Password Policy

Objective

The purpose of the Password Policy is to establish parameters for secure authentication when accessing University Information Resources. Access to University Information Resources by an unauthorized party may cause loss of information, a breach of confidentiality and/or integrity, and may compromise availability.

Applicability

The Password Policy applies to students, faculty or staff members, whether full-time or part- time, paid or unpaid, temporary or permanent, as well as all agents and representatives of the University, including any third party service provider providing services to the University who create, use or otherwise access or interact with any University Information or University Information Resource ("University Users").

Definitions

University Information: any information in any form whether electronic, hardcopy, audial, or otherwise which is created, collected, stored, accessed or used in connection with the operation and/or management of the University, or which is created, collected, stored, accessed or used by a party authorized by the University.

University Information Resource: any tool, device, equipment, or system used to create, collect, record, process, store, retrieve, display and transmit University Information, including but not limited to email, mainframes, servers, computers, laptops, personal digital assistants (PDA), telecommunication resources, fax machines, printers, file cabinets, software and embedded technology.

Policy

- Any and all passwords, including initial passwords, must meet the following requirements when technically feasible:
    - must be changed at least every 120 days
    - must not be anything that can be easily tied back to the account owner such as: user name, social security number, nickname, relative's names, birth date, etc
    - must have a minimum length of 8 alphanumeric characters
    - must contain a mixture of both upper and lower case characters
    - must include at least one (1) number and one (1) special character, such as: # $ % ^ * ( ) _ + | ~ - = \ : ; < > ? , . / @
    - must lock a User Account after ten (10) invalid login attempts, and will require an authorized administrator to unlock the account
    - must be forced to be changed upon first use
    - must keep history for at least two (2) previous passwords
    - must be encrypted during transmission and storage
- A screen-saver or a power timeout shall be configured after a period of 15 minutes (staff) and 30 minutes (faculty) of idle activity to the extent technically feasible, and such timeout shall require password re-enter
- Default passwords must be changed prior to system use.
- Stored passwords must be encrypted when feasible.
- User account passwords must not be shared with anyone. Suffolk University Information Technology Services (ITS) and ITS third-party service providers will not ask for University User account passwords.
- University Users must not circumvent password entry with auto logon, application remembering, embedded scripts or hardcoded passwords in client software, except for University User email which is password secured by the overlaying operating system on University User workstations or personal digital assistants (PDA).

- Computing devices must not be left unattended without enabling a password-protected screensaver or logging off of the device.

If a University User suspects or has reason to know that the security of a password may be compromised, the password must be changed immediately. Under such circumstances, University Users should immediately report the discovery to the Suffolk University ITS Help Desk (617) 557-2000.

Users should contact the ITS Helpdesk to change a password. When a user seeks a password change, ITS must undertake the following procedures:

- authenticate the User's identify before changing the password
- change to a strong password
- require the User to change the password at first login.

Violation of Policy

The University reserves the right to monitor network traffic, perform random audits, and to take other steps to insure the integrity of its information and compliance with this Policy. Violations of this Policy may lead to appropriate disciplinary action, which may include temporary or permanent restrictions on access to certain information or networks. Willful or repeated violations of this Policy may result in dismissal from the University.

Revision History

Version	Date	Responsible University Office	Approved By
1.0	09/14/10	Provost Office	Provost Barry Brown
1.1	02/12/13	Senior VP of Finance and Administration and Treasurer Office	Senior VP Danielle Manning