University System of New Hampshire

USNH PASSWORD POLICY

Responsible Executive/University System Officer: Chief Information Officer
Responsible Office: Information Technology
OLPM Reference: USY.VI.F.5.7.1.2 & 5.7.1.3
Authorized Distribution: Public
Status: APPROVED

1 PURPOSE

The purpose of this policy is to establish the standards for the proper construction, usage, handling and maintenance of passwords at all USNH institutions. This policy applies to applicant, student, prior student/alumni, employee, sponsored user, and contract/vendor level passwords.

2 POLICY STATEMENT

2.1 Password Change Frequency

2.1.1 All passwords associated with USNH accounts must be changed annually with the following exceptions:

- System Administrator Accounts (every six months)
- All non-primary identity accounts accessed by employees with privileged access must have passwords changed upon departure of employee.

2.1.2 Users will be notified of the need to change their password via formal email prior to the password's expiration date in order to remain compliant with this policy.

2.1.3 Users with expired passwords shall be restricted from accessing USNH resources.

2.2 Password Construction

2.2.1 Passwords shall:

- be between 14 and 64 characters in length
- be sufficiently different from previous passwords
- contain a minimum of 5 unique characters

2.2.2 Passwords shall not:

- include the user's first, last, or preferred name, the user's USNH username, or the user's USNH ID

- be re-used
- contain number or character sequences of 4 or more. Examples: abcd, 6789, sTuV
- contain characters repeated 4 or more times. Examples: bbbb, 8888, TttT, &&&&

2.2.3 Known compromised or commonly used weak passwords are disallowed.

2.3 Password Usage

2.3.1 Passwords used for USNH purposes shall not be used for purposes outside of USNH including but not limited to personal banking, Amazon, Netflix, Gmail, etc.

2.3.2 Passwords used for accessing USNH information technology resources that require local application accounts for authentication shall not be the same as the user's USNH password.

- Local application accounts are accounts for official university applications that do not use USNH username and password to log in
- Examples: Salesforce, USNH Benefits

2.4 Password Handling

2.4.1 Passwords shall be treated as sensitive, confidential information.

2.4.2 Passwords shall not be shared with anyone, including administrative assistants or supervisors.

2.4.3 Passwords shall not be written down or stored on-line in clear text.

2.4.4 Passwords shall not be shared in email, chat, electronic forms, or other electronic communication.

2.4.5 Passwords shall not be spoken in front of others.

2.4.6 Users shall not use the "Remember Password" feature of web browsers to store USNH passwords.

2.4.7 Forgotten passwords shall be reset using USNH approved automated mechanisms.

2.4.8 Users with forgotten passwords who are unable to reset their password using automated mechanisms must provide verification of identity via the approved university process.

2.4.9 Members of USNH IT organizations will never ask users to provide their password for any USNH account.

2.5 Compromised Passwords

2.5.1 Users who believe their password has been compromised must notify the Service Desk/Help Desk at their institution immediately.

2.5.2 If USNH has reason to believe a user's password has been compromised, the user's access may be revoked until the password can be reset without notification to the user.

2.5.3 Users with potentially compromised passwords shall provide verification of their identity and must set a new password to regain access to USNH information technology resources.

University System of New Hampshire

3 SCOPE

This policy applies to all passwords used to authenticate to USNH information technology resources or any information technology resource that stores non-public USNH data.

It does not apply to the following types of passwords, the requirements for each are defined elsewhere:

- Service Account Passwords - defined as passwords used by an information technology resource to contact or interface another information technology resource
- UNH Parent Portal Account Passwords

4 AUDIENCE

All USNH employees, students, applicants, sponsored users, contractors, vendors, former employees, and prior students/alumni with access to USNH systems.

5 ENFORCEMENT

Failure to comply with this policy puts USNH information at risk and may result in disciplinary action in accordance with the appropriate institutional disciplinary procedures for students, faculty, and staff, as outlined in the relevant student regulations (e.g., Student Rights, Rules, and Responsibilities), faculty handbooks, or staff handbooks. USNH Faculty or staff who are members of a University-recognized bargaining unit are covered by disciplinary provisions set forth in the agreement for their bargaining units.

Contractors or vendors that fail to comply with this policy may be in violation of their contract with USNH and risk penalties up to contract termination.

6 EXCEPTIONS

Requests for exceptions to this policy must be submitted in writing to the USNH Information Security Officer and may be granted on a case by case basis based on business need and other factors.

7 ROLES & RESPONSIBILITIES

Users

- Comply with all restrictions and requirements outlined in this policy
- Maintain the confidentiality of USNH passwords
- Report all information security events or incidents to UNH Information Security Services

- Notification to users of expiring passwords
- Disabling of accounts with out-of-policy passwords

8 DEFINITIONS

Authentication: Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

Compromised Account: An account that is or has been accessed by an unauthorized party, prior to the password being changed by the authorized user.

Identity: The set of physical and behavioral characteristics by which an individual is uniquely recognizable

Non-Primary Identity: An identity established for a USNH employee or student that is separate from their primary identity. Examples of non-primary identities are Pool, Secondary, Service, Privileged/Admin. Non-primary identities are used to provide different access than an individual's primary identity.

Password: A trusted secret used for authentication.

Primary Identity: The identity associated with a user's USNH username, each individual person has only one primary identity across the entire University System of New Hampshire and its institutions.

Service Account: An account used by an information technology resource to contact or interface another information technology resource.

System Administrator Account: Account associated with a non-primary identity used by members of the USNH community to administer information technology resources.

User-level Password: Passwords associated with primary and non-primary identity accounts that are used by an individual user to authenticate. Passwords used by information technology resources to authenticate to other information technology resources, without human intervention, are not user-level passwords.

9 RELATED POLICIES, STANDARDS, PROCEDURES, AND GUIDELINES

USNH Information Security Policy (in development)

University System of New Hampshire

CONTACT INFORMATION

SUBJECT	CONTACT	EMAIL/URL
Policy Questions Report a Violation Request for Information	USNH Information Security Officer	It.security@unh.edu

DOCUMENT HISTORY

Effective Date:	20 JAN 2020
Approved by:	USNH ISC, 20 NOV 2019 B POIRIER, USNH CIO, 19 Dec 2019 ADMIN BOARD, 9 JAN 2020
Reviewed by:	B POIRIER, USNH CIO, 23 OCT 2019 USNH ISC, 20 NOV 2019
Revision History:	Revised per USNH CIO review, 24 OCT 2019