University System of New Hampshire

# ACCESS TO PASSWORD-PROTECTED INFORMATION STANDARD

**Responsible Executive/University System Officer:** Chief Information Security Officer
**Responsible Office:** ET&S Cybersecurity GRC
**Approved Distribution:** Public
**Status:** IN FORCE

## 1. PURPOSE

This standard shall establish the requirements and define the processes that apply when a USNH entity or non-community member seeks access to or disclosure of any electronic information that can only be accessed using a specific community member's USNH credentials. Additionally, the standard specifies the circumstances that information may be accessed and/or disclosed without the community member's consent.

## 2. SCOPE

This standard applies to:

- Requests for access to or disclosure of information stored in USNH information technology resources accessible with a specific community members' USNH credentials or by the administrators of that resource.
- All information, including both institutional and personal, is captured, stored, processed, transmitted, or otherwise managed by a USNH information technology resource.
- All community members - internal or external to USNH seeking access or disclosure of the information described in this standard are subject to the requirements and processes defined.

Note: Institution-specific data sharing policy covering research data exempts this Standard.

## 3. AUDIENCE

All USNH community members who access USNH information technology resources should be familiar with this Standard.

## 4. STANDARD

All information stored in USNH information technology resources is considered the property of USNH or one of its component institutions. USNH has a responsibility to protect the confidentiality, integrity, and availability of that information and preserve our community member's privacy. For this reason, access to institutional information stored in information technology resources is, by default, only provided where a legitimate business need exists and where the owners of that data have provided authorization.

Institutional information associated with a specific community member and requires using their USNH credentials to access accounts will be referred to as password-protected information for the remainder of this standard. This includes access to community members' accounts, USNH technology resources, and activity while accessing USNH technology resources.

USNH may access or disclose password-protected information without user consent only under the limited circumstances described in this standard.

### Password-Protected Information Request Types

There are eleven distinct types of requests for password-protected information:

- Subpoena court order, search warrant, or another legal requirement
- Legal Hold (to preserve data)
- Conduct Investigation
- Freedom of Information/Right-to-Know Request
- Personal Information for a deceased community member
- Life & Safety Event
- Academic honesty investigation
- Cybersecurity investigation
- Regular information technology resource operations
- Request to delete/takedown publicly accessible content belonging to another community member
- Mission-critical business continuity

### Subpoena, Court Order, Search Warrant, or Other Legal Requirement

All requests for password-protected information arising from a legal process, including subpoenas, court orders, search warrants, government investigations, or litigation, shall be referred to the USNH General Counsel's Office (GCO) before any action is taken.

### Legal Holds

Legal holds, preserving a snapshot of specific records indefinitely but that do not involve a search of those records, shall be referred to the USNH GCO before taking action. Only members of the GCO shall access information preserved under a legal hold.

### Conduct Investigations

Access to password-protected information related to a Human Resources (HR), Title IX Office, or Student Conduct Office investigations shall be referred to the USNH GCO for review before any action. Access to the information requested as part of an HR conduct investigation can only be given to HR personnel, the Director of the Title IX Office, the Director of the Student Conduct Office (as applicable), or the USNH GCO.

### Freedom of Information Act/Right to Know Requests

Members of the public can request and receive certain types of institutional information of public record under the Freedom of Information Act (FOIA) or Right to Know (RTK). In some circumstances, these requests include password-protected information, requiring the assistance of Enterprise Technology &

Services (ET&S) to fulfill. Before any action, FOIA and RTK requests shall be referred to the USNH GCO to determine the legitimacy and legality of the request.

FOIA and RTK requests are not considered confidential. USNH community members whose password-protected information is included in the target of a FOIA or RTK request shall be notified via e-mail using their institutional e-mail address prior to the search. As USNH is legally required to fulfill these requests, community members' consent is not applicable.

NOTE: Student e-mail is not considered a public record for these purposes.

### Access to Personal Information for Deceased Community Members

In circumstances where information contained in password-protected accounts associated with a deceased community member, a request shall be made in writing to Cybersecurity Governance, Risk, and Compliance (GRC) that specifies the following:

- Name of the community member
- Name of the requester
- The request for specific information may include search terms, e-mails sent to specific addresses, etc.
- The relationship of the requester to the deceased community member

Only the executor of the estate or the next of kin will be granted access to a deceased community member's information. Documentation is required to establish this relationship. The USNH GCO shall review and validate the legality of this documentation prior to any action. The USNH GCO and HR will authorize or decline the release of information.

Once the USNH GCO authorizes ET&S to provide the requested information, Cybersecurity GRC shall coordinate the provision of the information with the appropriate ET&S service lines. Cybersecurity GRC may require a management review of the appropriate administrative, academic, or business unit before releasing information.

