Dyersburg State Community College

Policies and Procedures

11:04:05:00 Password Management Policy

Purpose:

The purpose of this guideline is to establish a minimum expectation with respect to password construction in order to protect data stored on computer systems at DSCC.

Scope:

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

Policy:

1. Policy
   a. A combination of a personal user login ID for identification and a unique password for authentication will be required of all users before they are allowed access to institutional networks and systems.
   b. Passwords will be used for authentication of access to all institutional network and systems except where strong authentication methods are deemed necessary.
   c. The effectiveness of passwords to protect access to the institution's information directly depends on strong construction and handling practices.
2. Password Construction
   a. All users must construct strong passwords for access to all institution networks and systems, using the following criteria where technically feasible:
   i. Must be a minimum of 10 characters in length
   ii. Must be composed of a combination of at least three of the following four types of characters:

1. Upper case alphabetic character;
2. Lower case alphabetic character;
3. Numeric character;
4. Non-alphanumeric character
   a. Valid special characters include (!%*+-/:?_
   iii. Or, as an alternative:

1. A passphrase of a minimum of 14 characters

3. Password Management – End User or Privileged Accounts
   a. The following requirements apply to end-user password management.
   i. Storage and Visibility

1. Passwords must not be stored in a manner which allows unauthorized access. For example, passwords can not be displayed in clear view.
2. Passwords will not be stored in a clear text file.
3. Passwords will not be sent via unencrypted e-mail.
   ii. Changing Passwords

1. Users must change their passwords at least every 120 days.
2. Users with privileged accounts (such as those with root or administrator level access)
   must change their passwords at least every 120 days.

4. Password Management – System Accounts
   a. System Accounts are not required to expire but must meet the password construction requirements above (where supported by the underlying technologies).
   b. Vendor provided passwords must be changed upon installation using the password construction requirements above.
5. Password Protection – All Accounts
   a. Passwords must be changed immediately if any of the following events occur:
   i. Unauthorized password discovery or usage by another person;
   ii. System compromise (unauthorized access to a system or account);
   iii. Insecure transmission of a password;
   iv. Accidental disclosure of a password to an unauthorized person; or
   v. Status changes for personnel with access to privileged and/or system accounts.
6. References
   a. TBR Policy – Access Control: 1.08.03.00 -formerly G-051 & G-052

Compliance:

All faculty, staff, students, temporary employees and vendors utilizing DSCC’s information resources must comply with this policy. Anyone found to have violated this policy may be subject to disciplinary action or suspension of their account. Justifications for exceptions to this policy must be documented and approved by the Vice President for Technology.

Definitions:

System Accounts – Accounts used for automated processes without user interaction or accounts used for device management.
Passphrase – A sequence of words or other text used to control access to a computer system

Revision History:

Policy approved by Administrative Council on 10/31/14. Policy approved by Administrative Council on 1/31/2020