University System
of New Hampshire

PSU IT POLICIES
HIGH LEVEL MAPPING

OVERVIEW

The Enterprise Technology & Services (ET&S) Policy & Standard initiative consolidates all existing USNH and institutional information technology policies into a new structure that is applicable across the entirety of USNH. The decision to consolidate all institutional information technology functions and resources into a single organization makes this consolidation necessary.

This document provides a high-level mapping of the existing Plymouth State University IT Policies to the new Technology/Cybersecurity Policies & Standards.

POLICIES

Acceptable Use of Computing Resources (FIN-ITS-001)

Sensitive and Confidential Information Policy (FIN-ITS-002)

User Credentials Policy (FIN-ITS-003)

Email Use Policy (FIN-ITS-004)

Departmental Server Policy (FIN-ITS-005)

Voice Mail Use Policy (FIN-ITS-006)

Secure Web Application Development Policy (FIN-ITS-007)

Shared Drives Policy (FIN-ITS-009)

Email Distribution Lists Policy (FIN-ITS-011)

Purchasing Technology Equipment, Services and Software

Surplus Computer Equipment Policy (FIN-ITS-012)

Repair Services Policy (FIN-ITS-013)

Supported Computer Equipment Policy (FIN-ITS-014)

Digital Millennium Copyright Act (DMCA) Implementation at PSU

Appendix A: USNH Acceptable Use Policy Mapping

Appendix B: USNH Information Classification Policy Mapping

Appendix C: PSU User Credentials (FIN-ITS-003) Policy Mapping

Appendix D: PSU Email Use Policy (FIN-ITS-004) Mapping

Acceptable Use of Computing Resources (FIN-ITS-001)

https://campus.plymouth.edu/it/wp-content/uploads/sites/44/2017/10/FIN-ITS-001-Acceptable-Use.pdf

This policy covers the use of institutional and USNH information technology resources.

To Be Replaced By:

- USNH Acceptable Use Policy (AUP)

Detailed mapping of the provisions in this policy to the new USNH AUP are provided in *Appendix A: USNH Acceptable Use Policy Mapping*.

Sensitive and Confidential Information Policy (FIN-ITS-002)

https://campus.plymouth.edu/it/wp-content/uploads/sites/44/2018/10/FIN-ITS-002-Sensitive-and-Confidential-Information.pdf

This policy is intended to help employees determine the relative sensitivity of information, where information should be stored, and what information can be disclosed to non-employees.

To Be Replaced By:

- USNH Information Classification Policy (revised version of existing USNH Policy)
- Public/Sensitive Information Handling Standard
- Protected Information Handling Standard
- Restricted Information Handling Standard
- Confidential Information Handling Standard

Detailed mapping of the provisions in this policy to the new USNH Information Classification Policy and the various data handling and data management Standards are provided in *Appendix B: USNH Information Classification Policy Mapping*.

User Credentials Policy (FIN-ITS-003)

https://campus.plymouth.edu/it/wp-content/uploads/sites/44/2017/10/FIN-ITS-003-User-Credentials.pdf

This policy is intended to inform employees of their responsibility to protect all institutional user credentials entrusted to them.

To Be Replaced By:

- USNH Cybersecurity Policy
- USNH Password Policy
- Access Management Standard
- Account Management Standard
- Endpoint Management Standard
- Non-Primary Identity Management Standard
- Sponsored/Guest Access Management Standard

As the provisions in this policy are split across multiple policies and standards, a detailed mapping of the provisions in this policy is provided in *Appendix C: User Credentials Policy Mapping.*

Email Use Policy (FIN-ITS-004)

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

This policy covers the use of any email sent from a PSU email address.

To Be Replaced By:

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

As the provisions in this policy are split across multiple policies and standards, a detailed mapping of the provisions in this policy is provided in *Appendix D: Email Use Policy Mapping.*

Departmental Server Policy (FIN-ITS-005)

https://campus.plymouth.edu/it/wp-content/uploads/sites/44/2017/10/FIN-ITS-005-Departmental-Server.pdf

This policy establishes standards for departmental servers.