Information provided to the community member’s executor or next of kin shall be restricted to the specific information approved by the GCO. No direct access to USNH information technology resources or USNH user credentials will be granted to the requester.

### Access to Information Related to an Ongoing Event Impacting Life & Safety

In the event of an incident with potential life and safety considerations, ET&S shall be empowered to provide all available information that might, in the opinion of the emergency response team, help preserve life and safety.

The following individuals shall have the power to authorize this kind of emergency access and use:

- Chief Information Officer
- Chief Information Security Officer
- Institutional Chief Operations Officer
- Institutional Chief of Police

- Institutional CEO

Emergency access and use of password-protected information shall utilize the least intrusive means to obtain only the information necessary to assess and resolve the emergency. The authorizing individual should weigh the need for access/use against other USNH or institutional concerns, including academic freedom, personal privacy, and integrity of institutional operations, and determine if the need for emergency access and use outweighs countervailing considerations.

The aforementioned leaders may verbally provide authorization for emergency access to the ET&S emergency response team member during an event. The authorizing ET&S member, Institutional CEO, or COO shall notify the appropriate institutional Chief of Police or Campus Safety director (if not the authorizing entity) of the emergency action taken.

The ET&S representative shall document the authorization and act as the primary point of contact for the emergency response team for the duration of the event.

### Access to Information Related to an Academic Honesty/Integrity Investigation

In circumstances where a faculty member suspects a violation of the institution's policy on academic honesty or integrity has occurred, they may request ET&S to assist the investigation by providing information regarding information technology resource usage. Resources may include but are not limited to network activity, application access, and activity.

Faculty shall submit requests for this type of information to ET&S in writing and require sign-off from either an Associate Dean, Dean, or the Registrar. ET&S shall treat this request as confidential and maintain an audit trail that includes the initial request and academic leadership sign-off.

Faculty members and academic departments making the request shall ensure the completion of all requirements defined in the relevant institution's policy.  Requirements include but not are not limited to a notification to students and/or academic leadership and making any determinations about suspected violations and penalties.

Note: There are limits to the information available to ET&S.  Requests will be met where possible and practical.

### Access to Information Related to a Cybersecurity Incident Investigation

In a declared cybersecurity incident, individuals within ET&S may require access to information, including password-protected information that exceeds the access those individuals would normally be granted to perform their assigned roles.   In these circumstances, a Cybersecurity & Networking (CS&N) team representative shall submit a written request to Cybersecurity GRC. The Chief Information Security Officer (CISO) or Chief Information Officer (CIO) shall approve the request.

This request shall be considered confidential and not be discussed or shared with anyone outside the designated Incident Response Team or CS&N leadership.  Community members whose password-protected information is included in this request shall not be notified or asked for consent to preserve the confidentiality of the incident investigation. Access granted shall be limited to the minimum information necessary.

### Access to Information During Regular Information Technology Resource Operations

USNH information technology resources require operational management and ongoing maintenance to ensure proper operation, the deployment of software or hardware updates, and adherence to regulatory and contractual obligations. Accordingly, to perform this work, ET&S-approved vendors and other authorized individuals may access password-protected information, solely for these purposes, without user consent or notification.

During this kind of access, ET&S personnel may observe password-protected information. Except as provided elsewhere in this standard, ET&S personnel is not permitted to seek out password-protected information that is not germane to the specific information technology resource operations and support activities being performed. Any unavoidable examination of password-protected information shall be limited to the minimum required to perform such duties. ET&S personnel are not exempt from the prohibition against personal or confidential information disclosure.

In their duties, ET&S personnel may inadvertently discover or suspect violations of law or USNH policy listed. In that case, they may preserve the data and report such violations using the appropriate reporting mechanism for the violation observed.

### Request to Take Down Publicly Accessible Content

A USNH entity may submit a request for access to password-protected information to remove publicly accessible content belonging to another community member. The community member should first attempt to reach a takedown agreement with the account owner serving the content. In cases wherein an agreement is not reached, Cybersecurity GRC will submit a petition to the content owner for removal on behalf of the requester. If consent is not granted, Cybersecurity will consult with the GCO and proceed with the request as deemed appropriate.

Note: The DMCA Compliance Standard addresses takedown requests related to copyrighted material.

### Access to Password Protected Information for mission-critical business continuity

Individuals may need access to information associated with an account to support mission-critical services.
Examples may include:

- Post-separation business continuity
- A faculty member requesting access to another faculty member's course in a learning management system
- A supervisor requesting access to a team member's e-mail account while that person is out on leave

If a USNH entity identifies a legitimate need to access the password-protected information of a USNH community member, every effort shall be made to obtain the information from the individual. However, if the direct transfer of information is not possible, a supervisor or an individual in the leadership hierarchy of the community member shall submit the request. The written consent of the community member is the preferred mechanism for approval. However, if consent is not available, written authorization from an appropriate institutional Vice President shall be required.

