere to all policies and procedures relating to account management through the creation, enabling, modifying, disabling and removal of accounts. Role-based access controls are used to manage users and do not require additional security attribute definitions. Role membership is based upon the <Role>’s appointment letter. [COMPANY NAME] policy prohibits group/shared account credentials. All accounts are verified on an annual basis for compliance. The process and requirements for onboarding non-privileged users is the same as described for <Role> personnel. Personnel in any of these roles can be assigned the privileged user level functionality necessary in the performance of their job duties and are assigned group memberships that parallel those of the <Role> but have only the needed privileges. <Role>s assign permissions utilizing least privileged principles.
2. The <Role> is responsible for ensuring that all <Role>s supporting the organization have met the requirements for accessing the IS and are aware of their roles and responsibilities. After the <Role> clears a <Role>for access, the <Role>is issued an appointment letter that details their roles and responsibilities regarding administration of the IS. The <Role> signed approval also serves as an approval to begin the account creation process. All accounts within the organization are unique and new (i.e. no reuse of prior accounts). Accounts are created and assigned IAW the role the <Role> has been appointed. These roles establish the permissions granted to the account when assigned membership to the role. Once the <Role> has approved access and the appointment letter has been signed by the on-boarded personnel and <Role>, designated <Role>s will create the accounts and/or distribute applicable authenticators. All <Role>s are authorized by the <Role> by appointment letter to perform account management functions within their respective areas.

**AC.L1-3.1.20 – Verification, Control, And Limitations Of Connections To And Use Of External Information Systems:**

1. Connections to external systems are identified to include; for example, personally owned systems or devices, commercial or public systems, contractor systems, systems owned by other organizations and cloud services.
2. Connecting to external systems for the processing, storage and transmission of CUI data is only permitted as part of the business function, specifically authorized by the <role>, based on project requirements, and in accordance with client/owner requirements. Prior to individuals connecting to and use of an external information system, the organization will: Verify the implementation of required security controls on the external system and obtain approved system connection or processing agreements with the organizational entity hosting the external system.
3. [COMPANY NAME] currently is using (virtual environments) to access their secure GCC-H enclave and thus no external connections other than one physical device for printing if needed. The physical device is maintained and verified by the <Role> to have the same suite of tools as all devices connected to the company secure GCC-H as mentioned in Configuration Management.
4. Prior to individuals connecting to and use of an external information system, the organization will: Verify the implementation of required security controls on the external system and obtain approved system connection or processing agreements with the organizational entity hosting the external system.
5. [COMPANY NAME] currently controls or limits access to the physical external device by Role Based Access Control through Azure Active Directory and a physical access control list maintained by the <Role>. Only authorized users are able to access the physical external device.
6. Connecting to external systems for the processing, storage and transmission of CUI/FCI data is only permitted as part of the business function, specifically authorized by the <role>, based on project requirements, and in accordance with client/owner requirements.

**AC.L1-3.1.22 – Control Information Posted Or Processed On Publicly Accessible Information Systems:**

1. Only authorized individuals (<Human Resources> and <Privileged Users>) are authorized to post information onto publicly accessible systems.
2. In accordance with laws, Executive Orders, directives, policies, regulations, or standards, the public is not authorized access to nonpublic information (e.g., information protected under the Privacy Act, FCI, CUI, and proprietary information). Only authorized individuals (Human Resources and Privileged Users) are authorized to post information onto publicly accessible systems (e.g., www. [COMPANY NAME].com - company website, LinkedIn, Facebook, etc.). procedures to ensure Federal Contract Information (FCI) / Controlled Unclassified Information (CUI) is not posted or processed on publicly accessible systems (e.g., www.[COMPANY NAME].com - company website, LinkedIn, Facebook, etc.).
3. Content of publicly accessible information for nonpublic information is reviewed annually by HR or whenever modifications are made to the system.
4. Proposed content of information is reviewed and approved prior to posting onto the publicly accessible system to ensure that nonpublic information is not included.
5. Any nonpublic information found to be on the system will be removed, if discovered. [COMPANY NAME] is to follow proper internal protocols for employee disciplinary actions upon discovery.

