Authentication Policy

Issued 6/17/2024

Version 52

Purpose

Salem State University (hereafter referred to as “Salem State”) utilizes passwords and multi-factor authentication to provide secure access to a number of important electronic systems and applications. This policy establishes a standard for the creation, maintenance and usage of passwords within Salem State systems.

Scope

This policy applies to anyone receiving an account on any Salem State computer or system.

Policy

Your user ID and password serves as your primary digital identity at Salem State. It works in tandem with Salem State’s Active Directory and LDAP (Lightweight Directory Access Protocol) to provide the foundation of authentication (who you are) and authorization (what you can do).

Salem State requires that the guidelines below are followed when accessing secure systems at the University, which follow the SANS institutes Password Construction Guidelines and Password Protection Policies. This applies to all personnel, students, business partners, contractors and consultants utilizing Salem State electronic systems, regardless of their actual physical location:

General Guidelines

* Whenever possible, systems will rely on the University’s Active Directory or Azure system to integrate username/password information. Two-factor systems shall be used whenever possible to further protect against attackers exploiting credentials to gain access to data and systems.

* Each user is responsible for maintaining the confidentiality of passwords and any other authentication factors that are used to gain access to University systems and services.

* Passwords and other authentication factors should not be shared with anyone, including assistants. All authentication factors are to be treated as sensitive, confidential information. It is permissible to share your password with Information Technology support personnel for troubleshooting purposes only and you should change your password immediately after the work is performed.

* Passwords used to gain access to personal systems or services should always be different from passwords used to gain access to University systems or services.

* If a password is compromised or believed to be compromised, users will inform the Help Desk and, if possible, change it immediately.

* Passwords should not be written down or stored electronically without encryption.

* Users should never attempt discovery of a system or another user’s passwords.

Password Construction Guidelines

Strong passwords are long. The more characters a password has the stronger it is. We recommend a minimum of 16 characters in all work-related passwords. In addition, we encourage the use of passphrases, passwords made up of multiple words. Examples include “It’s time for vacation” (spaces are allowed) or “block-curious-sunny-leaves”. Passphrases are both easy to remember and type yet meet the strength requirements.

Password cracking or guessing may be performed on a periodic or random basis by the ITS Security Team or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including loss of access rights and/or termination of employment under adherence to their respective collective bargaining agreement. Students found to have violated this policy may have their access removed and may have additional actions taken as directed by the Student Code of Conduct.

Security Level Public