**CMMC V1.02 Level 1 System Security Plan Template**

<*Replace all highlighted text with your information*>

<Department Name>

< Date>

# ENVIRONMENT PROFILE

<Provide context by briefly describing the nature and purpose of your operating environment associated with Federal Contract Information (FCI) and Controlled Unclassified Information (CUI).>

# ENVIRONMENT AND ASSETS

<It is critical to inventory and document the systems and devices involved with storing, processing, accessing, and safeguarding FCI and CUI.

Use this section to briefly give an overview of the environment and systems associated with storing, processing, accessing, and safeguarding FCI and CUI.

The Appendix section includes a template for documenting asset information in greater detail that could be recorded in a separate document.

Sample language:

‘*The Enclave is made up of three Linux systems used to store FCI. The Enclave resides on a designated subnet and is isolated from the rest of the UW network using a managed firewall that limits connections to and from the subnet to only authorized systems. Husky OnNet-Department (HON-D) VPN is used to ensure that only authorized accounts can connect to the Enclave systems.’*

>

# PRACTICES

## ACCESS CONTROL (AC)

### Access Control - C001

| Capability | |
| --- | --- |
| ID | C001 |
| Description | Establish system access requirements. |

| Practice | |
| --- | --- |
| AC.1.001 | Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). |
| Implementation Details:  < REPLACE HIGHLIGHTED TEXT WITH YOUR DOCUMENTATION  Documentation should include:   * Process for ensuring that only authorized users have access. Include processes for onboarding, offboarding and regularly auditing access. * The technical controls used for limiting access to systems to only authorized staff (Ex: Each employee is issued a unique UW NetID with specific password requirements that must be used to log on to all computers and systems that store FCI and CUI. Departmental policy requires that staff use two-factor authentication to access systems that store and process sensitive information. We use Windows Group Policies to auto-lock workstations and servers after 15 minutes of inactivity.) * Process for approving devices that are allowed to connect to UW/departmental systems (Ex: Employees using wireless to connect to UW and departmental systems must use Eduroam which requires UW NetID authentication and provides an encrypted session. Remote connections (from home) must be made from department-issued computers and require the use of Husky OnNet VPN which provides an encrypted secure connection to UW/departmental systems.)   *UW Services that could be leveraged to meet control requirements include\*:*   * *ASTRA Access Management* * *Active Directory, Azure AD, Azure ExpressRoute* * *Directory Services* * *Certificate Services* * *Enterprise Web Services & Events* * *Husky OnNet VPN / HON-D VPN* * *DUO (2-Factor Authentication)* * *Kerberos* * *LDAP* * *UW Groups* * *UW NetID* * *Web SSO*   *\*List of services may not be complete or applicable for a given configuration. The use of a given service does not necessarily satisfy control requirements or may require specific configuration to meet control requirements. Documentation should include how the service is implemented to meet the control requirements. >* | |

### Access Control - C002

| Capability | |
| --- | --- |
| ID | C002 |
| Description | Control internal system access. |

| AC.1.002 | Practice |
| --- | --- |
| Practice: Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | |
| **Implementation Details:**  **< REPLACE HIGHLIGHTED TEXT WITH YOUR DOCUMENTATION**  Documentation should include:   * The processes and controls by which access and functions for authorized staff are granted the minimum level of permissions required to perform their assigned job function (principal of least privilege). *(Ex: Staff do not have administrative access on their workstations. Active Directory user groups are used to limit access to departmental folders and files to only authorized personnel. Support staff use designated administrative accounts to perform system maintenance tasks. Staff access and security group memberships are reviewed regularly by managers.)*   *UW Services that could be leveraged to satisfy control requirements include\*:*   * *ASTRA Access Management* * *Active Directory, Azure AD, Azure ExpressRoute* * *Directory Services* * *Certificate Services* * *Enterprise Web Services & Events* * *Husky OnNet VPN / HON-D VPN* * *DUO (2-Factor Authentication)* * *Kerberos* * *LDAP* * *UW Groups* * *UW NetID* * *Web SSO*   \**List of services may not be complete or applicable for a given configuration. The use of a given service does not necessarily satisfy control requirements or may require specific configuration to meet control requirements. Documentation should include how the service is implemented to meet the control requirements. >* | |