ET&S - Identity & Access Management (IAM) shall administer and facilitate these requests as outlined in this standard's roles and responsibilities section.

Access request requirements and limitations:

- A specific business need shall accompany the request; the IAM team may deny submissions lacking a legitimate business purpose
- The request shall name specific individual(s), and any access granted will be limited to the named individuals.
- Access granted shall be limited to the minimum password-protected information necessary to address the business need.
- Successful granting access does not alter or modify any intellectual property or content ownership rights addressed in other USNH and/or institutional policies or contracts.
- Requests granting access to e-mails or documents contained in a former employee's account, which is also an active or prior student, shall be limited to specific terms.

## Special Notice Regarding Personal Information

All information processed through or stored on institutional information technology resources (e.g., enterprise e-mail, cloud storage) is subject to discovery in legal proceedings and requests for the Right to Know Act. USNH advises community members that information they might consider private can be legitimately accessed or disclosed under any of the above-mentioned circumstances. Any personal information stored on USNH information technology resources is subject to disclosure.

## Transparency and Traceability

Anytime access to or disclosure of password-protected information requiring the involvement of ET&S is approved without community member consent, a record of that access or disclosure shall be created that includes, at a minimum, the following:

- The type of password-protected information requested
- A description of the password-protected information that was accessed or disclosed
- The justification for the access or disclosure
- The designated approver(s) name(s)
- Documentation supporting all required approvals
- Any notifications sent to the community member

These records shall be collected and maintained by Cybersecurity GRC under the oversight of the Chief Information Security Officer (CISO) for seven years.

## 5. MAINTENANCE OF PROCESSES AND PROCEDURES SUPPORTING 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 standard 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).

Employees who are members of institutionally recognized bargaining units are subject to this standard and are covered by the disciplinary provisions set forth in the agreement for their bargaining units for any violation.

## 7. EXCEPTIONS

Exceptions cannot be granted to this Standard.

## 8. ROLES AND RESPONSIBILITIES

**ASSOCIATE DEAN, DEAN, REGISTRAR:**

Access to Information Related to an Academic Honesty/Integrity Investigation

- Sign-off on requests for information related to academic honesty/integrity investigations

**CHIEF INFORMATION OFFICER (CIO):**

**General:**

- Standard enforcement

**Access and/or use information related to an ongoing event impacting life and safety:**

- Authorize ET&S to access and/or use information related to an ongoing event impacting life and safety as deemed necessary.
- Notify appropriate institutional Chief of Police or Campus Safety director (if not the authorizing entity) of authorization granted.

**Access and/or use information related to a cyber incident investigation:**

- Authorize ET&S to access and/or use information related to a cybersecurity incident investigation as deemed necessary.

**CHIEF INFORMATION SECURITY OFFICER (CISO):**

**General:**

- Standard enforcement
- Cybersecurity Governance, Risk & Compliance oversight

**Access and/or use information related to an ongoing event impacting life and safety:**

- Authorize ET&S to access and/or use information related to an ongoing event impacting life and safety as deemed necessary.
- Notify appropriate institutional Chief of Police or Campus Safety director (if not the authorizing entity) of authorization granted.

**Access and/or use information related to a cyber incident investigation:**

- Authorize ET&S to access and/or use information related to a cybersecurity incident investigation as deemed necessary.

**CHIEF OPERATIONS OFFICER (COO):**
**Access and/or use information  related to an ongoing event impacting life and safety:**

- Authorize ET&S to access and/or use information related to an ongoing event impacting life as required.
- Notify appropriate institutional Chief of Police or Campus Safety director (if not the authorizing entity) of authorization

**CYBERSECURITY & NETWORKING:**
**Access and/or use information related to a cyber incident investigation:**

- Submit written requests approved by the USNH CIO or CISO to GRC for access to information.

**CYBERSECURITY GOVERNANCE, RISK, & COMPLIANCE (GRC):**
**General:**

- Collect and maintain all records regarding access to or disclosure of password-protected information requiring the involvement of ET&S is approved without community member consent.
- Verify all records regarding access to or disclosure of password-protected information requiring the involvement of ET&S is approved without community member consent; contain the following information:
  - The type of password-protected information requested
  - A description of the password-protected information that was accessed or disclosed
  - The justification for the access or disclosure
  - The designated approver(s) name(s)
  - Documentation supporting all required approvals
  - Any notifications sent to the community member
  - Maintain detailed audit trail of all requests for password-protected information requests.