Recommendation:

- Policy will remain in place until the new Server Security and Management Standard, which is planned for Phase 2, goes into effect

Voice Mail Use Policy (FIN-ITS-006)

https://campus.plymouth.edu/it/wp-content/uploads/sites/44/2017/10/FIN-ITS-006-Voice-Mail-Use.pdf

This policy covers the use of any Voice Mail received on a PSU phone extension.

Recommendation:

- Policy should be retired on 01 May 2021 when the USNH Acceptable Use Policy becomes effective as most provisions in this policy overlap with the AUP, which governs use of institutional telecommunication services. An example specific to voicemail was added to the AUP for clarity. Networking & Telecom SLL is in agreement with this recommendation.

Secure Web Application Development Policy (FIN-ITS-007)

https://campus.plymouth.edu/it/wp-content/uploads/sites/44/2017/10/FIN-ITS-007-Secure-Web-Application-Development.pdf

This policy defines requirements for Web application development and security for all PSU Web applications deployed on or off-campus.

To Be Replaced By:

- Application Administration Standard
- System Acquisition, Development, and Maintenance Lifecycle Standard

A detailed mapping of how the provisions in this policy will be replaced by the two referenced standards will be provided as part of the implementation plan for those standards, which are currently slated for Phase 3. This Policy will remain in place until those Standards are implemented.

Shared Drives Policy (FIN-ITS-009)

https://campus.plymouth.edu/it/wp-content/uploads/sites/44/2017/10/FIN-ITS-009-Shared-Drives.pdf

This policy establishes standards for creation and maintenance of shared file services at PSU.

To Be Replaced By:

- Shared File Storage Standard

A detailed mapping of how the provisions in this policy will be replaced by the referenced standard will be provided as part of the implementation plan for that standard, which is currently slated for Phase 3. This Policy will remain in place until those Standards are implemented.

Email Distribution Lists Policy (FIN-ITS-011)

https://campus.plymouth.edu/it/wp-content/uploads/sites/44/2017/10/FIN-ITS-011-Email-Distribution-List.pdf

This policy establishes standards for creation and management of distribution lists at PSU.

To Be Replaced By:

- Email Security and Use Standard

No detailed mapping required as the existing policy will be replaced in by the referenced Standard.

Purchasing Technology Equipment, Services and Software

This is listed on the PSU IT Policies page, but the link refers to the PSU Client Portal Page.

Recommend immediate removal of this link from the PSU IT Policy page

Requirements and mandates for purchasing technology equipment (other than endpoint devices), services, and software will be addressed in the System Acquisition, Development, and Maintenance Lifecycle Standard and the Vendor Cloud Service Security Standard.

Surplus Computer Equipment Policy (FIN-ITS-012)

https://campus.plymouth.edu/it/wp-content/uploads/sites/44/2017/10/FIN-ITS-012-Surplus-Computer-Equipment.pdf

This policy establishes standards for the retirement and disposal of computer and related equipment.

To Be Replaced By:

- Endpoint Management Standard
- Information Technology Resource Secure Disposal Standard

Already removed from PSU IT Policy Page.

Repair Services Policy (FIN-ITS-013)

https://campus.plymouth.edu/it/wp-content/uploads/sites/44/2017/10/FIN-ITS-013-Repair-Services.pdf

This policy establishes level of service, population served and the extent of qualified services available at the Repair Center.

To Be Replaced By:

- Endpoint Management Standard

No detailed mapping required as the existing policy will be replaced in by the referenced Standard.

SUPPORTED COMPUTER EQUIPMENT POLICY (FIN-ITS-014)

https://campus.plymouth.edu/it/wp-content/uploads/sites/44/2017/10/FIN-ITS-014-Supported-Computer-Equipment.pdf

This policy establishes ITS as being responsible for support and maintenance of all institutional computer equipment.

