Additionally, all USNH employees participate in the USNH Phishing Awareness Program outlined below.

Employees whose responsibilities require interaction with certain types of institutional information as well as those with specific cybersecurity responsibilities shall be required to complete role-specific cybersecurity training courses. Managers in administrative, academic, and business units with cybersecurity role-based training requirements are responsible for notifying Cybersecurity GRC when new employees join the unit. Managers of these units shall provide a current list of employees, annually, to facilitate completion of training requirements.

Although specific required frequencies are defined for each role-based training requirement, substantial chang

Computer-Based Training
Confidentiality
Cybersecurity
Exception
Gramm Leach Bliley Act (GLBA)
Health Insurance Portability and Accountability Act (HIPAA)
Information
Information Security
Information Technology Resource
Institutional Information
Integrity
Out of Band
PCI-DSS
Phishing
Policy
Standard
Susceptible
USNH Community Member
Waiver

USNH Cybersecurity Policy
Cybersecurity Exception Standard

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.

EffectiveDate:	19 AUG 2021
Approved by:	CHIEF INFORMATION SECURITY OFFICER, T NUDD, 19 AUG 2021 v1