**AC.L2-3.1.3** - **Control the flow of CUI in accordance with approved authorizations:**

1. Information flow control policies are defined in the CUI data flow diagram available for review in the [COMPANY NAME] System Security Plan Appendix \_\_\_ .
2. Site-to-site information flow to client owned and operated systems are in accordance with client requirements, with enforcement that is accomplished using a combination of static routes, firewall Access Control Lists (ACL), and end-to-end encryption.
3. Designated sources and destinations (e.g., networks, individuals, and devices) for CUI within the system and between interconnected systems are identified on the CUI flow diagram available for review in the System Security Plan.
4. Authorizations for controlling the flow of CUI are defined by the Employee onboarding process or upon submission and approval of the employee submitted SAAR to the IT department.
5. Approved authorizations for controlling the flow of information between interconnected systems has been provided via the use of system access permissions and boundary protection devices such as gateways, encrypted tunnels, and firewalls. [COMPANY NAME] utilizes [Firewall Solution] groups as an application and IP-layer proxy to filter inbound and outbound Internet traffic. The firewall is configured to block inbound and outbound connections to bots, foreign countries, spyware, virus sources and inappropriate web content.

**AC.L2-3.1.4 – Separate The Duties Of Individuals To Reduce The Risk Of Malevolent Activity Without Collusion:**

1. The duties of individuals requiring separation are the Regular users and <Role>s divided into the following roles:
   * System Administrator
   * Network Administrator
   * Super Administrator
   * Regular User
2. Separation of duties is determined during the onboarding and transfer process where appointment letters and team membership are established. Only designated, trained, and appropriately cleared personnel have authority to access or modify IS components and is based on a demonstrated need-to-know.
3. Team assignments are documented in each appointment letter. There is more than one System Administrator assigned to each of the above listed teams always, all with the same access and permission levels. Other authorizations are granted in accordance with an <Role> approved letter. Audit review is performed by the <Role>, which utilizes software to look for indicators of compromise (IOC). Lastly, [COMPANY NAME] has a cyber team to further audit the IS components concerning software and configuration compliance.

**AC.L2-3.1.5 - Employ The Principle Of Least Privilege, Including For Specific Security Functions And Privileged Accounts:**

1. Privileged accounts are identified by the <Role> and approved by the <role>. The <Role> will keep documentation outlining privileged accounts.
2. Users are provided the lowest level of access required to perform their assigned mission/business function, ensuring that the principal of least privilege is enforced. Users access level and associated need-to-know, is verified prior to granting access to the information system and CUI data.
3. Security functions are identified as any privileged function. (e.g., access control configuration, system configuration settings, or privileged account lists)
4. Accounts that provide access to security functions (any privileged function), to include access to system configuration, auditing, and data transfers, are restricted to only those individuals who have been properly vetted by the organization and approved by the <role>. Elevated commands are restricted to authorized personnel for compelling operational needs (e.g., auditing, installing authorized software, etc.). The <role> determines who requires this access, why the access is required, and what mission impact will occur if the access is not granted.

**AC.L2-3.1.6 - Use Non-Privileged Accounts Or Roles When Accessing Non-Security Functions:**

1. Access to security functions is restricted to Privileged Users (e.g., Network and Server Administration). Power Users are restricted to those functions necessary to perform assigned job duties (e.g., workstation administration, auditing, data transfers, etc.). Non-Security functions are defined as anything not necessary to perform assigned job duties as a Privileged user.
2. All Privileged Users are also provided with a non-privileged General User account. This account is used when accessing non-security functions.

**AC.L2-3.1.7- Prevent Non-Privileged Users From Executing Privileged Functions And Capture The Execution Of Such Functions In Audit Logs**.