To Be Replaced By:

- Endpoint Management Standard

No detailed mapping required as the existing policy will be replaced in by the referenced Standard.

DIGITAL MILLENNIUM COPYRIGHT ACT (DMCA) IMPLEMENTATION AT PSU

https://campus.plymouth.edu/it/wp-content/uploads/sites/44/2017/10/Digital-Millennium-Copyright-Act.pdf

This document establishes PSUs procedures for complying with DMCA.

To Be Replaced By:

- DMCA Compliance Standard

No detailed mapping required as the existing policy will be replaced in by the referenced Standard.

APPENDIX A: USNH ACCEPTABLE USE POLICY MAPPING

Note: this information is identical to the same information provided in the stand-alone PSU AUP to USNH AUP Mapping Document.

OVERVIEW

The new USNH Acceptable Use Policy consolidates existing policy provisions from the institutional AUP/CNUPs into a single, comprehensive, USNH-wide Policy that defines acceptable use of information technology resources for all USNH institutions and community members.

MAPPING TO CURRENT POLICIES

The new USNH Acceptable Use Policy does not fundamentally change the intent of the existing institutional policies defining acceptable use of information technology resources. It pulls from all four of the institutional policies to create a comprehensive and inclusive system-wide Policy. Additionally, the new Policy contains:

- Updated language to reflect current, consistent terminology across all Cybersecurity Policies & Standards
- Adjusted responsibilities to address organizational changes
- Explicit Policy requirements in place of vague or general provisions
- Provisions written at the appropriate level of detail, moving implementation or compliance details to the related Standards, where they belong

The following institutional policies will be replaced in full by the new USNH Acceptable Use Policy. A complete mapping of each impacted policy's provisions to the new Policy is provided below.

- PSU – Acceptable Use Policy (FIN-001)

NEW PROVISIONS FOR PSU

As the USNH AUP is a consolidation of the existing institutional policies, there are some policy provisions that will be new for the PSU community.

- **Scope**
  - Includes all uses of USNH or component institution information technology resources irrespective of where those resources are being used
  - Includes personally owned endpoints as described below
  - Allows for Business Application Owners or Technology Service Owners to establish more restrictive requirements for use of specific information technology resources
- **Personally Owned Endpoints**

    - Included in the scope of the policy when used to connect to a USNH network or to perform USNH/institutional business
    - Specific requirements related to the use of personally owned endpoints are outlined
- **Policy Statements**
    - Establishes that USNH information technology resources are shared, and responsible use of those shared resources benefits the entire community
    - Establishes that community members have a responsibility to report any suspicious activity related to any USNH or component institution information technology resource
    - Identifies the following types of use as explicitly prohibited:
        - use that is illegal, disruptive, or that has the potential to negatively impact other community members or shared information technology resources
        - use that violates a USNH or component institution policy, a contractual obligation, or that does not align with the mission of USNH and its component institutions
        - use that is inconsistent with the University System's non-profit status
        - use for the purpose of lobbying that connotes USNH or component institution involvement in or endorsement of any political candidate or ballot initiative
        - Use that results in the display of obscene, lewd, or sexually harassing images or text in a public area or location that can be in view of others
        - use of USNH information technology resources to gain unauthorized access to networks or other information technology resources, whether they belong to USNH or not, with the intent to impair or damage the operation of those resources or exfiltrate information
        - Removal of any USNH-owned or administered information technology resource from its normal location without authorization

PSU – Acceptable Use Policy (FIN-ITS-001) Mapping

Current Policy: https://campus.plymouth.edu/it/wp-content/uploads/sites/44/2017/10/FIN-ITS-001-Acceptable-Use.pdf

Annotations below indicate how each of the provisions in these policies are addressed by the new USNH Acceptable Use Policy and/or the relevant USNH Cybersecurity Standards.

