University System of New Hampshire

INSTITUTIONAL EMAIL SECURITY STANDARD

Responsible Executive/University System Officer: Chief Information Security Officer
Responsible Office: Cybersecurity & Networking
Approved Distribution: Designated Reviewers Only
Status: INFORCE

1 PURPOSE

This Standard informs all University System of New Hampshire (USNH) community members of the expectations around acceptable and secure use of institutional email across the University System. Email is an enterprise tool improving education and administrative efficiency and to enable internal and external communications. It serves as a primary means of communication from the University System and its component institutions to all community members.

This Standard outlines what constitutes responsible use and mandates acceptable use practices designed to achieve three goals:

1. Ensure trusted availability of the electronic communication delivery mechanisms used by the University System and all faculty, staff, and students of the individual component institutions.
2. Reduce the risk of non-PUBLIC institutional data being exposed via unsafe email practices.
3. Ensure that all USNH and component institution communications are conducted via approved enterprise email systems.

2 SCOPE

This Standard applies to all emails sent or received as part of conducting USNH or component institution business or the business of one of its component institutions, as well as to any email sent by or received in an enterprise email account. It specifically includes:

- Administrative, academic, and/or research-related emails sent between employees and students (e.g., emails from faculty to students, as well as emails from students to faculty)
- All non-employee email, including but not limited to sponsored accounts, sent or received while conducting USNH or institutional business or used to communicate with external parties as a representative of USNH or one of its institutions

- Email used for marketing, recruitment, and outreach

For clarification purposes, email services are those provided by Enterprise Technology & Services to send and receive email using individual institutional email accounts or shared accounts assigned to administrative, academic, or business units as well as associated features (e.g., calendar, contacts, etc).

3 AUDIENCE

This Standard applies to all members of the USNH community who are granted access to email services by virtue of their relationship with the University System or one of its component institutions.

4 STANDARD

Enterprise email services are provided to faculty, staff, students, emeritus, prior students/alumni, sponsored users, and other affiliated individuals for USNH institutions and the system-office to conduct University System and component institution business and shall be used whenever employees are acting in an official capacity.

Use of enterprise email services shall comply with local, state, and federal laws and regulations and adhere to all relevant USNH Policies and Standards.

EMAIL AS AN OFFICIAL MEANS OF COMMUNICATION

Use of an email address with the domains listed below clearly identifies the sender as a member of the University System community. It informs the recipient that the communication constitutes official business on behalf of the University System or its component institutions.

- @granite.edu
- @keene.edu
- @plymouth.edu
- @unh.edu
- @law.unh.edu
- @usnh.edu

Conducting USNH/institution business via email addresses not attached to one of the listed domains introduces unnecessary risk into the USNH environment. These risks include, but are not limited to:

- Loss of institutional information
- Exposure of regulated information that requires reporting under FERPA, HIPAA, GLBA, or other regulations
- Loss or theft of intellectual property or research data

- Risk of non-standard cybersecurity control application

In addition to the listed domains, some USNH community members with email addresses using deprecated, legacy domains may have continued use of those email addresses. However, new email addresses using these legacy domains will not be created.

Ownership of Email Data

USNH owns all enterprise email accounts. Enterprise email accounts are subject to underlying copyright and other intellectual property rights under applicable laws and University System or component institution policies.

Confidentiality, Security and Privacy of Email

USNH and its component institutions strive to provide secure and reliable email services by following industry standard information technology and cybersecurity practices.

Additionally, there are specific restrictions regarding the use of email when handling some types of institutional information. These requirements are detailed in the *Restricted Information Handling Standard.*

All USNH employees who interact with institutional information are responsible for understanding specific handling requirements, restrictions, and procedures related to the use of email for transmitting those types of information.

Users of the USNH Enterprise Email services have a reasonable expectation of privacy. However, under certain circumstances, email may be accessed by authorized personnel as governed by the USNH *Access to Password Protected Information Standard*. This includes, but is not limited to

- Circumstances where access is required by law (e.g., court orders, freedom of information act / right to know laws)
- Conduct Investigations
- Academic Honesty Investigations
- Enterprise Technology & Services (ET&S) has the authority to access and inspect the contents of any equipment, files, or email on its information technology resources for troubleshooting and cybersecurity investigation purposes with appropriate, prior approval.
- ET&S may also review, filter, reject, preserve, and/or remove from enterprise systems, any email that is confirmed, identified, and or reported to contain malware, viruses, phishing attempts, spam, or other harmful or inappropriate content.

See the *Access to Password Protected Information Standard* for additional information.

All users of the USNH email system are encouraged to protect the privacy of their personal information by retaining a clear separation between institutional/academic email and personal email by using a separate, non-USNH email account for conducting personal business.

ROLE-BASED RULES FOR ENTERPRISE EMAIL ACCOUNTS

Faculty and Staff

Email services are available for faculty and staff to conduct USNH and component institution business.

Email services for faculty and staff are provided while those community members are employed by the University System. Employees whose employment at USNH ends, or whose role-based grace period for continued access ends, shall have their email accounts disabled and access to that account shall no longer be allowed. Auto-forwarding of email to an address that is external to USNH is prohibited.

