University of Portland

APPLICATION AND NETWORK ACCOUNTS POLICY

1. **PURPOSE:** This policy defines standards for administration and construction of computing accounts that grant access or change University of Portland (UP) institutional data. Standardizing the naming of network accounts promotes professionalism and increases security (i.e. no more first name-only accounts, generic accounts, etc.) This policy outlines the standards for creating accounts, issuing accounts and managing accounts.

2. **SCOPE:** Information Services (IS) established standards for the naming of student, faculty, staff, and members of the University community who use, access, or otherwise encounter University data. This policy is applicable to those responsible for the management of user accounts or access to shared information or network devices. This policy covers departmental accounts as well as those managed centrally.

3. **POLICY:**

   a. **Account Creation:**

   - **Naming of email accounts – Students**: The email account name for students will be the first eight characters of their last name with the two-digit expected year of graduation for a total of 10 characters (e.g., Kent Thompson 2026 = thomson26, Bruce Robertson 2020 = robertso20). Replicas will be resolved using the first seven characters of their last name and the first letter of their first name (e.g., Kent Thompson 2026 = thompsok26, Bruce Robertson 2020 – robertsb20). The process will repeat until we have a unique name (e.g., Kent Thompson 2026 = thompske26, Bruce Robertson 2020 – robertbr20). If a unique name cannot be found, the Director of Technical Services will decide what name to use based on input from the Technical Support Manager. Students will not be allowed to change their email account name from the expected year of graduation to reflect an actual graduation year. An alumni email alias will be added for each student upon their graduation as follows: username@almuni.up.edu

   - **Naming of email accounts – faculty and staff**: The email account name for faculty and staff will be the first eight characters of their last name without any punctuation (e.g., Kent Thompson = thomson, Bruce Robertson = robertso). Replicas will be resolved by using the first seven characters of their last name and the first letter of their first name (e.g., Kent Thompson = thomsok, Bruce Robertson = robertsb). The process will repeat until we have a unique name (e.g., Kent Thompson = thomske, Bruce Robertson = robertbu). If a unique name cannot be found, the Director of Technical Services will decide what name to use based on input from the Technical Support Manager.

   b. **Issuing Accounts:**

   - The owners of data shall make decisions regarding access to their respective data (e.g., the Registrar will determine who has access to registration data, and what kind of access each user has). Account setup and modification shall require the signature (paper or electronic) of the requestor's supervisor.

   - The organization responsible for a resource shall issue a unique account to each individual authorized to access that networked computing and information resource. It is also responsible for the prompt deactivation of accounts when necessary, i.e., accounts for terminated individuals shall be removed/disabled/revoked from any computing system at the end of the individual's employment or when continued access is no longer required; and, the accounts of transferred individuals may require removal/disabling to ensure changes in access privileges are appropriate to the change in job function or location.

- When establishing accounts, standard security principles of "least required access" to perform a function must always be used, where administratively feasible. For example, a root or administrative privileged account must not be used when a non-privileged account will do.

- The identity of users must be authenticated before providing them with account and password details. If an automated process is used, then the account holder should be asked to provide several information items that in totality could only be known by the account holder. In addition, it is highly recommended that stricter levels of authentication (such as face-to-face) be used for those accounts with privileged access.

- Passwords for new accounts should NOT be emailed to remote users UNLESS the email is encrypted.

- The date when the account was issued should be recorded in an audit log or captured electronically.

c. <u>Managing Accounts:</u>

- All accounts shall be reviewed at least annually by the data owner to ensure that access and account privileges are commensurate with job function, need-to-know, and employment status. Information Services may also conduct periodic reviews for any system connected to the UP network.

- All guest accounts (for those who are not official members of the UP community) with access to UP computing resources shall contain an expiration date of one year or the work completion date, whichever occurs first. All guest accounts must be sponsored by the appropriate authorized member of the administrative entity managing the resource.

4. **EXCEPTIONS:** Usernames will not be changed unless the individual's name changes in the official University databases and the individual personally requests such a change, or in cases where there might be personal danger to the individual if they have a commonly derived username. Changes will also be allowed where the combinations of characters result in an objectionable name or term. Vanity username changes will not be permitted.

5. **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.