- *Italics* = existing Policy language
- **NP =** USNH Acceptable Use Policy section
- **ST=** USNH Cybersecurity Standard
- **Removed –** provisions that are not being carried forward at this time

I. Purpose of the policy

Computing resources (“Resources”) at Plymouth State University (“PSU”) support the educational, instructional, research, and administrative activities of PSU, and the use of these resources is a privilege *extended to members of the PSU Community. Through the privilege to use Resources, a member of the community may have access to valuable PSU tools, services, and sensitive data. Consequently it is imperative to behave in a responsible, reasonable, ethical, and legal manner.*

The Acceptable Use Policy ("AUP") seeks to ensure that all members of the PSU Community have appropriate access to functional, safe, and timely computing resources. The AUP seeks to prevent any misuse, damage, inappropriate access to, or illegal use of PSU computing resources.

- **NP** = Section 1

II. Applicability and Authority

The Acceptable Use Policy applies to all users of computing resources owned, managed, licensed, or entrusted to PSU, regardless of whether the user is on campus or operating from a remote location. Individuals covered by the AUP include, but are not limited to, PSU Faculty, visiting Faculty, Students, Alumni, Staff, guests, agents of the administration, external individuals, and organizations that access PSU computing resources.

- **NP** = Section 2

Access to and use of any PSU computing resources acknowledges and accepts this AUP as well as any other PSU computing policy. It is each PSU community member's responsibility to keep up-to-date with changes in the computing environment and PSU computing policies, including the AUP.

- **NP** = Section 3

Computing resources include, but are not limited to, all PSU owned, licensed, or managed hardware and software, the PSU telephony system, and the use of the PSU wireless and wired data network regardless of the ownership of the device connected to it. Computing resources also include any and all information maintained in any form, and in any medium, within the university's physical computing resources or by license on other systems.

- **NP** = Section 8

The AUP applies to all PSU owned and/or licensed computing resources, regardless of the department or individual administering, maintaining it, or scheduling its use.

- **NP** = Section 2

III. Detailed Policy Statement

PSU has provided access and use of PSU computing resources to members of the PSU Community with a reasonable expectation of unobstructed use, however in turn each member of the PSU Community is responsible for exercising good judgment and knowing and following the regulations and policies of PSU which apply to their use.

- **NP** = 4.1.1, 4.2.1

Just because an action is technically possible does not mean that the action is appropriate and permitted. Members of the PSU Community must comply with Federal, State and local laws; University and University System rules, regulations and policies; and the terms of applicable contracts – including software licenses – when using PSU computing resources.

- **NP** = 4.2.2 and 4.4.2

Plymouth State University reserves the right to access and affect computing resources to the extent necessary to manage and administer the resources. This includes direct access of data on PSU's networks, PSU owned computing resources, and data stored in PSU systems.

- **NP** = 4.5.5

Acceptable Use is always ethical, reflects academic integrity, and shows restraint in the consumption of shared resources. It demonstrates respect for intellectual property, ownership of data, system security, and freedom from intimidation and harassment.

- **NP** = 4.3.1, 4.3.2

Guidelines for Acceptable Behavior:

Use only computing resources for which you have been granted proper authorization. Access does not imply authorization.

- **NP** = 4.3.3.2

Do not use computing resources to violate any policy or regulation of PSU, the University System of New Hampshire ("USNH"), or federal state or local law

- **NP** = 4.4.2 and 4.4.3.2

Respect the privacy and property of others.

- **NP** = 4.2.2 and 4.5

Employ appropriate standards of civility when communicating with other individuals.

- **NP** = 4.2

Be sensitive to the needs of others, and use only your fair share of computing resources.

- **NP** = 4.3.1

Wired and wireless network services may not be modified or tampered with, nor may they be extended beyond the limits provided.

- **NP** = 4.8.2

You are ultimately responsible for the use of your credentials ("Credentials") and network connection. This includes your account, computer, network address/port, software and hardware.

- **NP** = 4.4.3.1

You must make a reasonable effort to protect your passwords and secure computing resources against unauthorized use or access.

