XAVIER UNIVERSITY

Password Policy

Effective: September 17, 2018

Last Updated: N/A

Responsible University Office: Information Technologies

Responsible Executive: Associate Provost and Chief Information Officer

Scope: This policy applies to all University owned information that is present on or transmitted through University owned systems and networks. University owned information assets can take the form of electronic and hard copy information.

A. REASON FOR POLICY

Passwords are the primary form of authentication used to grant access to Xavier University information systems. To ensure that password provide as much security as possible, they must be carefully created and used.

Without strict usage guidelines, the potential exists that passwords will be created that are easy to break, thus allowing easier illicit access to Xavier University information systems, and thereby compromising the security of those systems.

B. POLICY

The Password Policy applies to all information systems, and all individuals that have access to Xavier's information resources, including but not limited to: all faculty, staff, students, alumni, retirees, temporary workers, library patrons, visitors, contractors and vendors using University information resources, whether on- or off-site (hereafter collectively referred to as "Users").

Where feasible passwords will be maintained in the following manner:

1. Passwords must be constructed according to set length and complexity requirements. As such, passwords must be at minimum 12 characters in length and must include 1 upper and 1 lower case letter, and a minimum of 1 number. The password may also contain the following Banner special characters;
   ! % * + - / : ?_ ' ;

2. Passwords will have both a minimum and maximum lifespan. As such, passwords must be replaced at a maximum of 180 days and at a minimum of 30 days
3. Passwords may not be reused any more frequently than every 15 password refreshes. Reuse includes the use of the exact same password or the use of the same root password with appended or pre-pended sequential characters.
4. Passwords are to be used and stored in a secure manner. As such, passwords are not to be written down or stored electronically. Passwords are to be obscured during entry into information system login screens and are to be transmitted in an encrypted format.
5. Passwords are to be individually owned and kept confidential and are not to be shared under any circumstances.

Other applicable policies and/or resources:

This document is part of the University's cohesive set of security policies. Other policies may apply to the topics covered in this document and, as such, the applicable policies should be reviewed as necessary. Please refer to the other Xavier security policies below for further information:

Acceptable Use Policy

Remote Access

Vulnerability Management

Data Classification

Incident Response

Technology Services Website – Accounts & Password

User Account Policy

Web Privacy Policy

Information Technologies Change Management Policy