Students

Email services are available for students to support learning and communication by and between their USNH institution and themselves. Email services are provided for the entire duration that a student is considered active at their specific institution. Auto-forwarding of email to an address that is external to USNH is prohibited. Emails sent to or from institutional email accounts belonging to active students who have no other roles at any USNH institution are not considered public records under the Freedom of Information Act/NH Right to Know Law, RSA-91-A.

Other Community Members

Individuals with special relationships with the University System or one of its component institutions, such as sponsored users or official visitors, who are neither employed by USNH nor enrolled at any USNH component institution, may be granted limited email privileges, including an email address, commensurate with the nature of their special relationship. Auto-forwarding of email to an address that is external to USNH is prohibited. USNH is free to discontinue these privileges at any time without warning or cause.

MODIFICATIONS TO EMAIL ON COMMUNITY MEMBER ROLE CHANGES

Enterprise email is provided to community members based on qualifying roles. Changes to those roles can impact access to email accounts and all emails sent or received via those accounts. This includes any personal emails sent or received using an enterprise email account.

PROHIBITED USE OF EMAIL SERVICES

Use of USNH Email services are subject to the USNH Acceptable Use Policy.

Use of email in violation of other USNH policies is also a violation of this Policy.

Abuses of USNH's enterprise email services shall be directed to the email address below that corresponds with the relevant domain.

- abuse@usnh.edu

MASS EMAIL COMMUNICATIONS

USNH, along with its component institutions, offers a variety of email tools specifically designed to support communication with large groups internally, externally, or with mixed audiences. The appropriate tool for a specific need depends on the institution the communication is being sent from and the intended audience.

The following requirements apply to all mass email communications sent on behalf of USNH or one of its component institutions, regardless of the tool used for distribution. USNH mass email communications shall:

1. Follow all local, state, and federal laws and regulations and USNH and component institution policies and standards.
2. Represent a recognized USNH entity, such as a college, department, committee, team, group, or student organization.
3. Include a 'from' line/signature of an individual or for a USNH/institutional group that describes/explains who that person/group is and how to contact them.
4. Only be sent to individuals who are:
    - A member of the group the email communication applies to (e.g., an anthropology department can email all anthropology students, an information system owner can email all individuals with access to that information system), or
    - Have opted in to receive communications from the entity sending the communication, or
    - Have expressed at least indirect interest in the topic (e.g., someone who signed up for an outing hosted by Campus Rec can receive emails from Campus Rec about other outings).

Mass email communications sent by USNH or institutional administrative, academic, or business units shall only use the institutionally approved mechanisms for mass email communication distribution.

Attempts to use enterprise email accounts to send email to large groups outside of these mechanisms may be blocked by administrators, and the sender's email account may be secured.

Information on approved mechanisms for a specific institution can be requested from the ET&S Help Desk.

University System of New Hampshire

USNH Distribution Lists

USNH distribution lists provided within an enterprise email service (e.g., the Global Address List/GAL) available for use by all community members are subject to the following restrictions:

- Employee use of USNH distribution lists for mass mailing is allowed only for legitimate academic or administrative purposes
- Use of USNH Distribution lists shall be approved by the owner of the list.
- Student organizations and their members who wish to use USNH distribution lists shall seek prior approval from the appropriate institutional authority to use defined lists for surveys and announcements
- Use of any enterprise email system for creating or obtaining lists of USNH community members for any purpose not directly related to an employee's job responsibilities is prohibited.

Automated Email Communications Sent from Information Technology Resources

Whenever possible, automated email communications sent from information technology resources should include the following content:

- Designate which recognized USNH or component institution administrative, academic, or business unit, such as a college, department, committee, team, group or student organization is sending the communication
- Include appropriate institutional branding
- Include a 'from' line/signature of an individual or for a USNH or component institution group that describes/explains who that person/group is and how to contact them

External Email

When email communications must be sent to USNH community members via a third-party service or application, the external email address(es) used to send those communications may need to be identified as legitimate. This process, called Allow Listing and informs the enterprise email service that communications sent from safe-listed addresses are safe to deliver. This ensures those communications will not be flagged as "junk" or "spam".

If a company passes SPF and DMARC settings as per email standards, safe listing should not be required or needed.

If email is getting blocked by filters, please work with the company sending the emails to make sure they pass these settings maybe give them a link to a message header reader they can send to the company. If the work is deemed critical, a case will be needed to Enterprise Email Administrators and Cybersecurity & Networking (CS&N), with IP addresses.

Email being sent from sources external to USNH are required to be tagged with caution external banner.

Requests for adding to the Enterprise Email Allow List shall be subject to approval by the ET&S Enterprise Email Administrators and ET&S Cybersecurity & Networking (CS&N).

Administrative, Academic, and Business Unit Shared Email Boxes

Administrative, academic, or business units that provide services in response to email requests may request a shared mailbox to support business continuity for managing email.

Access to Email Services via Mobile Device

Access to USNH email on mobile phones, whether those phones are owned by USNH or one of its institutions or are personal devices, should, at a minimum, have the following protections enabled on the mobile phone.