- **NP** = 4.4.3.1

The use of university computing resources is for PSU related work. Persons are not permitted to engage in consulting or other business ventures using PSU computing resources for personal gain or other commercial purposes.

- **NP** = 4.4.3.3

Do not attempt to circumvent any security measure.

- **NP** = 4.4.3.4.3

The following activities are specifically prohibited:

disclosing your password to others;

- **NP** = 4.4.3.1.3

using somebody else's password to gain access to PSU and USNH Resources;

- **NP** = 4.4.3.1.2

forging messages;

- **NP** = 4.4.3.5

cracking passwords and systems;

- **NP** = 4.4.3.4.3

sending harassing or threatening messages;

- **NP** = 4.4.3.2.2

the sending of unauthorized anonymous messages;

- **NP** = 4.4.3.5 and 4.4.3.6.1

misrepresentation of identity;

- **NP** = 4.4.3.5

the sending of bulk unsolicited messages; phishing;

- **NP** = 4.4.3.6.1

entering, without authorization, into any account to use, read, transfer or change the contents in any way;

- **NP** = 4.4.3.1.1

system attacks; denial of services; and other malicious uses of Resources;

- **NP** = 4.4.3.4

altering system software and/or hardware;

- **NP** = 4.4.3.3.4 and 4.4.3.4.1

and using Resources to interfere with the normal operation of computing systems and connected networks.

- **NP** = 4.4.3.3.4, 4.4.3.4.1, 4.4.3.4.3, and 4.4.3.6

IV. Non-compliance

Plymouth State University considers violation of the AUP to be a serious offense, and may lead to disciplinary action and/or criminal prosecution. In accordance with established PSU practices, policies and procedures, confirmation of unexcused inappropriate use of PSU computing resources may result in termination of access, expulsion from the University, termination of employment, legal action, and/or other disciplinary measures.

- **NP** = Section 5

Plymouth State University reserves the right to take actions to investigate and examine potential violations of the AUP, and to protect computing resources from systems and events that threaten or impact operations. Plymouth State University reserves the right to access, monitor, and report the contents and activity to the proper authorities.

- **NP** = 4.5.5

V. Definitions

PSU Plymouth State University Resources Computing and telecommunications equipment (including computers, tablets and cellphones), software and services maintained or contracted by Plymouth State University or the University System of New Hampshire.

AUP Acceptable Use Policy

USNH University System of New Hampshire

Credentials Username, passwords, PIN numbers, copy codes and access codes

- **NP** = Section 8

VI. Related Policies / References for More Information

Written Information Security Protocol ("WISP")

- **NP** = Section 9

University System of New Hampshire

Appendix B: USNH Information Classification Policy Mapping

Note: this information is identical to the same information provided in the stand-alone PSU Sensitive and Confidential Information Policy to USNH Information Classification Mapping Document.

Overview

As the provisions in this policy are split across two USNH policies and several ET&S Standards, a detailed mapping of the provisions in this policy to the new and existing USNH policies and the proposed and planned standards is provided here.

Mapping to Current Policies

In addition to replacing the USNH Data Classification Policy, the following institutional policy will also be replaced in full by the new USNH Information Classification Policy. A complete mapping of each of the impacted policy's provisions to the new Policy is provided below.

- PSU – Sensitive and Restricted Information Policy (FIN-ITS-002)

PSU – Sensitive and Restricted Information Policy (FIN-ITS-002) Mapping

Current Policy: https://campus.plymouth.edu/it/wp-content/uploads/sites/44/2018/10/FIN-ITS-002-Sensitive-and-Confidential-Information.pdf

Annotations below indicate how each of the provisions in this policy are addressed by the new USNH Information Classification Policy and/or the relevant USNH Cybersecurity Standards.

- *Italics* = existing Policy language
- **NP =** USNH Information Classification Policy (or other Policy when named)
- **ST=** USNH Cybersecurity Standard
- **Removed –** provisions that are not being carried forward at this time

Sensitive and Confidential Information / FIN-ITS-002

I. Purpose of the policy

The Sensitive and Confidential Information Policy is intended to help employees determine where information should be stored and what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed without proper authorization. Plymouth

State University expects all users of its administrative data to manage, access, and utilize this data in a manner that is consistent with the University's need for security and confidentiality.

