Password Policy

General Description

Purpose:
Trinity University is committed to a secure information technology environment in support of its mission. In today's environment, the need for a strong password policy is greater than ever. Many systems at the University require the use of passwords including but not limited to e-mail, academic and administrative applications, computing labs, netfiles, and VPN. A poorly chosen password may result in the compromise of Trinity University's entire network. The Password Policy ensures a consistent measure of security for the University's Information and Technology resources as well as the safeguard of personal and confidential information of the University community.

Scope:
The Password Policy applies to all persons accessing the TUNetwork regardless of their capacity, role or function. Such persons include students, faculty, staff, third party contractors, visitors (guests), consultants and employees fulfilling temporary or part-time roles.

Policy Content

All Trinity owned electronic devices must have password protection enabled. Users are required to comply with the following guidelines for passwords:

- All passwords (e.g., email, Internet, voice mail, computer, smartphones, etc.) must be changed at least every 12 months. Individuals with access to critical areas of information will be required to change their T.U. password at least every 90 days. Such users will be identified by the Director of Information Technology Services. For example, employees of Trinity University with “change level access” to the university administrative system(s) will be required to change their passwords every 90 days.

- Passwords must not be inserted into email messages or other forms of electronic communication and should not be shared with anyone, including via email or phone conversations.

- Passwords should not be written down or stored electronically without encryption.

- Individuals are responsible for safeguarding passwords for computing accounts. Passwords must not be shared or disclosed to anyone, including friends or family. Passwords that are found to be compromised, should be changed immediately.

- All passwords must be at least 8 characters long, contain at least 2 numbers or special characters, not be a word in the dictionary, and not be part of your name or user name. If the device or application does not permit a password to meet these criteria, the password
should satisfy as many of these criteria as possible.

**Guidelines and suggestions for creating strong passwords.**

**Performance Evaluation**

**Consequences of Policy Violation:**

**Enforcement**

Any behavior in violation of this policy is cause for disciplinary action. Violations will be adjudicated, as appropriate, by the CIO, the Office of the Dean of Students, the Office of Housing and Residential Life, and/or the Office of Human Resources. Sanctions as a result of violations of this policy may result in, but are not limited to, any or all of the following:

- Attending a class or meeting on password policy issues, as well as successful completion of a follow up quiz;
- Loss of University computing, email and/or voice mail privileges;
- Disconnection from the residential hall internet network;
- University judicial sanctions as prescribed by the student Code of Conduct;
- Monetary reimbursement to the University or other appropriate sources;
- Reassignment or removal from University housing and/or suspension or expulsion from the University;
- Prosecution under applicable civil or criminal laws;
- Employees may be subject to disciplinary action.

**Violations**

Reports of compromised passwords should be reported to ITS immediately (helpdesk@trinity.edu / 210-999-7401).

**Requirements**

**Approvals:**

Chief Information Officer
Terms and Definitions:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>A secret series of characters that enables a user to access a file, computer, or program.</td>
</tr>
</tbody>
</table>

Revision Management

Revision History Log:

<table>
<thead>
<tr>
<th>Revision #:</th>
<th>Date:</th>
<th>Recorded By:</th>
</tr>
</thead>
<tbody>
<tr>
<td>v1.0</td>
<td>8/14/2019 5:06 PM</td>
<td>Courtney Cunningham</td>
</tr>
</tbody>
</table>