University System of New Hampshire

PSU EMAIL USE POLICY MAPPING

Note: this information is identical to the same information provided for this Policy in the PSU IT Policy High Level Mapping Document.

MAPPING TO CURRENT POLICIES

The provisions in the existing PSU Email Use Policy will be replaced by the following USNH Policies and Enterprise Technology & Services Standards. A detailed mapping is provided below.

- USNH Acceptable Use Policy
- USNH Cybersecurity Policy
- Email Security and Use Standard
- Identity Management Standard
- Access to Password Protected Information Standard

PSU – EMAIL USE POLICY (FIN-ITS-004) MAPPING

Current Policy: https://campus.plymouth.edu/it/wp-content/uploads/sites/44/2018/10/FIN-ITS-004-Email-Use-1.pdf

Annotations below indicate how each of the provisions in this policy are addressed by new or existing USNH Policies and/or the relevant ET&S Cybersecurity Standards.

- *Italics* = existing Policy language
- **NP =** USNH Policy
- **ST=** ET&S Cybersecurity Standard
- **Removed –** provisions that are not being carried forward at this time
- **Note –** Additional recommendation

I. Purpose

Email services are provided to the Plymouth State University (PSU) community in support of the teaching, learning and mission of the University along with supporting administrative functions necessary to carry out that mission. Users of University email services are expected to always act in accordance with the Acceptable Use Policy (AUP) and with professional and personal courtesy and conduct.

- **NP =** USNH Acceptable Use Policy, section 4.1 and 4.2
- **ST=** Email Security and Use Standard

II. Applicability and Authority

This policy covers the use of any email sent from a PSU email address and also applies to vendors, and agents operating on behalf of the University.

- **NP =** USNH Acceptable Use Policy, section 4.1 and 4.2
- **ST=** Email Security and Use Standard, section 2

III. Detailed Policy Statements

Persons may not use email in violation of USNH or PSU policies, or local, state or federal laws. This includes, but is not limited to:

- *Stalking, harassment (including sexual harassment), or other unlawful activity.*
- *Sending or forwarding private or sensitive information (e.g. social security numbers, credit card information, user credentials) in an unencrypted format (see the Sensitive Data policy).*
- *Fraudulent acts, including the use of a deceptive alias to disguise one's true identity.*
- *Intentional distribution of viruses (real or simulated) or otherwise destructive software using E-mail.*
- *Any use of PSU resources for personal commercial gain, solicitation for self or other promotion except in cases of officially sanctioned University activities.*
- *Political advocacy and related activities are not permitted. Additional information can be found in USNH policy. (https://www.usnh.edu/policy/usy/vpersonnel-policies/d-employee-relations).*
- *Participation in chain-letters*

    - **NP =** USNH Acceptable Use Policy, section 4.4
    - **ST=** Email Security and Use Standard, Prohibited Use of Email Services

IV. Procedures

General

i. Any communications may become the subject of litigation. As such, disclosure may be granted pursuant to any subpoena filed for such a purpose upon direction from the Chief Information Officer (CIO) or any Principal Administrator.

- **ST=**
    - Email Security and Use Standard, Access to Email by Authorized Personnel
    - Access to Password Protected Information Standard

ii. Email containing official business of PSU shall be addressed to an official University email address and should not be addressed to alternative addresses. Such email shall not be automatically forwarded to an external address.

iii. PSU employees shall only use PSU email systems for conducting official University business. The use of private or third-party email systems for official business is prohibited.

- **ST=** Email Security and Use Standard, Email as an Official Means of Communication *iv. Email accounts may be accessed by system administrators for the purposes of maintenance, forensics, and/or to support investigations. ITS may filter, reject, preserve and/or remove from PSU systems, any email that is suspected to contain viruses, phishing attempts, spam or other harmful or inappropriate content.*

- **ST=** Email Security and Use Standard, Access to Email by Authorized Personnel

v. Upon receiving an appropriately authorized written request from Student Affairs or Human Resources as applicable, the Chief Information Officer (CIO) or Chief Security Officer (CSO) can grant access to a users' email to support an official investigation.

- **ST=**
  - Email Security and Use Standard, Access to Email by Authorized Personnel
  - Access to Password Protected Information Standard

vi. Upon employee termination, resignation, or withdrawal, these materials remain the property of the University and any associated email account(s) will be terminated. All information not retained by PSU will be deleted.

- **ST=** Email Security and Use Standard, Modifications to Email on Community Member Role Change and Ownership of Email Data

Exceptions to this policy may be granted for individuals who maintain a continued relationship in good standing with PSU and who actively use their accounts.

- **Removed –** not aligned with security best practices or other institutional policy, will not be carried forward to new policies and standards. The Sponsored Access process, defined in the Sponsored/Guest Access Management Standard would be the only mechanism for providing this kind of ongoing access post-termination.

vii. PSU email servers are configured with quotas for e-mail storage, and no email will be systematically archived. It is the sole responsibility of end users to remain within the limits of the quota and archive their email as necessary.

- **Removed –** no longer applicable

viii. Any official PSU auto-populated LISTSERV or distribution list used for campus-wide email communication shall be subject to the policies of each list, as defined by the list owner and/or the Office of Public Relations.

- **ST=** Email Security and Use Standard, USNH Distribution Lists and Mass Email Communications

ix. No group accounts will be created

- **ST=** Email Security and Use Standard, Administrative, Academic, and Business Unit Email Boxes *x. New, or changed, usernames are generated using the established USNH standard, with no exceptions.*

- **ST=** Identity Management Standard, Primary Identity

xi. All newly created accounts are given a user-friendly email address (alias) that can be used as an alternate address.

- **Removed –** not carried forward to allow flexibility for the email administrators

V. Non-compliance

Members of the PSU community who violate this policy may be denied access and be subject to disciplinary action within and outside the University.

- **NP =** USNH Cybersecurity Policy, section 6

VI. Definitions

USNH A term used to describe the collective group consisting of Keene State College, Granite State College, Plymouth State University and the University of New Hampshire

Group Accounts A username / password that is shared among multiple individuals.

LISTSERV An electronic mailing list which offers an efficient way to disseminate information to large numbers of people and hold long-distance discussions among many people.

- **NP =** USNH Cybersecurity Policy, section 9
- ET&S Glossary of Terms

VII. Related Policies / References for More Information

- *Acceptable Use Policy*
- *User Credentials Policy*
- *Sensitive and Confidential Information Policy*
    - **NP =** USNH Cybersecurity Policy, section 10

Plymouth State Policy
Policy Title: Email Use Policy
Effective date: 08/11/2014
Last Revision: 10/01/2018

- **NP** = Document Information provided at the end of each Policy and Standard