- **NP** = Section 1

II. Applicability and Authority

Applies to all employees including students acting in an employee role (e.g. student workers, grad students, etc.) and anyone granted access to university data.

- **NP** = Section 3

III. Detailed Policy Statement

This policy establishes three data security classifications:

- *Confidential – Specific data elements subject to more stringent security requirements (typically a legal obligation to protect).*
  - **NP** = 4.2, 4.3, 4.4
- *Sensitive – Unless otherwise classified, all information used in the conduct of university business is restricted, and not open to the general public.*
  - **NP** = 4.5
- *Public – University data that has been explicitly made available to the public, with no authentication required.*
  - **NP** = 4.6

All information at Plymouth State University should be protected.

- *Plymouth State University administrative functional areas must develop and maintain clear and consistent procedures for access to university administrative data, as appropriate.*
  - **NP** = 4.7.2

- *Such information shall only be shared between, and released to, authorized parties with a need to know and as necessary to execute job-related duties.*
  - **NP** = Section 4

- *Students exercising their rights pursuant to the PSU Student Handbook shall be considered authorized parties.*
  - **Removed, inconsistent with existing Policy at other institutions**

- *All information that is protected under local, state and federal law is confidential and is to be stored in a secure manner.*
  - **NP** = 4.2, 4.3, 4.4

- *Information not protected by law is sensitive and shared accordingly.*
  - **NP** = 4.5

- *Confidential information is only shared between and disseminated to others in the necessary performance of job duties.*
    - **NP** = Section 4

IV. Procedures

It is NOT permissible to transmit sensitive information via Email unless it is separately encrypted (e.g. Adobe Secure document Envelope).

- **ST=**
    - Public and Sensitive Information Handling Standard
    - Protected Information Handling Standard
    - Restricted Information Handling Standard
    - Confidential Information Handling Standard

All sensitive information, data, and/or files containing sensitive data must be stored in an ITS approved secure location, which includes but is not limited to:

- *PSU/USNH Hosted Shared drive*
- *USNH SharePoint*
- *Secure database (e.g. PSU Banner, USNH Banner)*
- *Encrypted media (Encrypted drive only)*
- *Moodle*
- *Microsoft OneDrive for Business*
    - **ST=**
        - Public and Sensitive Information Handling Standard
        - Protected Information Handling Standard
        - Restricted Information Handling Standard
        - Confidential Information Handling Standard

Upon receiving an appropriately authorized written request from Human Resources, the Chief Information Officer (CIO) or Chief Security Officer (CSO) can grant access to data to support an official investigation of prohibited activity.

- *Information will be disclosed to relevant parties in order to fulfill any requirements pursuant to a subpoena issued for such a purpose, under the direction of the Chief Information Officer (CIO), any Principal Administrator or the President. Information sharing will be limited to only those personnel whose access is required, and such personnel shall respect the sensitive, confidential nature of the investigation.*
    - **ST=** Access to Password Protected Information Standard

Sensitive data includes but is not limited to:

- *Personal Identifying Information*
- *Name in combination with date of birth and/or social security number or other information that can be used to identify an individual.*
    - **NP** = 4.3, 4.4

- *Security-related information (including but not limited to card validation codes/values, full magnetic-stripe data, PINs, and PIN blocks) used to authenticate cardholders and/or authorize payment card transactions.*
    - **NP** = 4.2

- *Any data protected by local, state and/or federal law, such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA),*
    - **NP** = 4.2

- *the Family Educational Rights and Privacy Act of 1974 (FERPA),*
    - **NP** = 4.4

- *the Graham-Leach-Bliley Act of 1999 (GLB).*
    - **NP** = 4.3

- *Confidential academic information such as student performance and/or research on human participants.*
    - **NP** = 4.4, 4.3, 4.2

- *Confidential administrative information such as Human Resources and/or financial records.*
    - **NP** = 4.5

V. Non-compliance

Members of the PSU community who violate this policy will be subject to disciplinary action, up to and including termination of employment and/or expulsion.