### Access Control – C004

| Capability | |
| --- | --- |
| ID | C004 |
| Description | Limit data access to authorized users and processes. |

| AC.1.003 | Practice |
| --- | --- |
| Practice: Verify and control/limit connections to and use of external information systems. | |
| **Implementation Details:**  **< REPLACE HIGHLIGHTED TEXT WITH YOUR DOCUMENTATION**  Documentation should include:   * The processes and controls used to limit and control access to users and processes between internal systems and external systems. External systems can include systems external to the UW network (internet) or external to a private internal network.  *(Ex: Internal systems are configured with private IP addresses managed by UW IT and separated from the internet via an Enterprise firewall and an Intrusion Prevention System (IPS). Internal systems are not configured with public IP addresses and are therefore not reachable from outside the UW network without a VPN connection. Remote users must use work issued laptops and Husky OnNet VPN to connect to internal information systems. Eduroam is used for all internal wi-fi connections. Departmental systems are on a designated subnet and use the UW-IT Managed Firewall Service to limit connections to/from external systems, etc.)*   *UW Services that could be leveraged to satisfy control requirements include\*:*   * *Intrusion Prevention System* * *Managed Firewall Service* * *Private Address Routing* * *Husky OnNet VPN / HON-D VPN*   \**List of services may not be complete or applicable for a given configuration. The use of a given service does not necessarily satisfy control requirements or may require specific configuration to meet control requirements. Documentation should include how the service is implemented to meet the control requirements. >* | |

| AC.1.004 | Practice |
| --- | --- |
| Practice: Control information posted or processed on publicly accessible information systems. | |
| **Implementation Details:**  **< REPLACE HIGHLIGHTED TEXT WITH YOUR DOCUMENTATION**  Documentation should include:   * Processes and controls used to ensure systems that store FCI and CUI cannot be accessed anonymously (no password required), and that sensitive data are not shared with unauthorized personnel, or anyone outside of the contract. Review access regularly. * Processes and technical controls used to prevent sensitive information from becoming publicly available (websites or the media) or in ways that could be accessed by the public. Document how information is vetted before it is released to the public. * Separation of Duties to prevent errors.   *UW Services that could be leveraged to satisfy control requirements include\*:*   * *ASTRA Access Management* * *Active Directory* * *Active Directory Security Groups* * *DUO (2-Factor Authentication)* * *UW Groups* * *UW NetID* * *Web SSO*   \**List of services may not be complete or applicable for a given configuration. The use of a given service does not necessarily satisfy control requirements or may require specific configuration to meet control requirements. Documentation should include how the service is implemented to meet the control requirements. >* | |

## IDENTIFICATION AND AUTHENTICATION (IA)

### Identification and Authentication – C015

| Capability | |
| --- | --- |
| ID | C015 |
| Description | Grant access to authenticated entities. |

| IA.1.076 | Practice |
| --- | --- |
| Practice: Identify information system users, processes acting on behalf of users, or devices. | |
| **Implementation Details:**  **< REPLACE HIGHLIGHTED TEXT WITH YOUR DOCUMENTATION**  Documentation should include:   * Processes and controls used to confirm the identity of users, processes, or devices before allowing them to access information systems. (*Ex: Unique UW NetID (username and password) accounts are assigned to all UW employees and are required to access all departmental computer systems.* Shared accounts by individuals should only be used when individual accounts cannot be used. (See Risk Advisory: The Use of Shared Accounts by Individuals on the CISO web site for more information) * Processes and controls used to limit access to specific systems from other systems. (Can be accomplished using unique system identifiers such as media access control addresses (MAC address) or IP addresses.) * Process and controls associated with service accounts in use for automatic service processing. System account credentials should be kept secret and safe. Auditing and logging should be in place to track when accounts are accessed by individuals.   *UW Services that could be leveraged to satisfy control requirements include\*:*   * *Active Directory, Azure AD* * *DUO (2-Factor Authentication)* * *Kerberos* * *UW NetID* * *Web SSO*   \**List of services may not be complete or applicable for a given configuration. The use of a given service does not necessarily satisfy control requirements or may require specific configuration to meet control requirements. Documentation should include how the service is implemented to meet the control requirements. >* | |

