Password Policy

Policy Information

Issuing Office

Information Services

Affected Parties

Students, Faculty, Staff, Alumni

Policy Language

All Liberty University systems will be accessed via a user account that is protected by a password that meets standardized strength checks (as defined below) to improve protection against hacking attempts, and ensure compliance with Payment Card Industry (credit card merchant) regulations.

Policy Rationale

This policy defines the necessity for adequate password protection of all Liberty University network user accounts.

Definition of Glossary Terms

None specified

Procedural Information

Procedures

1.? General password standards.

1.1.? All users shall avoid keeping a record (e.g. paper, software file or hand-held device) of passwords, unless this can be stored securely.?

1.2.? Users shall change passwords whenever there is any indication of possible system or password compromise

1.3.? Users shall not share individual user passwords. Liberty University will never ask a user for their password.

1.4.? Users shall not use the same password for business and non-business purposes.

2.? Students and Alumni passwords.?

2.1.? Must be a minimum of eight (8) characters in length.

2.2.? Must contain at least 3 of the following character sets:

2.2.1. Upper case alphabetic (A-Z)

2.2.2. Lower case alphabetic (a-z)

2.2.3. Numerals (0-9)

2.2.4. Special characters (%, +, , !, #, ^, ?, :, ., ~, -, _)??

2.2.4.1.? NOTE: the following special characters are prohibited: $ & ; ( ) [ ] { } " ' ` * @ /

2.3.? The alphabetic portion must not be a single common dictionary word. For example, ?Liberty1? is prohibited. Multi-word phrases such as, ?2BigBoxes? are allowed.

2.4.? Students and alumni must change their passwords yearly.

2.5.? The new password cannot be the same as any of the previous 10 passwords that the student or alumnus has used.

3.? Faculty and Staff passwords.

3.1.? Must be a minimum of ten (10) characters in length.

3.2.? Must contain at least 3 of the following character sets:

3.2.1. Upper case alphabetic (A-Z)

3.2.2. Lower case alphabetic (a-z)

3.2.3. Numerals (0-9)

3.2.4. Special characters (%, +, , /, !, #, ^, ?, :, ., ~, -, _) 3.2.4.1.? NOTE: the following special characters are prohibited: $ & ; ( ) [ ] { } " ' ` * @

3.3.? The alphabetic portion must not be a single common dictionary word. For example, ?Liberty1? is prohibited. Multi-word phrases such as, ?2BigBoxes? are allowed.

3.4.? Faculty and staff must change their passwords every 90 days.

3.5.? The new password cannot be the same as any of the previous 10 passwords that the faculty or staff member has used.

4.? IT System Administrator passwords.

4.1.? Must be a minimum of fifteen (15) characters in length.

4.2.? Must contain at least 3 of the following character sets:

4.2.1. Upper case alphabetic (A-Z)

4.2.2. Lower case alphabetic (a-z)

4.2.3. Numerals (0-9)

4.2.4. Special characters (%, +, , /, !, #, ^, ?, :, ., ~, -, _)

4.2.4.1.? NOTE: the following special characters are prohibited: $ & ; ( ) [ ] { } " ' ` * @

4.3.? The alphabetic portion must not be a single common dictionary word. For example, ?Liberty1? is prohibited. Multi-word phrases such as, ?2BigBoxes? are allowed.

4.4.? IT System Administrators must change their passwords every 90 days.

4.5.? The new password cannot be the same as any of the previous 10 passwords that the IT System Administrator has used.

5.? Password Lockouts and Resets.

5.1.? In almost all cases, users will be able to reset passwords without assistance from the IT Helpdesk.?? If a user makes 5 faulty attempts when entering his or her password, the account will be locked.? It will unlock automatically 30 minutes later so that they can reset their password without IT assistance.

Sanctions

None specified

Exceptions

None