# Maturity Level 1 Controls

All Maturity Level  Controls must be documented in the System Security Plan.

| | | |
|---|---|---|
| **ACCESS CONTROL (AC)** | | |
| Practices | | |
| 1.001 Limit information systems access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).<br>1.002 Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | AC-2 | Account Management |
| | AC-3 | Access Enforcement |
| | AC-17 | Remote Access |
| 1.003 Verify and control/limit connections to and use of external information systems. | AC-20 | Use of External Information Systems |
| | AC-20(1) | Use of External Information Systems<br>Limits on Authorized Use |
| 1.004 Control information posted or processed on publicly accessible information systems. | AC-22 | Publicly Accessible Content |
| **IDENTIFICATION AND AUTHENTICATION (IA)** | | |
| Practices | | |
| 1.076 Identify information system users, processes acting on behalf of users, or devices | IA-2 | Identification and Authentication (Organizational Users) |
| 1.077 Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems | IA-5 | Authenticator Management |
| **MEDIA PROTECTION (MP)** | | |
| Practices | | |
| 1.118 Sanitize or destroy information system media containing CUI before disposal or release for reuse | MP-6 | Media Sanitization |
| **PHYSICAL ENVIRONMENT (PE)** | | |
| Practices | | |
| 1.131 Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals | PE-2 | Physical Access Authorizations |
| 1.132 Escort visitors and monitor visitor activity | PE-3 | Physical Access Control |

| | | |
|---|---|---|
| 1.133 Maintain audit logs of physical access | PE-3 | Physical Access Control |
| 1.134 Control and manage physical access devices | PE-3 | Physical Access Control |
| **SYSTEM AND COMMUNICATIONS PROTECTION (SC)** | | |
| Practices | | |
| 1.175 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 organizational system | SC-7 | Boundary Protection |
| 1.176 Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks | SC-7 | Boundary Protection |
| **SYSTEM AND INFORMATION INTEGRITY (SI)** | | |
| Practices | | |
| 1.210 Identify, report, and correct information and information system flaws in a timely manner | SI-2 | Flaw Remediation |
| 1.211 Provide protection from malicious code at appropriate locations within organizational systems | SI-3 | Malicious Code Protection |
| 1.212 Update malicious code protection mechanisms when new releases are available | N/A | |
| 1.213 Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed | SI -3 | Malicious Code Protection |

# Maturity Level 1 Controls Implementation SAMPLE

| **ACCESS CONTROL (AC)** | | | |
|---|---|---|---|
| Practices Security Requirements | | | Implementation Status (check all that apply):<br>☐ I=Implemented<br>☐ PI=Partially implemented.<br>☐ P=Planned.<br>☐ AI=Alternative implementation.<br>☐ N/A=Not applicable |
| 1.001 Limit information systems access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).<br>1.002 Limit information system access to the types of transactions and functions that authorized users are permitted to execute. | AC-2 | Account Management | ☐ I=Implemented<br>The Program is responsible to identify all accounts within the system, establish role and group membership criteria (if needed), to establish the authorization process, to approve users, to monitor all accounts, notifying all managers when account is terminated or transferred, and to authorize access. |
| | AC-3 | Access Enforcement | ☐ I=Implemented<br>The Program is responsible to enforce approved authorizations for access. |
| | AC-17 | Remote Access | ☐ N/A=Not applicable<br>The Program does not allow remote access. |
| 1.003 Verify and control/limit connections to and use of external information systems. | AC-20 | Use of External Information Systems | ☐ N/A=Not applicable<br>The Program does not allow access to external systems. |
| | AC-20(1) | Use of External Information Systems<br>Limits on Authorized Use | ☐ N/A=Not applicable<br>The Program does not allow access to external systems. |
| 1.004 Control information posted or processed on publicly accessible information systems. | AC-22 | Publicly Accessible Content | ☐ N/A=Not applicable<br>The Program boundary does not include publicly accessible content. |

| | | | |
|---|---|---|---|
| **IDENTIFICATION AND AUTHENTICATION (IA)** | | | |
| Practice Security Requirements | | | |
| 1.076 Identify information system users, processes acting on behalf of users, or devices | IA-2 | Identification and Authentication (Organizational Users) | ☐ I=Implemented<br>The Program users are uniquely identified via username and password prior to accessing the system. |
| 1.077 Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems | IA-5 | Authenticator Management | ☐ I=Implemented<br>The Program utilizes unique individual user accounts and passwords to authenticate to the system. |
| **MEDIA PROTECTION (MP)** | | | |
| Practice Security Requirements | | | |
| 1.118 Sanitize or destroy information system media containing CUI before disposal or release for reuse | MP-2 | Media Access | ☐ N/A = Not Applicable<br>The Program does not hold any CUI |
| **PHYSICAL PROTECTION (PE)** | | | |
| Practice Security Requirements | | | |
| 1.131 Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals | PE-2<br>PE-5 | Physical Access Authorizations /Access Control for Output Devices | ☐ I=Implemented<br>The Program limits physical access to authorized individuals |
| 1.132 Escort visitors and monitor visitor activity | PE-3 | Physical Access Control | ☐ I=Implemented<br>The Program escorts visitors and monitors visitor activity. |
| 1.133 Maintain audit logs of physical access. | | | ☐ I=Implemented<br>The Program maintains audit logs of physical access |
| 1.134 Control and manage physical access devices. | PE-3 | Physical Access Control | ☐ I=Implemented<br>The Program controls and manages physical access to devices. |

| SYSTEM AND COMMUNICATIONS PROTECTION | | | |
|---|---|---|---|
| Practice Security Requirements | | | |
| 1.175 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 | SC-7<br>SA-8 | Boundary Protection /Security Engineering Principles | ☐ I=Implemented<br>The Program is controlled at the external boundary by a firewall and boundary protection. |
| 1.176 Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks. | SC-7 | Boundary Protection | ☐ N/A = Not Applicable<br>The Program has no publicly accessible components. |

| SYSTEM AND INFORMATION INTEGRITY (SI) | | | |
|---|---|---|---|
| Practice Security Requirements | | | |
| 1.210 Identify, report, and correct information and information system flaws in a timely manner. | SI-2 | Flaw Remediation | ☐ I=Implemented<br>The Program uses manual and automated scans and checks to determine system flaws. ACAS scanning, SCAP scans, STIG checklists are completed quarterly at a minimum. System flaws are tracked in The Program POA&M. |
| 1.211 Provide protection from malicious code at appropriate locations within organizational information systems. | SI-3 | Malicious Code Protection | ☐ I=Implemented<br>The Program is protected by malicious code by using only COTS products. |
| 1.212 Update malicious code protection mechanisms when new releases are available. | SI-3 | Malicious Code Protection | ☐ I=Implemented<br>The Program is protected by malicious code by using only COTS products and Vulnerability and Code Review scans. |
| 1.213 Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed. | SI-3 | Malicious Code Protection | ☐ I=Implemented<br>The Program is protected by malicious code by using only COTS products and Vulnerability and Code Review scans. |