| IA.1.077 | Practice |
| --- | --- |
| Practice: Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems. | |
| **Implementation Details:**  **< REPLACE HIGHLIGHTED TEXT WITH YOUR DOCUMENTATION**  Documentation should include:   * Processes and controls used to confirm that a user or device is who or what it claims to be before granting access to information systems. (Ex: *Ex: Unique UW NetID (username and password) accounts are assigned to all UW employees and are required for accessing all departmental computer systems. Duo two-factor authentication is required to verify a user’s identity before they can access information systems with sensitive information.)* * Processes and controls used to limit access to specific systems from other systems. (Can be accomplished using unique system identifiers such as media access control addresses (MAC address) or IP addresses.) * Process and controls associated with service account passwords in use for automatic service processing. System account credentials should be kept secret and safe. Auditing and logging should be in place to track when such accounts are accessed by individuals and passwords changed if known by individuals who no longer need access. * Process for changing default passwords on devices are changed to unique strong passwords before deployment.   *UW Services that could be leveraged to satisfy control requirements include\*:*   * *Active Directory, Azure AD* * *DUO (2-Factor Authentication)* * *Kerberos* * *UW NetID* * *Web SSO*   \**List of services may not be complete or applicable for a given configuration. The use of a given service does not necessarily satisfy control requirements or may require specific configuration to meet control requirements. Documentation should include how the service is implemented to meet the control requirements. >* | |

### Media Protection – C024

| Capability | |
| --- | --- |
| ID | C024 |
| Description | Sanitize media. |

| MP.1.118 | Practice |
| --- | --- |
| Practice: Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse. | |
| **Implementation Details:**  **< REPLACE HIGHLIGHTED TEXT WITH YOUR DOCUMENTATION**  Documentation should include:   * Methods for sanitizing all media containing FCI before the media is reused (Ex: redeploying a computer) or disposed. Applies to all media, including digital (soft copy; hard drives, tapes, CDs, DVDs, mobile phones, etc.) and non-digital (hard copy; paper, microfilm, etc.). Sanitization removes information from the media or alters the media in a way such that the information may not be retrieved or reconstructed. Sanitization methods for digital media include cryptographic erase or physical destruction to prevent the disclosing of sensitive information. Sanitization methods for non-digital media include shredding or removing FCI and CUI from redacted sections or words in a manner equivalent to removing the words or sections from the document.   For more information, please see NIST Special Publication 800-88, Revision 1, Guidelines for Media <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf>  *UW Services that could be leveraged to satisfy control requirements include\*:*   * *UW Surplus Disposal*   \**List of services may not be complete or applicable for a given configuration. The use of a given service does not necessarily satisfy control requirements or may require specific configuration to meet control requirements. Documentation should include how the service is implemented to meet the control requirements. >* | |

## PHYSICAL PROTECTION (PE)

### Physical Protection – C028

| Capability | |
| --- | --- |
| ID | C028 |
| Description | Limit physical access. |

| PE.1.131 | Practice |
| --- | --- |
| Practice: Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals. | |
| **Implementation Details:**  **< REPLACE HIGHLIGHTED TEXT WITH YOUR DOCUMENTATION**  Documentation should include:   * Processes and controls used to limit physical access to information systems and their operating environments. (*Ex: Servers that store sensitive information are located in a room that requires an electronic key card to access. Key cards are assigned only to authorized individuals. Access is audited regularly and removed when no longer needed. Department workstations are contained within a large office that requires a key card to access. Only departmental staff have access. Access is removed as part of the off-boarding process.)* * Process and controls used to limit physical access to hard and soft copies of sensitive information. *(Ex: Printouts, CDs, and thumb drives with sensitive information are stored in a locked cabinet within a locked office. Keys are held by the Director and staff must request approval to gain access.)*   *UW Services that could be leveraged to satisfy control requirements include\*:*   * *Data Center Co-location Services* * *Router Room Co-location Services*   \**List of services may not be complete or applicable for a given configuration. The use of a given service does not necessarily satisfy control requirements or may require specific configuration to meet control requirements. Documentation should include how the service is implemented to meet the control requirements. >* | |

