Credentials and Password Maintenance Policy

APPROVED BY POLICY COMMITTEE 4/15/24 Effective Date 4/15/2024

(Impact Area – Dept Name) SUNY Morrisville *Morrisville Campus *Norwich Campus *EOC	(General Subject Area) Administrative	(Specific Subject Area) Password Maintenance
	Author: Technology Services	**Supersedes Policy #**
Relates to Procedure #	**Impact:**	
Legal Citation (if any):		
SUNY MORRISVILLE		

Policy Summary [Page 1 of 4]

The purpose of this policy is to provide best practices and guidelines for the security of account credentials and the passwords. A weak password may result in the compromise of individual systems and services, exposure of sensitive data and personally identifiable information (PII). This policy outlines appropriate steps to select and secure passwords.

1. Scope

This policy applies to any person who is provided authentication credentials by SUNY Morrisville for access to the various electronic services both internal and 3rd party (cloud). This applies, but is not limited to, faculty, staff, students, guests, contractors, partners, vendors, etc.

2. Policy

2.1 Password Creation

SUNY Morrisville mandates and enforces that all persons change their passwords from the default generated password, upon credential distribution or at first use. Selection of a new password must adhere to the following guidelines for password creation per NIST 800-63B by the National Institute of Standards and Technology:

- Must be at least **10** characters in length.
- Should meet complexity requirements, comprised of upper-case and lower-case characters (A-Z, a-z), digits (0-9) and special characters (punctuation marks and symbols).
- Must not be any of the previous 10 chosen passwords.
- Should not be known to have been exposed by any previous breaches or compromises.
- Should not be comprised of a single word that can be found in a dictionary (phrases or combined words are better).
- Should not be comprised of an obvious keyboard sequence (ex: qwerty7890, asdfGH123).
- Should not include personal information such as birthdates, addresses, phone numbers, or names of family members, pets, friends, and fantasy characters.
- Should not be comprised of work-related information such as building names, system commands, sites, companies, hardware, or software.
- Should not be any of the above spelled backward or preceded or followed by a number (ex: secret123, password123, JustPutAOneAfterIt1).

2.2 Confidentiality

Credentials for authentication should be treated as sensitive and confidential information. The following guidelines apply to maintain the confidentiality of a person's credentials:

- Persons must not disclose their credentials to anyone (co-workers, managers, family, friends, etc.).
- Managers / Supervisors are not authorized to request credentials from staff.
- Persons must not write down their credentials and leave them unsecured.
- Persons must not send their credentials via email, phone, or any mode of communications.
- Persons must not utilize the same password for their SUNY Morrisville college credentials as for other non-University related accounts and access.
- Do not reveal a password on questionnaires or security forms.
- Do not hint at the format of a password (ex: "my pet name")
- Do not use the "Remember Password" feature of applications (for example, web browser)

2.3 Account Lockout

- A person's credentials will be locked out after 3 failed authentication attempts.
- The credential lockout duration will be 15 minutes.
- Further attempts, post lockout is limited to 1 failure, resulting in subsequent lockouts, with restoration of the 3-attempt limit commencing one hour after the next successful logon.

2.4 Change Frequency

The Frequency of password resets has evolved. Per NIST 800-63B:

- All system-level passwords (for example, administration accounts, switches, routers, firewall, and so on) must be changed at least every 180 days.
- Persons are encouraged to utilize longer length passwords in exchange for periodic changes to shorter length passwords. (See increased length requirement in section 2.1). Reduction in frustrations arising from repeated changes, often across multiple devices, lead to the choice of simpler or weak passwords that are easier to remember.
- Password resets should only be done when there is good reason, either at the request of that person or that the password has been compromised. There is no periodic time limit enforced.

2.5 Incident Reporting

The Technology Services department will monitor for any suspicious activities regarding credential usage to minimize or eliminate unauthorized access or exploitation of the campus network/system resources.

- It is the person's responsibility to report any suspicious activity to the Technology Services department.
- Request of passwords over the phone, email or any mode of communications should be expediently reported to the Technology Services department.
- The Technology Services department may request, or trigger enforced password reset procedures if there have been indicators of compromise of a person's credentials.

3. Enforcement

This policy will be enforced by the Technology Services department and verify compliance through various methods, including but not limited to periodic network traffic and activities monitoring, tool reports, internal and external audits, and feedback.

- Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination.
- Where illegal activities are suspected, the Technology Services department will report such activities to University Police.
- If any provision of this policy is found to be unenforceable or voided for any reason, such invalidation will not affect any remaining provisions, which will remain in force.

Reference: ***https://www.sans.org/security-resources/policies***

https://csrc.nist.gov/

https://www.educause.edu/cybersecurity-and-privacy-guide

Contact Information

Technology Services
Ground Floor – Charlton Hall
Morrisville, NY 13408

Phone: (315) 684-6053