PASSWORD POLICY AND PROCEDURES

INTRODUCTION

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

1.0 – POLICY

1.1 The Department of Postsecondary Education’s Information Services Division is committed to maintaining systematic controls over access to the Department’s data and resources. Therefore, all users, including contractors and vendors with access to DPE systems, are required to create and use strong passwords.

1.2 All user-level and system-level passwords must conform to the *Password Construction Guidelines*.

1.3 Users must not use the same password for DPE accounts as for other non-DPE access (for example, personal email, banking, etc…).

1.4 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.

1.5 All user-level passwords (for example, email, web, desktop computer, and so on) must be changed at least every four months.

1.5.1 All user-level passwords for Executive Directors, Vice Chancellors, the Deputy Chancellor, the Chancellor, and other accounts with access to highly sensitive information must be changed at least every 60 days.

1.6 Password cracking or guessing may be performed on a periodic or random basis by the Staff of the Information Services Division 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 Construction Guidelines* in Section 3 of this document.

1.7 Passwords must not be shared with anyone. All passwords are to be treated as sensitive, Confidential DPE information.

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

1.9 Passwords must not be revealed over the phone to anyone.

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

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

1.12 Do not share DPE passwords with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, and family members. Documents and files that may need to be shared with administrative assistants, secretaries, managers, co-workers should be saved on the appropriate network drive.

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

1.14 Any user suspecting that his/her password may have been compromised must report the incident to the Director of Information Services and change all passwords.

1.15 The Information Services Division will verify compliance to this policy through various methods, including but not limited to, periodic walk-thrus, business tool reports, internal and external audits, and feedback to the policy owner.

1.16 Any exception to the policy must be approved by the Deputy Chancellor only upon the recommendation of the Director of Information Services in advance.

2.0 - PROCEDURES

2.1 The Information Services Division uses Group Policy to enforce compliance to strong password standards and password expiration.

2.1 A **strong** password for DPE follows these rules:

- A minimum of 8 characters
- Cannot contain the User's account name
- Contains at least one character from 3 of the following 4 categories
  - Uppercase letters (A-Z)
  - Lowercase letters (a-z)
  - Numbers (0-9)
  - Special Characters (e.g., !@#$%^&*(_+=<>/?{}{][-)
- Cannot be the same as any previously used passwords

3.0 GUIDELINES

These are general "rules of thumb" to apply to password.

3.1 Creating a **strong password**:

- Combine short, unrelated words with numbers or special characters.
  For example:
  Random Word #1 – **lobster**
  Random Word #2 – **phone**
  A significant number - **42**
  A non-obvious method: **The 3rd letter of each word will be capitalized**
  Put them all together: **loBster42phOne**

- Make the password difficult to guess but easy to remember
- Substitute numbers or special characters for letters. (But do not just substitute)
  For example:
  - **brownhat** - is a bad password
  - **Br0wnHat** - is better and satisfies the rules, but setting a pattern of 1st letter capitalized, and o's substituted by 0's can be guessed
  - **bR0wnh@T** - is far better, the capitalization and substitution of characters is not predictable

3.2 Avoid passwords that are easy to guess. That means they **should <u>not</u>:**

- be your Username
- be your name
- family member names
- be your nickname
- be your social security number
- be your birthday
- be your license plate number
- be your pet's name
- be your address
- be your phone number
- be the name of your town or city
- be the name of your department
- be street names
- be makes or models of vehicles
- be slang words
- be obscenities
- be technical terms
- be school names, school mascots, or school slogans
- be any information about you that is known or is easy to learn (favorite - food, color, sport, etc.)
- be any popular acronyms
- be words that appear in a dictionary
- be the reverse of any of the above