| PE.1.132 | Practice |
| --- | --- |
| Practice: Escort visitors and monitor visitor activity. | |
| **Implementation Details:**  **< REPLACE HIGHLIGHTED TEXT WITH YOUR DOCUMENTATION**  Documentation should include:   * Processes and controls used to ensure that visitors and guest activities are authorized and monitored. *(Ex: All visitors must be accompanied by a staff worker. Visitors are assigned a visitor’s badge that must be worn and visible at all times. Staff are required to question unaccompanied visitors in restricted areas to ensure that they are authorized to be there. Unaccompanied visitator access is reported as an incident to the department manager.) >* | |

| PE.1.133 | Practice |
| --- | --- |
| Practice: Maintain audit logs of physical access. | |
| **Implementation Details:**  **< REPLACE HIGHLIGHTED TEXT WITH YOUR DOCUMENTATION**  Documentation should include:   * Processes and controls used to log the physical access to systems containing FCI and CUI and areas that house those systems; A record of who is accessing both your facility and your equipment. Logs are required for both staff and visitors. Audit logs can be procedural (Ex: sign-in sheets used when individual access the facility, office, or locked cabinet) automated (Ex: Personal Identity Verification (PIV) key card), or a combination of both.   *UW Services that could be leveraged to satisfy control requirements include\*:*   * *Data Center Co-location Services* * *Router Room Co-location Services*   \**List of services may not be complete or applicable for a given configuration. The use of a given service does not necessarily satisfy control requirements or may require specific configuration to meet control requirements. Documentation should include how the service is implemented to meet the control requirements. >* | |

| PE.1.134 | Practice |
| --- | --- |
| Practice: Control and manage physical access devices. | |
| **Implementation Details:**  **< REPLACE HIGHLIGHTED TEXT WITH YOUR DOCUMENTATION**  Documentation should include:   * Processes for managing physical access devices such as key cards, badges, keys/locks, etc. *(Ex: Staff are issued keycards that provide access to electronically locked areas. UW Facilities manages keycard building access via Campus Automated Access Management System. Offboarded employees are required to turn in their cards. Mangers can also request that key-card access for an individual be removed when an employee no longer needs access to a specific area or is terminated.)*   *UW Services that could be leveraged to satisfy control requirements include\*:*   * *Data Center Co-location Services* * *Router Room Co-location Services* * *Key requests: UW Housing Desk Services, UW Building Coordinators, UW Lock Shop* * *Key Cards: UW Facilities Campus Automated Access Management System (CAAMS)*   \**List of services may not be complete or applicable for a given configuration. The use of a given service does not necessarily satisfy control requirements or may require specific configuration to meet control requirements. Documentation should include how the service is implemented to meet the control requirements. >* | |

### System and Communications Protection – C039

| Capability | |
| --- | --- |
| ID | C039 |
| Description | Control communications at system boundaries |

| SC.1.175 | Practice Information |
| --- | --- |
| Practice: Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems. | |
| **Implementation Details:**  **< REPLACE HIGHLIGHTED TEXT WITH YOUR DOCUMENTATION**  Documentation should include:   * Technical controls used to limit connections at boundaries to only authorized systems and/or processes. Components include gateways, routers, firewalls, guards, and network-based malicious code analysis. *(Ex. All departmental computer systems that store FCI or CUI use private IP addresses on a designated subnet and are behind a managed firewall that blocks all traffic from the internet and all other subnets by default. External connections to internal systems require a specific firewall exception. Connection logs are available for review as needed. An Intrusion Prevention System managed by UW IT is located in front of the managed firewall at the outside perimeter of the network.)*   *UW Services that could be leveraged to satisfy control requirements include\*:*   * *Managed Firewall Service* * *Private Address Routing* * *Husky OnNet VPN / HON-D VPN* * *Intrusion Prevention System* * *Network Monitoring* * *Splunk* * *Azure Security Portals, Azure Express Route*   \**List of services may not be complete or applicable for a given configuration. The use of a given service does not necessarily satisfy control requirements or may require specific configuration to meet control requirements. Documentation should include how the service is implemented to meet the control requirements. >* | |