1. Privileged functions are defined as functions that involve the control, monitoring or administration of the system, including security functions and log management.
2. Non-privileged accounts are identified by the <Role>. The <Role> will keep documentation outlining non-privileged accounts.
3. The Information System is configured to prevent non-privileged users from executing privileged functions. This includes disabling, circumventing, or altering implemented security safeguards and countermeasures.
4. The Information System is configured to audit privileged functions. Audit reviews are completed on a weekly basis using [SIEM Solution]. The tracking software is updated and maintained by the <ISSO>.

**AC.L2-3.1.8 - Limiting Unsuccessful Login Attempts.**

1. Account lockout policy is a security feature that locks a user account after 10 failed login attempts have occurred within a specified period.
2. The number of allowed attempts and the period are based on the values that are configured for the policy. The systems that manage the lockout policy include [Access Control Solution] and [End Point Manager]. System components are configured to point to the account management systems where they depend upon most settings associated with account lockout policy. Additionally, all system components are configured to include any local account management requirements if applicable. The account lockout policy/procedures are compliant with DOD defined parameters as follows:

* The maximum number of consecutive invalid logon attempts is ten.
* The minimum time-period for the invalid login attempts is 15 minutes.
* The account shall be locked until released by the appropriate administrator when the account lockout has been activated

**AC.L2-3.1.9 - Provide Privacy And Security Notices Consistent With Applicable CUI Rules:**

1. The approved warner banner is documented in the Directive-Type Memorandum (DTM) 08-060, “Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement,” September 2013. The warning banner is mandatory, and deviations are not permitted except as authorized in writing by the Deputy Assistant Secretary of Defense for Information and Identity Assurance. The warning banner remains on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the IS. Publicly accessible systems (i.e. servers defined as public) do not exist.
2. Privacy and security notices are displayed on all Digital and Physical CUI data to include the mobile devices. [COMPANY NAME] Warning Statement is as follows:

“WARNING WARNING WARNING

This is a [COMPANY NAME] computer system. [COMPANY NAME] computer systems

are provided for the processing of official [COMPANY NAME] information only. All data contained

on [COMPANY NAME] computer systems is owned by [COMPANY NAME] and may be monitored, intercepted,

recorded, read, copied, or captured in any manner and disclosed in any manner, by

authorized personnel. THERE IS NO RIGHT OF PRIVACY IN THIS SYSTEM. System

personnel may give to law enforcement officials any potential evidence of crime

found on [COMPANY NAME] computer systems. The information system contains CUI with specific requirements

imposed by the Department of Defense; and Use of the information system may be subject to other specified

requirements associated with certain types of CUI such as Export Controlled information. USE OF THIS

SYSTEM BY ANY USER, AUTHORIZED OR UNAUTHORIZE, CONSTITUTES CONSENT TO THIS

MONITORING. INTERCEPTION, READING, COPYING, OR CAPTURING AND DISCLOSURE.

WARNING WARNING WARNING”

Interactive login banner for devices

<https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/interactive-logon-message-text-for-users-attempting-to-log-on>

Login banner for Azure Company Branding:

<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/customize-branding>

**AC.L2-3.1.10 - Use Session Lock With Pattern-Hiding Displays To Prevent Access And Viewing Of Data After A Period Of Inactivity:**

1. The period of inactivity after which the system initiates a session lock is defined as 15 minutes.
2. Screen lock is deployed on all virtual workstations/ virtual servers and activated after 15 minutes of inactivity or by explicit user action. Once screen lock is enabled, only authorized users with valid, unique authenticators can regain access. All other components within the IS utilize an inactivity timer that will log the user out when that timer expires.
3. Screen locks cover the entire visible area of the screen with unclassified content that was not previously visible on the display.

