University Administrative Policy

Policy Name: Password Protection Policy
Responsible Office: Information Security
Originator of the Policy: Chief Information Security Officer
Effective Date: July 24, 2017
Revision History:
Web Link: https://records.salemstate.edu/policy/password-protection-policy

1. Rationale

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of Salem State University's resources. All users, including contractors and vendors with access to Salem State University systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

2. Statement of Policy

2.1 Password Creation

2.1.1 All user-level and system-level passwords must conform to the following.
2.1.2 2.1.1.1 All passwords must have a minimum of 14 characters.
2.1.3 2.1.1.2 All passwords must contain three of four of each of the following types of characters including a lower case letter, an upper case letter, a numeric, and a symbol.
2.1.4 Users must not use the same password for Salem State University accounts as for other non-Salem State University access (for example, personal ISP account, option trading, benefits, and so on).
2.1.5 Where possible, users must not use the same password for various Salem State University access needs.
2.1.6 User accounts that have system-level privileges granted through group memberships or programs such as sudo must have a unique password from all other accounts held by that user to access system-level privileges.
2.1.7 Where Simple Network Management Protocol (SNMP) is used, the community strings must be defined as something other than the standard defaults of public, private, and system and must be different from the passwords used to log in

interactively. SNMP community strings must meet password construction guidelines.

2.2 Password Change

2.2.1 All system-level passwords (for example, root, enable, NT admin, application administration accounts, and so on) must be changed on at least a quarterly basis.

2.2.2 All user-level passwords (for example, email, web, desktop computer, and so on) must be changed at least annually. The recommended change interval is annually.

2.2.3 Password cracking or guessing may be performed on a periodic or random basis by the Information Security department or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it to be in compliance with the Password Policy.

2.2.4 Passwords for employees in specific departments and/or functions must change their user password every 90 days including Finance and Accounting, Human Resources, Information Technology Services, and Counseling and Health Services.

2.3 Password Protection

2.3.1 Passwords must not be shared with anyone. All passwords are to be treated as Confidential Salem State University information.

2.3.2 Passwords must not be inserted into email messages or other forms of electronic communication.

2.3.3 Passwords must not be revealed over the phone to anyone except for password reset.

2.3.4 Do not reveal a password on questionnaires or security forms.

2.3.5 Do not hint at the format of a password (for example, "my family name").

2.3.6 Do not share Salem State University passwords with anyone, including administrative assistants, supervisors, managers, co-workers while on vacation, and family members.

2.3.7 Do not write passwords down and store them anywhere. Do not store passwords in a file on a computer system or mobile devices (phone, tablet) without encryption.

2.3.8 Do not use the "Remember Password" feature of applications (for example, web browsers).

2.3.9 Any user suspecting that his/her password may have been compromised must report the incident and change affected password(s) and report incident to Information Security or Information Technology Services.

2.3.10 Any user should take all precautions to protect their password from disclosure including from shoulder surfing.

2.4 Application Development

Application developers must ensure that their programs contain the following security precautions:

2.4.1 Applications must support authentication of individual users, not groups.

2.4.2 Applications must not store passwords in clear text or in any easily reversible form.

2.4.3 Applications must not transmit passwords in clear text over the network.

2.4.4 Applications must provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

2.5 Use of Passwords and Passphrases

Passphrases are preferred and are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

"The*?#>*@TrafficOnThe101Was*&#!#ThisMorning"

All of the rules above that apply to passwords apply to passphrases.

3. Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Salem State University facility, Salem State University network, or Salem State University information.

The scope of this policy includes all applications and Social Media accounts used on behalf of Salem State University and used by Salem State University staff, students, administrators, consultants, and other authorized third parties.

4. Fiscal Considerations

	Direct Costs / Savings / Revenue Generation	**Indirect Costs / Savings / Revenue Generation**
Initial Implementation	N/A	
Ongoing		

5. Responsibilities

Responsible Party	**List of Responsibilities**
Chief Information Security Officer	

6. Policy Enforcement

Compliance measurement	The Information Security department will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

	Any exception to the policy must be approved by the Information Security department in advance.
Potential violation consequences	An employee found to have violated this policy may be subject to disciplinary action up to and including termination of employment.
How to report	Chief Information Security Officer, 978.542.2745

7. Reference Documents

Policy or Document	**Web Address**
SANS Glossary	https://www.sans.org/security-resources/glossary-of-terms/ Simple Network Management Protocol (SNMP)
Information Security Policy	https://records.salemstate.edu/sites/records/files/policies/Information%20Security%20Policy.pdf
Acceptable Use Policy	https://records.salemstate.edu/sites/records/files/policies/Acceptable%20Use%20Policy.pdf
Email Policy	https://records.salemstate.edu/sites/records/files/policies/Email%20Communication%20Policy.pdf

8. Contact(s)

Subject	**Office or Position**	**Telephone Number**	**Email**
Passwords and/or Information Security	Chief Information Security Officer	978.542.2745	tcesso@salemstate.edu
Passwords and/or Information Security	Associate Director of Information Security	978.542.2739	jvalente@salemstate.edu

9. **Effective Date:** Upon approval by the president.

10. **Dissemination:** Posted on the university web site.

11. **Review Cycle:** Initial review after 12 months; subsequent review every 5 years.