- **NP** = Section 5

VI. Definitions

Confidential *All user information that is protected under law.*

Sensitive *All information not protected under law and not deemed public*

- **NP** = Section 8

VII. Related Policies / References for More Information

- *Student Handbook* *http://www.plymouth.edu/office/student-life/psustudent-handbook/handbook/rights-of-students/*

- *Acceptable Use Policy*
- *Email Use Policy*
    - **NP** = Section 9

Policy Title: Sensitive and Confidential Information
Effective date: 08/11/2014
Last Revision: 10/23/2018

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

Appendix C: PSU User Credentials (FIN-ITS-003) Policy Mapping

Note: this information is identical to the same information provided in the stand-alone PSU User Credentials Policy Mapping Document.

Mapping to Current Policies

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

- USNH Cybersecurity Policy
- USNH Password Policy
- Access Management Standard
- Account Management Standard
- Endpoint Management Standard
- Non-Primary Identity Management Standard
- Sponsored/Guest Access Management Standard

PSU – User Credentials Policy Mapping (FIN-ITS-003)

Current Policy: https://campus.plymouth.edu/it/wp-content/uploads/sites/44/2017/10/FIN-ITS-003-User-Credentials.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

User Credentials / FIN-ITS-003

I. Purpose of the policy

Every user has the responsibility to ensure the safe-keeping of each credential entrusted to them.

- **NP =** USNH Password Policy, section 8.2.4
- **ST=** Access Management Standard, Section 4, Community Member Responsibilities

II. Applicability and Authority

This policy covers any user credential provisioned by the University.

- **NP =** USNH Password Policy, section 8.4
- **ST=** Access Management Standard, Section 3

III. Detailed Policy Statement

The safe-keeping of each user credential is the responsibility of the user to whom it is

entrusted.

a. Users should not disclose or share credentials.

- **NP =** USNH Password Policy, section 8.2.4.2
- **ST=** Access Management Standard, Section 4, Community Member Responsibilities

However, they may, at their discretion, share credentials with authorized ITS personnel in order to facilitate troubleshooting and/or repair efforts in their absence.

- **Removed –** not aligned with security best practices or other institutional policy, will not be carried forward to new policies and standards

b. If Credentials must be shared (see III.a), the credentials must never be shared in any form of non-encrypted electronic communications or in which parties cannot be directly verified (e.g. in person). Users must immediately change their password after sharing it (see Password Protection below).

- **NP =** USNH Password Policy, Revised, Password Handling Section

c. Passwords must be sufficiently complex in order to deter certain types of guessing or brute force attacks. Therefore, all passwords must conform to the convention and change intervals defined by ITS as it appears on the Password change page in the myPlymouth portal.

- **NP =** USNH Password Policy, section 8.2.2

d. In the event a user discloses his or her credentials to an unauthorized party, the password must be changed immediately.

- **NP =** USNH Password Policy, section 8.2.5

e. Due to the complexity requirements in conjunction with the number of passwords people have, people may wish to record them somewhere. If such is the case, people must ensure the password is fully secured in a locked location, kept in a password-protected file or other secure method. Users should NOT post passwords on computer monitors, or on hidden pieces of paper under keyboards or other similar methods.

- **NP =** USNH Password Policy, section 8.2.4

IV. Procedures

a. Server- and System-Level Passwords

i. All server/system-level passwords must be changed from vendor defaults and/or after an employee with whom the account was shared is no longer authorized to access the account(s).

- **NP =** USNH Password Policy, section 8.2.1.1

ii. All server/system-level passwords must be no less complex than standard user passwords.