**AC.L2-3.1.11 - Terminate (Automatically) A User Session After A Defined Condition:**

1. All components of the information system are configured to terminate user sessions based on the following conditions:

* 15 minutes of user inactivity over a remote connection to a windows workstation
* 15 minutes of user inactivity over a remote connection to a windows server
* 15 minutes of user inactivity over a connection from the mobile devices.

1. All components of the information system are configured to terminate user sessions based on the conditions above.

**AC.L2-3.1.12- Monitor And Control Remote Access Sessions:**

1. Remote access methods permitted and utilized within the IS include authentication methods for controlling access.
2. Due to the nature of the decentralized configuration of the secure enclave, all access to the secure enclave will be a remote connection.
3. All components of the IS are configured IAW applicable STIGs for configuring and controlling approved remote access methods. Only designated and appropriately cleared <roles> have the authority to access or modify the IS. Usage of these remote access services is solely for the purposes of operating, administering, monitoring, and troubleshooting IS components. [COMPANY NAME] utilizes a managed and controlled desktop image that is deployed with the approved baseline image of applications including those approved for use for remote access.
4. [COMPANY NAME] monitors remote access methods utilizing audit record content generated by each IS component IAW the Audit Policy. All remote access sessions are logged and audited with the [SIEM Solution].

**AC.L2-3.1.13 - Employ Cryptographic Mechanisms To Protect The Confidentiality Of Remote Access Sessions**:

1. Information regarding approved remote access methods are covered in Remote Access and Automated Monitoring/Control utilize Federal Information Processing Standards (FIPS) 140-2 certified cryptographic mechanisms to protect the confidentiality and integrity of the remote access session.
2. Cryptographic mechanisms to protect the confidentiality of remote access sessions are implemented by default. All connections to the secure enclave are TLS 1.2.

**AC.L2-3.1.14 - Route Remote Access Via Managed Access Control Points.**

1. Managed access control points are identified by the [Firewall Solution] and implemented as the sole point in which traffic to and from the Secure GCC-H enclave goes.
2. All external remote access connections are routed through a managed network control point to the [Firewall Solution] which includes anti-malware, anti-virus, Intrusion Detection & Prevention capabilities. Logs are to be forwarded to the [SIEM Solution] for monitoring and auditing.

**AC.L2-3.1.15 - Authorize Remote Execution Of Privileged Commands And Remote Access To Security-Relevant Information.**

1. Remote access methods are authorized for use and specifically allow for system administration of the IS. This includes privileged command execution necessary in performing system administration tasks. Privileged functions and commands authorized for remote execution include:

* System account creation, modification, and deletion
* Performing system integrity checks
* Reviewing and administering system audit logs
* Administering intrusion detection and prevention mechanisms
* Administering malicious code detection mechanisms
* Administering cryptographic key management activities
* Configuration and security management of the system and system components

1. Remote access methods are authorized for use and specifically allow for system administration of the IS. This includes accessing security-relevant information necessary in performing system administration tasks. Security-relevant information authorized for remote access include:

* Audit logs and audit policies
* System account information
* Access control policies
* Intrusion detection and prevention mechanism data and alerts
* Malicious code detection data and alerts

1. Remote access methods are required for the efficient and timely management (privileged command execution) of the IS and only permitted for necessary operational functions. Privileged functions are delineated based upon a user’s role in the secure enclave. All users will follow the Principle of Least Privilege (PoLP), a security concept in which a user is given the minimum levels of access or permissions needed to perform their job
2. Remote access methods are required for the efficient and timely management (accessing security-relevant information) of the IS and only permitted for necessary operational functions. Security Relevant Information access are delineated based upon a user’s role in the secure enclave. All users will follow the Principle of Least Privilege (PoLP), a security concept in which a user is given the minimum levels of access or permissions needed to perform their job

**AC.L2-3.1.16 - Authorize Wireless Access Prior To Allowing Such Connections.**

1. Only company owned and maintained wireless devices (laptops and tablets) are authorized to be used for [COMPANY NAME] wireless access. Wireless components for desktop computer systems are not provided or permitted to be installed. Privately owned devices cannot access the Secure Enclave environment. A guest SSID is available for use. This guest SSID is configured on a separate VLAN from the internal wireless network.
2. Wireless access usage restrictions are as follows:

* Restricted to authorized users who are in need of use of the Secure Enclave environment to perform regular job duties.
* Must be approved by the <role> prior to use.
* The user wishing to access the guest SSID must provide device MAC address information to the MIS Manager before the device can authenticate into the guest SSID. All certificate-based authentication and MAC addresses filtering is configured and managed by the <role>.