| SC.1.176 | Practice |
| --- | --- |
| Practice: Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks. | |
| **Implementation Details:**  **< REPLACE HIGHLIGHTED TEXT WITH YOUR DOCUMENTATION**  Documentation should include:   * Technical controls used to separate publicly accessible systems from internal systems that need to be protected. Publicly accessible systems can be placed within Demilitarized Zones (DMZs) that separate external networks (Ex: internet) from internal networks. This helps to ensure that if a publicly accessible system is compromised, the attacker cannot easily gain access to the internal network. Boundary control devices can include routers, gateways, firewalls, or cloud networks that are separate from the rest of the network. A physical separation may utilize a dedicated infrastructure that employs a firewall between the internal network and the DMZ and a second firewall between the DMZ and the internet. Logical separations may include VLAN segmentation to create a DMZ between external and internal networks using a firewall and routing controls between subnets.   *UW Services that could be leveraged to satisfy control requirements include\*:*   * *Managed Firewall Service* * *Private Address Routing* * *UW IT Enterprise Intrusion Prevention System (IPS)*   \**List of services may not be complete or applicable for a given configuration. The use of a given service does not necessarily satisfy control requirements or may require specific configuration to meet control requirements. Documentation should include how the service is implemented to meet the control requirements. >* | |

## SYSTEM AND INFORMATION INTEGRITY (SI)

### System and Information Integrity – C040

| Capability | |
| --- | --- |
| ID | C040 |
| Description | Identify and manage information system flaws. |

| SI.1.210 | Practice |
| --- | --- |
| Practice: Identify, report, and correct information and information system flaws in a timely manner. | |
| Implementation Details:  **< REPLACE HIGHLIGHTED TEXT WITH YOUR DOCUMENTATION**  Documentation should include:   * Technical controls that ensure vulnerability awareness for systems and software. (*Ex: Automated credentialed vulnerability scans are conducted monthly on departmental systems to identify both operating system and application vulnerabilities.*) * Technical controls used to ensure system and software flaw remediations are applied in a timely matter, and without adversely affecting the department or organization. *(Ex. Workstations are centrally managed using Windows System Center Configuration Manager and are configured to download and install updates automatically when made available by Microsoft. Windows production servers are configured to auto-install security updates once a month during a designated maintenance window after patches have been tested and verified on the test and development systems. Anti-virus software is installed on all systems and configured to auto update.)* * Non-technical processes used to ensure awareness of system and software vulnerabilities. *(Ex: The software vendor or automatically notifies us when application and security updates are available. The department subscribes to the Office of the CISO’s Weekly Cyber Intelligence Report (contact the CISO’s office for details).* * Non-technical processes used to ensure system and software flaw remediations are applied in a timely matter, and without adversely affecting the department or organization. *(Ex: Vulnerability scan reports are reviewed monthly to ensure systems are being patched regularly, and to identify updates or security patches that 1) Need to be installed ahead of the scheduled maintenance window, 2) Warrant further review and testing before installing 3) Deemed as deferrable or an acceptable risk if certain criteria is met, which may include alternate mitigation strategies.)*   *UW Services that could be leveraged to satisfy control requirements include\*:*   * *Managed Workstation Service* * *Managed Server Service* * *Services and Systems Monitoring* * *Splunk* * *Backups* * *Azure Security Center* * *Anti-virus*   \**List of services may not be complete or applicable for a given configuration. The use of a given service does not necessarily satisfy control requirements or may require specific configuration to meet control requirements. Documentation should include how the service is implemented to meet the control requirements. >* | |

