POLICY: PASSWORD

Type of Policy: Information Technology
Effective Date: August 4, 2024
Last Revised: July 2, 2025

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

1. Purpose

The purpose of this policy is to define password practices at the University of the Virgin Islands (UVI) following the implementation of the Identity Management (IdM) system. It outlines systems where passwords are still required, including:

- Initial login to the myCampus portal (for new users and password changes)
- Wi-Fi access
- VPN
- University-owned computers on the network
- PaperCut print management system

Many applications are now accessed through myCampus using Single Sign-On (SSO), allowing users to authenticate once and seamlessly access multiple systems.

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

Each new user is assigned an initial password using the following format:

- Lowercase first two characters of the **first name**
- Dash (**-**)
- Lowercase first two characters of the **last name**
- **Last four digits** of the user's ID number
- **@UVI1962**

For example, Maria Thomas with user ID 900012345

- Username: **900012345**
- Initial Password: **ma-th2345@UVI1962**

Initial passwords are distributed through the Access and Enrollment Services office (for students) or Human Resources (for employees).

- First-time login is completed through the myCampus portal, where users are prompted to change their password and configure recovery options.

5. Password Requirements

Passwords must meet the following minimum requirements:

- At least **16 characters** in length
- Must include:
  - At least one uppercase letter
  - At least one lowercase letter
  - At least one number
- Must not include:
  - Spaces
  - User's name, email address, or ID number

  Users are encouraged to use passphrases (e.g., The1sthouseonthestreet).

  The last two passwords used cannot be reused.

6. Password Management

Upon initial login, users must set up password recovery options, including:

- **Email Recovery**: A verified non-UVI email address
- **Phone Recovery**: A verified phone number
- **Authenticator App**: Users are encouraged to set up an authentication, preferably the Microsoft Authenticator app for secure and convenient recovery

7. Password Expiration

Passwords do **not** expire on a set schedule. Users should only change their password if they suspect it has been compromised. Password changes can be made through the self-service portal.

8. Account Lockout

To protect against unauthorized access, accounts will lock after **five (5)** failed login attempts. Locked accounts are automatically unlocked after **30 minutes**.

9. Password Reset Options

- **Self-Service**: Users can reset passwords via the myCampus portal, provided they have set up recovery options.
- **In Person**: Users may also reset their password by presenting valid photo identification (e.g., driver's license, passport, or UVI-issued ID) at a designated IT support location.

10. Reporting a Suspected Compromise or Breach

If you suspect your password has been compromised or if someone has requested your credentials, notify the IT Helpdesk immediately at (340) 693-1466**.**

11. Exception Handling

Users who are unable to use multi-factor authentication or recovery methods should contact the IT Helpdesk at (340) 693-1466 for alternative arrangements.

12. User Training and Support

Training sessions and resources are available to help users understand and use secure authentication tools. Watch for announcements or contact the IT Helpdesk for assistance.

13. Compliance and Enforcement

Failure to comply with this policy may result in disciplinary action in accordance with university policies and procedures.

14. Review and Update of Policy

This policy will be reviewed annually and updated as needed to reflect current security standards and technologies.