University of the Virgin Islands

POLICY: PASSWORD

Type of Policy:	Information Technology
Effective Date:	March 11, 2019
Last Revised:	August 12, 2024
Policy Owner:	Information Services & Institutional Assessment
Policy Contact:	Sharlene Harris VP of Information Services & Institutional Assessment sharris@uvi.edu

1. Purpose

The purpose of this policy is to ensure the University of the Virgin Islands' (UVI) password policies are in line with the Identity Management (IdM) system. It covers the password for all network services and applications including Banner, BanWeb, Brightspace, MyCampus portal, Office365, and PeopleAdmin.

2. Scope

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

3. Individual Responsibility

Individuals are responsible for keeping their passwords secure and confidential.

4. Initial Password

A user's initial password will be composed using the following schema:

- Lowercase first two characters of the first name
- Dash
- Lowercase first two characters of the last name
- Last four digits of the user ID
- "@UVI"

For example, Jane Doe with user ID 900012345 will have the following initial login details:

- **Username:** 900012345
- **Initial Password:** ja-do2345@UVI

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:

- Password must be a minimum of 12 characters in length.

- Password must contain at least:
  - 1 uppercase letter
  - 1 lowercase letter
  - 1 number
  - 1 non-alphanumeric character
- Password must not contain:
  - Spaces
  - Values of Email Address, Last Name, First Name, Student ID, or Employee ID
- Phrases or sentences are recommended (e.g., 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, email, and phone.

- **Security Questions:** Users can pick from a pool of questions and set up three (3) security questions and answers to recover their password.
- **Email Recovery:** Users can recover their password using a verified non-UVI email address.
- **Phone Recovery:** Users can recover their password using a verified phone number.

7. Passwordless Authentication for MyCampus

Passwordless authentication eliminates the use of passwords after the initial setup of recovery options. Users will authenticate using a combination of factors such as:

- Security Questions
- One-time passwords (OTP) sent to a registered device, such as:
  - Email
  - Phone
  - Authenticator app

This method grants users secure access to their accounts without needing a traditional password.

8. Password Expiration

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

9. Account Lockout

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 and are unlocked automatically after 30 minutes.

10. 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.

- **Self Service:** Self-service password management was implemented for the convenience of all network accounts. By setting up password recovery options, users can manage their accounts without ISIA staff intervention.
- **In Person:** Present a valid identification card (must contain photo), such as a UVI issued ID, driver license, or passport.

11. Reporting 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 IT Helpdesk at (340) 693-1466.

12. Exception Handling

Having difficulty using multifactor authentication? Contact the IT Helpdesk at (340) 693-1466 for assistance and possible alternatives.

13. User Training and Support

Training and support resources are available to help you understand and implement the new authentication methods. Please look out for training opportunities announcements and contact IT Helpdesk at (340) 693-1466 for more information.

14. Compliance and Enforcement

Non-compliance with this policy may result in disciplinary actions in accordance with the University’s Acceptable Use Policy (AUP).

15. Review and Update of Policy

This policy will be reviewed and updated annually, and as necessary, to remain compliant with evolving security standards and technologies.