1 PURPOSE

This Standard aims to establish procedures and policies for CMMC (Cybersecurity Maturity Model Certification). It is a certification program created by the Department of Defense (DoD) that assesses an organization's cybersecurity posture. As a Department of Defense partner, USNH had identified a need to achieve at least Level 1 certification within the Cybersecurity Maturity Model Certification (CMMC) V1.0.

2 SCOPE

This standard applies to all USNH business and academic units and USNH-owned information systems that collect, store, process, share or transmit CMMC related data. CMMC is a unified standard that takes into account the various information security standards and best practices that need to be implemented within the defense industrial base supply chain to protect federal contract information (FCI) and controlled unclassified information (CUI). There are no Processes required to be documented within Level 1, only Practices. This standard focuses on Level 1 certification within the Cybersecurity Maturity Model Certification (CMMC) V2.0 for FCI related information. Both CUI (Controlled Unclassified Information) and FCI (Federal Contract Information) include information created or collected by or for the Government, as well as information received from the Government. However, while FCI is any information that is “not intended for public release,” CUI is information that requires safeguarding and may also be subject to dissemination controls. Both CUI and FCI are considered unclassified, but still sensitive information that requires a certain level of safeguards. For Level 2/CUI related issues, please refer to the CYBERSECURITY MATURITY MODEL CERTIFICATION STANDARD V2.0 LEVEL 2 Standard.

3 AUDIENCE
All USNH community members who access USNH CMCC Version 2.0 Level 1 related data and resources. Organizations seeking Level 1 requirements will not require 3rd party certification. Instead, the grant administrator must specify the people, technology, facilities, and external providers within their environment that process, store or transmit FCI. Organizations will be required to self-certify once per year that they meet the basic safeguarding requirements for FCI specified in FAR clause 52.204.21. There are 17 practices and an annual self-assessment for certification. This is for organizations with FCI only. These controls look to protect covered contractor information systems, limit access to authorized users.

4 STANDARD FOR CMMC V2.0 LEVEL ONE

4.1 ACCESS CONTROL (AC) domain focuses on the tracking and understanding of who has access to your systems and network. This includes user privileges, remote access, and internal system access.

- AC.1.001 - aligns to NIST SP 800-171 Rev 2 3.1.1 - Authorized Access Control - Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).
- AC.1.002 - aligns to NIST SP 800-171 Rev 2 3.1.2 - Transaction & Function Control - Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
- AC.1.003 - aligns to NIST SP 800-171 Rev 2 3.1.20 - External Connections - Verify and control/limit connections to and use of external information systems.
- AC.1.004 - aligns to NIST SP 800-171 Rev 2 3.1.22 – Control Public Information - Control information posted or processed on publicly accessible information systems.

4.2 IDENTIFICATION AND AUTHENTICATION (IA) domain focuses on the roles within your organization. It synergizes with the AC by ensuring that access to all systems and networks is traceable for reporting and accountability.

- IA.1.076 - aligns to NIST SP 800-171 Rev 2 3.5.1 – Identification - Identify information system users, processes acting on behalf of users, or devices.
- IA.1.077 - aligns to NIST SP 800-171 Rev 2 3.5 - Authenticate - Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

4.3 MEDIA PROTECTION (MP) focuses on identifying, tracking and ongoing maintenance of media. It also includes policies about protection, data sanitation and acceptable transportation.
4.4 PHYSICAL PROTECTION (PE) is often an overlooked domain for many organizations. Sure, most places implement a sign-in process, requiring card reader identification and access to certain portions of their location. Yet not every organization supervises its visitors throughout their entire stay. PE helps organizations with that.

- PE.1.131 - aligns to NIST SP 800-171 Rev 2 3.10.1 - Limit physical access - Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.
- PE.1.132 - aligns to NIST SP 800-171 Rev 2 3.10.3 - Escort Visitors - Escort visitors and monitor visitor activity.
- PE.1.133 - aligns to NIST SP 800-171 Rev 2 3.10.4 - Physical Access Logs - Maintain audit logs of physical access.
- PE.1.134 - aligns to NIST SP 800-171 Rev 2 3.10.5 - Manage Physical Access - Control and manage physical access devices.

4.5 SYSTEM AND COMMUNICATION PROTECTION (SC) is an integral part of every organization. That communication between employees needs to be secure so that no bad actor may eavesdrop and record sensitive data. The System and Communication Protection (SC) domain focuses on the implementation of boundary level defense on an organizational communication level.

- SC.1.175 - aligns to NIST SP 800-171 Rev 2 3.13.1 - Boundary Protection - 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 1.176 - aligns to NIST SP 800-171 Rev 2 3.13 - Public-Access System Separation - Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

4.6 SYSTEM AND INFORMATION INTEGRITY (SI). This domain focuses on the ongoing maintenance and management of issues within information systems. In other words, it enforces that organizations place efforts toward identifying malicious code, placing ongoing protections on email and system monitoring.

- SI.1.210 - aligns to NIST SP 800-171 Rev 2 3.14. - Flaw Remediation - Identify, report, and correct information and information system flaws in a timely manner.
• SI.1.211 - aligns to NIST SP 800-171 Rev 2 3.14.2 - Malicious Code Protection - Provide protection from malicious code at appropriate locations within organizational information systems.

• SI.1.212 - aligns to NIST SP 800-171 Rev 2 3.14.4 - Update Malicious Code Protection - Update malicious code protection mechanisms when new releases are available.

• SI.1.213 - aligns to NIST SP 800-171 Rev 2 3.14.5 - System & File Scanning - Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

5 MAINTENANCE OF PROCESSES AND PROCEDURES RELATED TO THIS STANDARD

As part of the mandatory annual review of this Standard required by the USNH Cybersecurity Policy, the processes and procedures that support the requirements defined in this Standard shall be reviewed and, where needed, updated to ensure currency and continuous improvement.

6 ENFORCEMENT

Failure to comply with this Policy puts the University System, its component institutions, and its information and information technology resources at risk and may result in disciplinary action. Disciplinary procedures will be appropriate for the individual responsible for non-compliance (e.g., students, faculty, staff, vendors) as outlined in the relevant institutional regulations for that individual (e.g., student conduct and/or applicable personnel policies).

Non-compliant technology and/or activities may be mitigated as deemed necessary by the CISO and/or CIO.

Employees who are members of institutionally recognized bargaining units are covered by the disciplinary provisions set forth in the agreement for their bargaining units.

CONTACT INFORMATION

For USNH community members: Questions about this Standard, requests for additional information or
training, or reports of violations can be directed to Cybersecurity Governance, Risk, and Compliance (GRC) via this Support Form.

All other requests can be submitted here: Submit an IT Question.

---

DOCUMENT HISTORY

<table>
<thead>
<tr>
<th>Effective Date:</th>
<th>December 16, 2022</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approved by:</td>
<td>Dr. David A Yasenchock, Interim CIO</td>
</tr>
<tr>
<td>Reviewed by:</td>
<td>Dr. David A Yasenchock, Director, Cybersecurity GRC</td>
</tr>
<tr>
<td>Revision History:</td>
<td>V 1.00</td>
</tr>
</tbody>
</table>