University System of New Hampshire

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

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

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

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.

University System of New Hampshire

- **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