

Enterprise Technology & Services Confidentiality and Cybersecurity Agreement

The purpose of this agreement is to codify the responsibilities of all ET&S employees, sponsored users, and student workers for maintaining the confidentiality, integrity, availability, and privacy of institutional information and information technology resources. The following agreement is between you and USNH, on behalf of its component institutions.

An employee, sponsored user, or student worker of USNH or one of its component institutions may, related to their job responsibilities or assigned tasks within ET&S, have access to or come in contact with institutional information that is not classified as Public Information (e.g., personally identifiable information, medical and research data, password protected information, security parameters and configurations, system logs and network traffic data). Use of this information is subject to USNH and component institution policies and standards, as well as special handling requirements dictated by local, state, and federal laws and regulations, industry group mandates, or grant terms.

Your signature below indicates that you understand all portions of this agreement and agree to the following:

1. I accept responsibility for appropriate handling and management of institutional information whether I come into contact with such information through my authorized access or in error.
 - a. I will only access institutional information and information technology resources for legitimate business purposes as permitted by USNH and its component institutions, as is appropriate for my role, and for the purposes intended when that access was granted.
 - b. I will not allow anyone else to use my access or allow others to access the institutional information or information technology resources I have been granted access to, unless I am explicitly authorized to provide such access to others as part of my role.
 - c. I will not download or extract any institutional information from the official secured USNH or institutional source systems or storage mechanisms, outside of standard business practices, to any external or removable storage mechanism, including documents (physical and electronic) unless storage of that information in that format has been explicitly approved by a member of the ET&S Leadership team (Orchestrator and above) in writing.
 - d. I will not use any institutional information, regardless of its classification, for personal use.
 - e. I will not leave institutional information in view of others who are not authorized to access or view that information.
 - f. I will not misuse my knowledge about USNH, its institutional information, and/or its information technology resources or environment to facilitate damage of or inappropriate access to institutional information and information technology resources, while I am a member of ET&S or after my affiliation with ET&S, USNH, or any of its component institutions ends.

- g. I am responsible for ensuring I understand how information is classified at USNH and for knowing the classification of all institutional information I use, manage, or interact with as part of my role.
 - h. I am responsible for understanding and following handling requirements for any institutional information I use, manage, or interact with as part of my role.
2. I will maintain the confidentiality of this information and the privacy of individual community members consistent with [USNH, Institution \(GSC, KSC, PSU, UNH\) and ET&S policies](#).
- a. I will only share institutional information with individuals who are authorized to access or view that information.
 - b. If I am uncertain about the appropriateness of who this information may be shared with, I will discuss any questions I have with my supervisor or the Cybersecurity & Networking team.
 - c. I understand that even the most innocuous file can contain information that must be kept confidential.
3. I will report all potential or confirmed Cybersecurity Incidents, as defined in the USNH ET&S glossary of terms, using the USNH Cybersecurity Incident Reporting procedure, both of which are available on the [USNH Enterprise Cybersecurity website](#).
- a. I am responsible for understanding how to identify a [Cybersecurity Incident](#) and for reporting any condition that has the potential for institutional information or information technology resources to be accessed, modified, compromised, or destroyed inappropriately and/or by unauthorized persons or processes.
 - b. I am responsible for understanding the USNH Cybersecurity Incident procedures appropriate to my role and my responsibilities during a Cybersecurity Incident.

In all instances as described above, I acknowledge my personal obligation to protect the confidentiality, integrity, availability, and privacy of this information in accordance with USNH policies and standards, regulatory or legal requirements, and/or other special handling requirements, and prevent unauthorized access, modification, destruction, or disclosure of institutional information. In the absence of stated guidance or without a clear indication of sensitivity, I will treat and handle all institutional information as if it is legally protected.

Intentional violations of this agreement may result in disciplinary action, up to and including termination of employment, suspension and loss of privileges, termination of authorization to work with institutional information, as well as possible legal sanctions.

University System of New Hampshire

I (please print name) _____ have read and understand this agreement and will abide by it for the duration of my affiliation with Enterprise Technology & Services (ET&S).

Signature _____ Date _____