**AC.L2-3.1.17- Protect Wireless Access Using Authentication And Encryption.**

1. Wireless devices are protected via user authentication protocols and encryption, at minimum utilizing wi-fi protected access II WPA2-AES.
2. [COMPANY NAME] employs physical network segmentation as well as wireless protected access 2 with pre-shared key (WPA2-PSK) technology to control access to the wireless networks. A physically separate wireless local area network (WLAN) with WPA2-PSK is utilized to provide secure wireless service for guests. Passwords are changed regularly by [COMPANY NAME] administrators. Wireless access to the [COMPANY NAME] commercial network employs the use of WPA2-PSK that is manually entered by Network Administrators on [COMPANY NAME] mobile devices. The pre-shared key (PSK) is not provided to the end-user and is changed on a regular basis. Additionally, the wireless access points (WAPs) limit the ability for WLAN clients to communicate with each other. Wireless connectivity is logged in the WAPs administrative console and reviewed weekly for anomalies.

**AC.L2-3.1.18** - **Control Connection Of Mobile Devices**:

1. Mobile devices that process, store, or transmit CUI are identified by the <role> and logged in the [MDM Solution].
2. Mobile devices that process, store, or transmit CUI are authorized access by the [MDM Solution] to the Information System.
3. Connection of unauthorized mobile devices are monitored using the [MDM Solution]. Logs are reviewed weekly for unauthorized connections by the <role>.

**AC.L2-3.1.19 - Encrypt CUI on mobile devices and mobile computing platforms**

1. [COMPANY NAME] Mobile device connections are currently controlled and identified by the [MDM Solution]
2. The <role> configures [MDM Solution] to force AES-256, FIPS 140-2 Compliant encryption on mobile devices accessing the [COMPANY NAME] information system. The <role> has the ability to remotely protect and erase any information store on [COMPANY NAME] mobile devices.

OR

1. [COMPANY NAME] does not authorize the use of any mobile devices (cellular phones, tablets, handheld devices) for accessing the secure enclave. No mobile devices are authorized to store, process, or transmit CUI data.
2. Connection of unauthorized mobile devices are monitored using the [SIEM Solution]. Logs are reviewed weekly for unauthorized connections by the System Administrator.

**AC.L2-3.1.21- limit use of portable storage devices on external systems.**

1. The use of portable storage devices containing CUI on external systems is identified and documented by the <Role>.
2. Portable storage devices are system components that can be inserted and removed from Information Systems for the purpose of storing data. Examples of portable storage devices include CD/DVD’s, thumb drives, USB hard drives and flash memory cards
3. The Portable store devices are restricted with GPO and IDS/IPS/Monitoring. By default, standard user devices are configured to disable the use of portable storage devices with the use of GPO. Any defined users that require the use of portable storage devices are restricted to only use [COMPANY NAME] authorized removeable media. IDS/IPS/Monitoring is configured to only allow authorized media on these systems. All non-authorized removable media is disallowed through IDS/IPS/Monitoring.

Media stations are placed around the [COMPANY NAME] facility that are designated for the use of removeable media. All media stations are monitored by the [SIEM Solution], IDS/IPS/Monitoring, and controlled by [COMPANY NAME] administrators.

**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** | **Date of change** | **Author** | **Rationale** |
| V.01 | 12/7/2022 | Securestrux | Initial draft |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |