University of Portland

AUTHENTICATION AND ACCESS POLICY

1. **PURPOSE:** To establish standards and guidelines for the creation of passwords, the protection of those passwords, the use of Multi Factor Authentication (MFA), and the minimum standards for authentication across the University of Portland. This policy is designed to ensure that authentication methods are consistent to safeguard account-based access to information assets.

2. **SCOPE:** This policy applies to all personnel who have or are responsible for an account (or any form of data communications access) on any system the University utilizes. All faculty, staff and students are bound by Information Services policies regulating their University of Portland (UP) accounts.

3. **DEFINITIONS:** Employees may be issued multiple accounts for accessing applications as well as computer or network access. University of Portland (UP) accounts cover all accounts issued to employees. Data risk classifications define authentication requirements and are categorized as low-risk, moderate risk, and high risk. See the *Data Classification Policy* for further guidance.

   a. **Account Types:** Typically fall into the 4 categories below. The type and usage of an account generally determines its authentication requirements. To distinguish between requirements based on account type, this policy refers to several different kinds of accounts according to the following definitions:

      - **User Accounts**: are those under the control of a specific individual and are not accessible to others.
      - **Shared Accounts**: An account that can be accessed by multiple individuals to allow them to appear as a single business entity or accomplish a single shared function. Shared accounts are strongly discouraged and only granted for approved use cases.
      - **Privileged Accounts**: A qualifier used to describe User Accounts and Shared Accounts that have elevated access to configure or significantly change the behavior of a computing system, device, application or other aspect of the Information Services (IS) resources or IS infrastructure. These accounts should be considered highly sensitive.
      - **Service Accounts**: Accounts that are intended for automated processes such as running batch jobs or applications or establishing connections between web, application, and database servers, or external applications or services. To be considered a service account, the account must not be primarily used for general login to systems by users.

   b. **Passphrase**: A secret consisting of a sequence of words or other text that a claimant uses to authenticate their identity. A passphrase is like a password in usage but is generally longer for added security.

   c. **Password**: A secret that a claimant uses to authenticate his or her identity. Passwords are typically character strings.

   d. **Secret:** Commonly referred to as a passphrase, password, or if numeric, a PIN. A secret value of sufficient complexity and secrecy intended to be impractical for an attacker to guess or otherwise discover the correct secret value.

e. **Multi Factor Authentication (MFA)**: Multiple forms of authentication. Typically, something you know, such as a PIN or password; something you have, such as a one-time passcode generator or token; or something you are, such as a fingerprint or other biometric.

4. **POLICY**: Authentication methods for moderate and high-risk data shall meet the standards outlined in the guidelines of this policy. All applications that house high-risk data will utilize MFA. Never share your network password with anyone. No one from the University will ever ask you to reveal your password.

5. **GUIDANCE:**

a. **Minimum password and passphrase requirements**: Applications that use passwords or passphrases as an authenticator type, the following password and passphrase length requirements represent a minimum standard for University of Portland accounts:

Account Type	Minimum Length Requirement
All Accounts (baseline)	10
Service Accounts	16
Additional Requirements: • Password must contain 3 of the 4: lowercase letter, uppercase letter, number and special character. • Passwords should not contain any part of your name • Passwords should not contain any publicly available information such as: names of family members, address, home phone or BannerID • Enforce password history requirements of last 12. *Note:* If you are a Degreeworks user do not use these special characters (+, %, &, $).	

b. **Password expiration**: Passwords will expire every 2 years. Passwords must be changed immediately if a compromise of credentials has been independently discovered, publicly disclosed, suspected, or if a device has been lost or stolen. This includes discovery of plaintext and/or hashed secrets. Service Account passwords will expire every 5 years.

c. **Multifactor Authentication**: User accounts that are used to access high risk data must use MFA. This requirement does not apply when students are exclusively access their own information.

d. **Requirements for continued access:** Accounts must only remain active while there is a valid business justification for having the account. However, there may be times where accounts need to remain active past their normal defined periods:

- Individuals who leave employment in good standing and retain a documented affiliation with the university (emeriti, sponsorship, retiree/annuitant, adjunct faculty, instructional staff/faculty, etc.) may retain account access provided they follow policy guidance.
- An individual's affiliation must be formally documented and verified at least once every 365 calendar days.
- Individuals retain access to campus IS resources/services, limited to those commensurate with their role .
- Individuals remains subject to all University policies and procedures.
- Individuals are required to annually complete information security awareness training.

- Access will be disabled after 1 year of inactivity based on last login date.

- Access for individuals who leave employment in good standing and do not retain a documented affiliation with the University, will be disabled on the termination date set in the Human Resource System. Access for these individuals may be retained for a period of up to 90 days to facilitate grade appeal process, if applicable.

- Access for individuals who are discharged with no notice and/or terminated for cause must be revoked immediately. If a criminal offense is involved in the termination, the University of Portland Office of General Counsel or Human Resources must be consulted to ensure no legal hold on account information, files, etc. is required.

6. **EXCEPTIONS:** There are no exceptions to this policy.

7. **SANCTIONS:** Accounts and network access may be administratively suspended by the University with or without notice when, in the University's judgment, continued use of the University's resources may interfere with the work of others, place the University or others at risk, or violate University policy. Any violation of this policy by a student may lead to disciplinary charges under the appropriate student disciplinary policy, which may include expulsion or suspension of student status. Faculty and staff violations will be addressed by their respective disciplinary policies and procedures. All known and/or suspected violations will be reported to the Vice President for University Operations. Users of University of Portland computing facilities are subject not only to University Policies, but also to applicable local, state and federal laws.