- **NP =** USNH Password Policy, section 8.2.2

iii. Simple Network Management Protocol (SNMP) community strings must be changed from system defaults and must be different from the passwords used to log in interactively. A keyed hash must be used where possible and practical.

- **NP =** USNH Password Policy, Revised, Password Handling Section

b. Password Protection

i. All passwords are confidential. If an account or password is suspected to have been compromised, report the incident to the Chief Security Officer and immediately change the affected password(s).

- **NP =** USNH Password Policy, section 8.2.5.1

ii. Since all users are responsible for the safe-keeping of their passwords, they are responsible for activity from systems that are accessed with their credentials.

- **NP =** USNH Cybersecurity Policy, section 5.8.6
- **ST=** Access Management Standard, Section 4, Community Member Responsibilities

c. New Account Creation

i. All authorized users shall be issued credentials using a process defined by PSU & USNH procedures.

- **NP =** USNH Cybersecurity Policy, section 5.8.8
- **ST=**
  - Access Management Standard
  - Account Management Standard

ii. Additional authorizations and/or credentials may be issued as appropriate to any user requiring access to resources not accessible using their standard credentials.

- **NP =** USNH Cybersecurity Policy, section 5.8.8
- **ST=**
  - Non-Primary Identity Management Standard
  - Account Management Standard

iii. For employees, such authorizations may be modified as required by the user's job responsibilities.

- **ST=** Access Management Standard, Section 4, Authorization – Least Privilege

iv. Access may be de-provisioned and/or modified upon any change in the user's relationship with PSU.

- **NP =** USNH Cybersecurity Policy, section 5.8.8
- **ST=**
  - Access Management Standard, Section 4, Access Management Responsibilities – Deprovisioning Access
  - Account Management Standard

d. Sponsored access

Grantees are responsible for complying with all applicable laws, and established university policies. The Account Sponsor assumes responsibility for educating the grantee about PSU policies, and for the activities carried out while making use of the account. ITS will make no effort to remind the sponsor or grantee prior to expiration.

Accounts in this category are subject to the following parameters:

i. Must not be requested to circumvent existing account policies or standards

ii. Require PA level approval

iii. Limited timeframe (typically 1-3 Months)

iv. Specific expiration date

v. Typical use examples include

1. Temporarily extend access to resources outside the teaching contract dates as means of facilitating the creation of online course content or to enable grade submission.

2. Provide a mechanism for approved vendors to maintain a temporary relationship.

3. Provide access while working on a university project.

4. Provide access for a specific constituent group that does not fit into a normal role (e.g. trustees, Plymouth Police and Fire departments)

- **NP =** USNH Cybersecurity Policy, section 5.8.8
- **ST=**
  - Access Management Standard
  - Account Management Standard
  - Sponsored/Guest Access Management Standard

e. Workstation Security

i. Employee workstations must be locked when unattended. This may be either a manual action or in conjunction with a screen saver that locks the workstation upon activation. Limits are determined based on computer type and use. For example, cluster, instructor and employee workstations will each require different activation times. These time-out intervals are defined by ITS as it appears on the Password Standards page of myPlymouth.

- **NP =** USNH Cybersecurity Policy, sections 5.10.1 and 5.12.7
- **ST=** Endpoint Management Standard

V. Non-compliance

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

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

VI. Definitions

User Credential A combination of a username and password, which together permit access to individual accounts and the resources for which that user is authorized.

Authorized user As defined by standard PSU business practices, any active student, alum, employee or appropriately sponsored user.

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

VII. Related Policies / References for More Information

USNH Password Policy

Plymouth State Policy

- **NP =** USNH Cybersecurity Policy, section 10

Policy Title: User Credentials

Effective date: 08/11/2014

Last Revision: 06/24/2014

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

APPENDIX D: PSU EMAIL USE POLICY (FIN-ITS-004) MAPPING

Note: this information is identical to the same information provided in the stand-alone PSU Email Use Policy 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) POLICY 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 –** while quotas exist, they are substantial, this information is not being carried forward at this time.

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 – aliases will still be provided

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