POLICY: PASSWORD POLICY

Type of Policy: Network Password
Effective Date: March 11, 2019
Last Revised: December 5, 2018

Policy Owner: Information Services & Institutional Assessment
Policy Contact: Sharlene Harris
Interim VP of Information Services & Institutional Assessment
sharris@uvi.edu

1. Purpose

The purpose of this policy is to consolidate the University of the Virgin Islands' (UVI) password policies upon implementing the Identity Management (IdM) system and covers the password for all network services and applications including Banner, BanWeb, Blackboard, email, myCampus portal and PeopleAdmin.

2. Scope

The policy applies to UVI employees, students and authorized third parties.

3. Individual Responsibility

Individuals are responsible for keeping passwords secure and confidential.

4. Initial Password

A user's initial password will be unique using characters from a combination of the first name, last name and UVI ID number with the following schema: first initial of first name + first initial of last name + last seven digits of the UVI ID number, totaling nine (9) characters). This initial password will be shared with students through the Access and Enrollment Services office and staff through the Human Resources office.

First time authentication may be handled through the myCampus portal. This allows for remote authentication via a secure site where once a user enters requested information, the initial login is changed and authentication allowed.

5. Password Requirements

The following parameters indicate the minimum requirements for passwords for all individual accounts where passwords are:

- Password must be a minimum of 9 characters in length
- Password must contain at least 1 uppercase letter
- Password must contain at least 1 lowercase letter
- Password must contain at least 1 number non-alphanumeric character (such as ` ~ ! @ # $ % ^ & * ( ) _ + - = { } | \ : " ; ' < > ? , . /)
- Password must not contain spaces
- Password must not contain the values of Email Address, AccountId, Last Name, First Name, Student ID or Employee ID
- Phrases or sentences are recommended (The1sthouseonthestreet!)
- The last 2 used passwords cannot be repeated

6. Password Management

Upon initial login, each user will be prompted to set up password recovery options. The password recovery options include security questions and email/phone.

a. **Security Questions**
   Users can pick from a pool of questions and set up three (3) security questions and answers to recover their password.

b. **Email Recovery**
   Users can recover their password using a verified non-UVI email address.

c. **Phone Recovery**
   Users can recover their password using a verified phone number.

7. Password Expiration

For preventive reasons, passwords must be changed every 120 days. For self-service, it is recommended passwords are changed through the portal.

8. Account Lockout

In order to limit attempts at guessing passwords or compromising accounts, an account lockout policy is in effect for all systems. Accounts are locked after five (5) failed login attempts. Accounts are unlocked automatically after 30 minutes.

9. Password Reset Options

Various options are available to assist users with changing a forgotten or expired password. The preferred and fastest method is through the myCampus portal.

a. **Self Service**
   Self-service password management was implemented for the convenience of all network accounts. By setting up password recovery options, persons can manage their accounts without ITS staff intervention.

b. **In Person**
   Present a valid identification card (must contain photo), such as a driver license, passport, UVI issued ID.

10. Report a Suspected Compromise or Breach

If you believe your password has been compromised or if you have been asked to provide your password to another individual, promptly notify the ITS Help Desk at extension 1466.