JACKSON STATE COMMUNITY COLLEGE

TBR Policy Reference: Original Date Effective: July 10, 2008
TBR Guidelines Reference: G-051 Modified Date: October 16, 2015
SUBJECT: Password Policy Approved By: Dr. Bruce Blanding, President
Office Responsible: Office of Information Technology

Purpose

Passwords are a critical part of information and network security. Passwords serve to protect user accounts, but a poorly chosen password, if compromised, could put the entire network of Jackson State Community College at risk. As a result, all employees of Jackson State Community College are required to take appropriate steps as outlined below to ensure that they create strong, secure passwords and keep them safeguarded at all times. The purpose of this policy is to set a standard for creating strong passwords, protecting those passwords, and establishing a frequency for changing those passwords.

Scope

This policy applies to all employees who have access to any technology resource (such as servers, computers, network, email, Banner, E-Learn, data, etc.) at Jackson State Community College that requires a password to gain access.

Policy

- A combination of personal user ID for identification and a unique password for authentication will be required of all users before they are allowed access institutional networks and systems.

- Passwords will be used for authentication of access to all institutional networks and systems.

- The effectiveness of passwords to protect access to the institution's information directly depends on strong construction and handling practices.

Password Construction

All users must construct strong passwords for access to all institution networks and systems, using the following criteria where technically feasible:

- Must be a minimum of 8 characters in length.

- Must be composed of a combination of at least three of the following four types of characters:
  a. Upper case alphabetic character;
  b. Lower case alphabetic character;
  c. Numeric character;
  d. Non-alphanumeric character (special characters)

- Or as an alternative
  a. A passphrase of a minimum of 14 characters.

- Old passwords cannot be re-used for a period of one year.
Password Management

The following requirements apply to end-user password management.

- Storage and Visibility
  a. Passwords must not be stored in a manner which allows unauthorized access.
  b. Passwords will not be stored in a clear text file.
  c. Passwords will not be sent via unencrypted e-mail.

- Changing Passwords
  a. Users must change their passwords at least every 365 days. (Student accounts are an exception to this requirement)
  b. Users who process or access restricted data (such as protected health information, student FERPA data, and Social Security Numbers or other personally identifiable information) should change their passwords at least every 90 days.
  c. Users with privileged accounts (such as those with root or administrator level access) must change their passwords at least every 90 days.
  d. Passwords must be changed immediately if any of the following events occur:
     1. Unauthorized password discovery or usage by another person;
     2. System compromise (unauthorized access to a system or account);
     3. Insecure transmission of password;
     4. Accidental disclosure of a password to an unauthorized person; or
     5. Status changes for personnel with access to privilege and/or system accounts.

Password Protection – System Accounts

- System accounts can be defined as:
  a. Accounts used for automated processes without user interaction.
  b. Accounts used for device management.

- System accounts are not required to expire but must meet the password construction requirements above.

- Vendor provided passwords must be changed upon installation using the password construction requirements above.

Compliance and Enforcement

- The policy applies to all users of information resources including students, faculty, staff, temporary workers, vendors, and any other authorized users.

- Any employee who is found to have violated this policy may be subject to disciplinary action.

- Justification for exceptions to this policy must be documented.

General Procedures

This policy will be posted to JSCC internal website and each employee is responsible for reading and noting any changes to the policy.