**Access requests relating to a subpoena, court order, search warrant, legal holds & conduct investigation, and Freedom of Information Act/Right to Know requests:**

- Receive GCO vetted requests and identify the appropriate team within ET&S to coordinate fulfillment of request
- Provide a single point of contact within ET&S for the GCO and/or HR.
- Ensure proper and timely handling within ET&S
- Facilitate and coordinate ET&S service lines to access and retrieve the required information as needed.

**Access to Personal Information for Deceased Community Members**

- Receive access to password-protected information requests and verify the following information:
    - The name of the deceased community member and requestor.
    - The relationship of the requester to the deceased community member
- Submit death certificate and/or related documentation to the GCO for validation before proceeding with the request.
- Collaborate with GCO and HR to determine the appropriate course of action regarding identifying deceased community member's next of kin or estate executor if not already on file.
- Coordinate the provision of the information with the appropriate ET&S service lines.
- Request management review of the appropriate administrative, academic, or business unit before releasing information as deemed necessary.

**Access and/or use information related to an ongoing event impacting life and safety and cybersecurity incident investigation:**

- Receive and maintain records of any emergency information access and use authorized during the event from the ET&S emergency response representative.

**Access and/or use information related to a cybersecurity incident investigation:**

- Coordinate approval between the requesting ET&S service line and the USNH CIO or CISO
- Document all granted requests for access to password-protected information, including:
    - Who made the request
    - The justification for the request
    - Who approved the request, when it was approved, and evidence of the approval
    - Whom the access was granted to and what specific information they were allowed to access
    - When access was granted and revoked

**Access requests to take down publicly accessible content:**

- Coordinate fulfillment of the request and provide a single point of contact for the requester and ET&S.
- Submit petitions on behalf of the requester to access another community member's password-

protected information as needed.

- Request assistance from the GCO office on the legality of the request as needed.
- Maintain all documentation relating to requests for consent.

**CYBERSECURITY IDENTITY & ACCESS MANAGEMENT (IAM):**
**General:**

- Collaborate with other ET&S groups facilitating all types of access requests as needed.

**Access and/or use of password-protected information related to mission-critical business continuity**

- Vet requests
- Request and obtain required approval for requests from appropriate business units.
- Coordinate fulfillment requests
- Maintain the required audit trail for requests for password-protected information involving the IAM team.

**ET&S REPRESENTATIVE TO EMERGENCY RESPONSE TEAM:**
**Access and/or use information related to an ongoing event impacting life and safety and cybersecurity incident investigation:**

- Obtain sign-off from the individual responsible for authorizing the emergency access and use.
- Perform duties as required under guidance and approval from authorizing leadership.
- Document records specifics of emergency information access/use for submission to Cybersecurity GRC.
- If needed, notify the appropriate Chief of Police or, Director of Camus Safety when access or use of information is authorized in an emergency.
- Act as the primary point of contact between ET&S and the emergency response team for the duration of the event.

**HUMAN RESOURCES, TITLE IX OFFICE DIRECTOR, STUDENT CONDUCT DIRECTOR:**

- Request access to password-protected information needed for an investigation.
- In collaboration with the USNH GCO, determine all access, notification, and confidentiality requirements for requests related to conduct investigations as needed.

**INSTITUTIONAL CHIEFS OF POLICE AND INSTITUTIONAL CEO:**

- Authorize ET&S to access and/or use information during an emergency.

**USNH GENERAL COUNSEL'S OFFICE (GCO):**
**General:**

- Work in collaboration with ET&S and other USNH business units to ensure the activities performed in the access request process are legal and incorporate due care.

**Access to password-protected information requests relating to a subpoena, court order, search warrant, legal holds & conduct investigation, Freedom of Information/Right to Know requests, and deceased community members.**

- Validate legitimacy and legality of requests submitted documentation related to the request
- Authorize or decline release of information as deemed appropriate for each request involving the GCO
- Grant authorization to the appropriate ET&S team member as deemed appropriate to retrieve requested password-protected information requests related to:
- Work in collaboration as needed with other business units to determine notification requirements to information-owners.
- Identify and apply the appropriate level of confidentiality for the requests involving the GCO.

## 9. RELATED POLICIES AND STANDARDS

- USNH Cybersecurity Policy
- Cybersecurity Exception Standard
- Access Management Standard

## 9. 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, & Compliance (GRC) via this Support Form.

A community member may submit other requests here: Submit an IT Question.

## 10. DOCUMENT HISTORY

Effective Date: May 31, 2021
Drafted: R Boyce-Werner, AUG 2020. v01
Revised, USNH Cybersecurity GRC Standards Committee, DEC 2021, v02
Reviewed by: Dr. David Yasenchock, Director Cybersecurity GRC, DEC 15, 2021, v02
Approved by: Thomas Nudd, Chief Information Security Officer, DEC 21, 2021, v02