



USNH CYBERSECURITY COMMITTEE CHARTER

Responsible Executive/University System Officer: Chief Information Security Officer

Responsible Office: ET&S Cybersecurity GRC

Approved Distribution: Public

Status: APPROVED

1. CYBERSECURITY COMMITTEE CHARTER

As adopted by the Office of the CIO on January 7, 2022. This Cybersecurity Committee Charter for the University System of New Hampshire has been adopted.

2. PURPOSE AND POLICY

The Cybersecurity Committee's primary purpose shall be to act on behalf of the USNH Board in fulfilling the Board's cybersecurity oversight responsibility with respect to USNH's information technology use and protection of its data. The operation of the Committee shall be subject to the Bylaws of the USNH.

3. COMPOSITION

The Committee shall consist of at least two (2) Chairs as a primary (CISO) and as alternate chairs (Director of Cybersecurity GRC). The Committee will include at least 5 members across the USNH community that have expertise in cybersecurity issues that include: faculty, staff, legal, and student populations. The Committee can appoint Committee members, fill vacancies occurring on the Committee.

4. MEETINGS AND MINUTES

The Committee shall hold such regular or special meetings as its members shall deem necessary or appropriate. Minutes of each meeting of the Committee shall be prepared and distributed to each member of the committee and several stakeholders as identified by the committee as well as posted on ETS secure teams site.

5. AUTHORITY

The USNH Cybersecurity Committee is committed to working with USNH community to monitor developments and effectively respond to cyber threats. In exercising its oversight responsibilities, the Committee may inquire into any matter that it considers to be of material concern to the Committee or the Board. The Committee shall have authority to recommend or authorize audits into any matters within the scope of its responsibilities and the authority, in its sole discretion, to select, retain and obtain the advice of outside counsel, cybersecurity or other advisors or consultants as it deems appropriate.

6. RESPONSIBILITIES AND GOALS

The Committee shall be responsible for the following:

- Data Governance – To provide oversight of policies, procedures, plans, and execution intended to provide security, confidentiality, availability, and integrity of the information.
- Cybersecurity Posture of Information Technology Systems – To oversee the quality and effectiveness of the USNH’s policies and procedures with respect to its cybersecurity posture of information technology systems, including privacy, network security and data security.
- Cybersecurity Incident Response – To review and provide oversight on the policies and procedures of USNH in preparation for responding to any material incidents.
- Cybersecurity Compliance Risks – To oversee USNH’s management of cybersecurity risks related to its information technology systems and processes, including privacy, network security and data security, and any internal audits of such systems and processes.
- Periodic and Annual Reports – To review and oversee the preparation of USNH’s annual cybersecurity risk assessment and disclosures in its reports filed with various agencies as required by law in respect to USNH’s information technology systems, including privacy, network security, and data security.
- IT/Engineering Security Budget – Review USNH’s information technology procurement relating to budgetary priorities based, in part, on assessing risk associated with various perceived threats.
- Advisory Role – To review the USNH’s information technology strategy or programs relating to new technologies, applications, and systems.
- Standing Members – CISO, Director of GRC, Legal/Privacy Council, Faculty Representative from ITC, and a Student Representative from a Technology Program.

7. DOCUMENT HISTORY

Effective Date: 7 January 2022

Drafted: Dr. David Yasenchock, Director Cybersecurity GRC, 7 January 2022

Revised, USNH Cybersecurity GRC Standards Committee, 7 January 2022

Reviewed by: Dr. David Yasenchock, Director Cybersecurity 7 January 2022

Approved by: Thomas Nudd, Chief Information Security Officer, 7 January 2022