### System and Information Integrity – C041

| Capability | |
| --- | --- |
| ID | C041 |
| Description | Identify malicious content. |

| SI.1.211 | Practice |
| --- | --- |
| Practice: Provide protection from malicious code at appropriate locations within organizational information systems. | |
| **Implementation Details:**  **< REPLACE HIGHLIGHTED TEXT WITH YOUR DOCUMENTATION**  Documentation should include:   * Technical controls used to prevent, detect and mitigate malicious code. Malicious code is code created to carry out an unauthorized function process that may compromise the confidentiality, integrity, or availability of an information system, or data stored on an information system. Detection and protection locations can include firewalls, web servers, proxy servers, servers, workstations, and mobile devices. (*Ex: Antivirus software and Microsoft Sysmon is installed on all departmental servers and workstations. Group policy settings applied using DoD Security Technical Implementation Guides (STIGs) Windows and Mac built-in firewalls are enabled on all systems. Known malicious web sites are blocked at the perimeter firewall.)*   *UW Services that could be leveraged to satisfy control requirements include\*:*   * *Anti-virus* * *Email Infrastructure Service* * *Intrusion Prevention System* * *Azure Security Center* * *Active Directory Group Policy*   \**List of services may not be complete or applicable for a given configuration. The use of a given service does not necessarily satisfy control requirements or may require specific configuration to meet control requirements. Documentation should include how the service is implemented to meet the control requirements. >* | |

| SI.1.212 | Practice |
| --- | --- |
| Practice: Update malicious code protection mechanisms when new releases are available. | |
| **Implementation Details**:  **< REPLACE HIGHLIGHTED TEXT WITH YOUR DOCUMENTATION**  Documentation should include:   * Technical controls used to protect against malicious code are kept up to date when product updates are available. *(Ex. Anti-virus software on all systems is configured to automatically check for and install updates and new definition files. Operating systems are configured to automatically download and install security patches. Workstations are centrally managed using Windows System Center Configuration Manager and are configured to download and install updates automatically when made available by Microsoft. Windows production servers are configured to auto-install security updates once a month during a designated maintenance window after patches have been tested and verified on the test and development systems. Mac workstations are configured to automatically download and install security updates when they are made available.)*   *UW Services that could be leveraged to satisfy control requirements include\*:*   * *Anti-virus* * *Email Infrastructure Service* * *Intrusion Prevention System* * *Managed Workstation Service* * *Managed Server Service*   \**List of services may not be complete or applicable for a given configuration. The use of a given service does not necessarily satisfy control requirements or may require specific configuration to meet control requirements. Documentation should include how the service is implemented to meet the control requirements. >* | |

| SI.1.213 | Practice |
| --- | --- |
| Practice: Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed. | |
| **Implementation Details:**  **< REPLACE HIGHLIGHTED TEXT WITH YOUR DOCUMENTATION**  Documentation should include:   * Technical controls used to carry out scans to detect malicious code on systems and files. *(Ex: Office 365 is configured to automictically scan email attachments for malicious code. Antivirus installed on all departmental systems is configured to perform quick scans daily, full system scans weekly, and to inspect all downloaded files automatically before they are opened.)*   *UW Services that could be leveraged to satisfy control requirements include\*:*   * *Anti-virus* * *Email Infrastructure Service* * *Intrusion Prevention System* * *Azure Security*   \**List of services may not be complete or applicable for a given configuration. The use of a given service does not necessarily satisfy control requirements or may require specific configuration to meet control requirements. Documentation should include how the service is implemented to meet the control requirements. >* | |

**Appendix**

**Detailed System Inventory**

<Detailed system inventory can be recorded in a separate document that is referenced here.>

| System Name | IP Address | Hostname | Platform (OS and Version) | Physical, Virtual, Other (ex: SaaS) | Location |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

# External Service Providers

<If external service providers are leveraged to operate or maintain a system, record the information below and where applicable throughout this document. >

‑

| System Name | Service Provider | Contact Information |
| --- | --- | --- |
|  |  |  |
|  |  |  |