- An enabled screen lock that requires a password, PIN, or biometric factor to gain access to the device
- Encryption enabled using the native encryption available on the device

Unit Guidelines/Procedures Permitted

This Standard provides the minimum requirements allowed. Administrative, academic, and business units may supplement this Standard with their own email use procedures and guidelines for their local team members. Unit-level procedures and guidelines may be more restrictive and/or prescriptive than this Standard but cannot be less restrictive.

In the event such procedures and guidelines are inconsistent with this Standard, this Standard shall govern.

Compromised Email Accounts

An enterprise email account that has been compromised shall be promptly remedied using the appropriate means. The appropriate means may include:

- Securing of the community member's enterprise account(s)
- Requiring an out of band password reset
- Reviewing the community member's accounts and access levels
- Cybersecurity investigation

Securing a USNH community member's account temporarily blocks the ability to use that account to

access any information technology resources that use centrally managed accounts for access. More information about this process can be found in the *Access Management Standard*.

Any enterprise email account holder who suspects their email account has been accessed by an unauthorized party shall report the potential compromise immediately per the process outlined in the *Cybersecurity Incident Response Plan.*

Failure to maintain a compliant password shall result in the Email account being disabled. Prior student/alumni accounts that are disabled for a non-compliant password shall be recoverable for 60 days, after which, the contents of the account will be irretrievably deleted.

In the event the same enterprise email account is confirmed to be compromised three or more times in any 12-month period, additional action may be taken, and additional requirements may be imposed, including, but not limited to account suspension, device quarantining, and mandatory community member training.

NON-ENTERPRISE EMAIL SYSTEMS

Per the *USNH Cybersecurity Policy*, USNH administrative, academic, and business units and individual community members shall not deploy, implement, or build enterprise information technology services that duplicate services provided by Enterprise Technology & Services (ET&S) without prior authorization. This provision specifically applies to email systems that leverage any of the USNH domains (e.g., sr.unh.edu).

EMAIL ANTI-MALWARE PROTECTION

Enterprise email services shall employ standardized anti-malware protection to protect against malware distributed by email. Automatic anti-malware protection mechanisms must receive regular updates from authorized threat sources to ensure rules used to identify potential malware emails reflect currently available threat intelligence.

EMAIL MULTI-FACTOR AUTHENTICATION

Multi-Factor Authentication will be deployed to enterprise email accounts as scheduled by ET&S to enhance network security posture and protection.

AUTOMATIC SPAM/PHISHING PROTECTION

Enterprise email services shall employ automatic spam/phishing protection mechanisms designed to detect and act upon email traffic that displays common characteristics of spam or phishing emails.

These automatic mechanisms shall be centrally managed by ET&S. Automatic spam/phishing protection mechanisms must receive regular updates from authorized threat sources to ensure rules used to identify potential spam/phishing emails reflect currently available threat intelligence.

Where possible, automatic spam/phishing protection mechanisms shall be self-learning to provide maximum real-time protection from spam/phishing with minimal disruption to legitimate email traffic.

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.

7 EXCEPTIONS

Requests for exceptions to this Standard shall be submitted and approved according to the requirements provided in the *Cybersecurity Exception Standard*.

8 ROLES AND RESPONSIBILITIES

Cybersecurity GRC:

- Approve/deny Email Allow List requests
- Validate adherence to standard

Cybersecurity Operations & IAM:

- Secure accounts identified as compromised based on email activity
- Identify standardized email security controls.

Email Administrators:

- Maintain email applications and the underlying infrastructure that supports them such that the availability of this critical enterprise information technology resource is preserved and protected
- Monitor email traffic for anomalous email behavior
- Provision and deprovision enterprise email accounts according to access and account management requirements and procedures
- Secure accounts identified as compromised based on email activity
- Approve/deny Email Safe List requests

USNH Community Members:

- Use email services and tools provided by USNH and its component institutions according to the requirements outlined in this Standard
- Understand the institutional information used in job responsibilities and any special handling requirements for that information regarding email
- Report suspected unauthorized access to or use of enterprise email accounts

9 DEFINITIONS

The following terms are defined in the ET&S Glossary of Terms:

- Access
- Account
- Administrator
- Availability
- Bulk Email
- Compromised Account
- Confidentiality
- Deprovision
- Domain
- Information
- Information Technology Resource
- Institutional Information
- Out of Band
- Phishing
- PROTECTED Information

- Provisioning
- RESTRICTED Information
- Spam

10 ET&S Related Policies and Standards

- USNH Cybersecurity Policy
- USNH Information Classification Policy
- USNH Password Policy
- Access to Password Protection Information Standard
- Access Management Standard
- Cybersecurity Exception Standard
- Restricted Information Handling Standard
- Confidential Information Handling Standard

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

Effective Date:	3 MAY 2022
Approved by:	CYBERSECURITY POLICY & STANDARD WORKING GROUP, 3 MAY 2022 V1.0
Reviewed by:	Tom Nudd, USNH CISO, 3 MAY 2022 V1.0
Revision History:	CYBERSECURITY COMMITTEE, 3 MAY 2022 V1.0