



PASSWORD POLICY

Approved by the Officers of the University on February 9, 2005

1. Scope: Passwords are a critical aspect of computer security. They are the front line of protection for user accounts. The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any University facility, has access to the University network, or stores any public or non-public University information.

2. Policy: The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords, and the frequency of change. A poorly chosen or poorly managed password may result in the compromise of the entire University network and/or critical information systems. As such, all University employees, including contractors and vendors with access to University systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2.1. The standard for the creation of a strong password is as follows:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Has digits and punctuation characters as well as letters (e.g., 0-9, !@#\$%^&*()_+ | ~ - = \ { } [] ; ' < > ? , . /)
- Be at least eight alphanumeric characters long
- Not be a common usage word such as:
 - A word found in a dictionary (English or foreign)
 - Slang, dialect, jargon, etc.
 - Names of family, pets, friends, co-workers, fantasy characters, etc.
 - Computer terms and names, commands, sites, companies, hardware, software, etc.
 - "UP", "UofP", "Portland", or any derivation
 - Not be based on personal information such as birthdays, addresses, pet names, phone numbers, etc.
 - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
 - Any of the above spelled backwards
 - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

2.2. The standard for the protection of a password is as follows:

- Do not write passwords down or store them on-line without encryption. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W > r ~" or some other variation. *NOTE: Do not use either of these examples as passwords!*
- Do not use the same password for University accounts as for other non-University access (i.e., personal ISP account, option trading, benefits, etc.). Where possible, do not use the same password for various University access needs.
- Do not share University passwords with anyone, including administrative assistants, secretaries,

bosses, family members, co-workers while on vacation, etc.

- Do not reveal a password over the phone or in an email to anyone.
- Do not talk about a password in front of others or hint at the format of a password.
- Do not reveal a password on questionnaires or security forms.
- If someone demands a password, refer them to the Vice President for Information Services.
- Avoid storing passwords within applications or using the “Remember Password” feature. These features do not adequately protect passwords. A computer virus or unauthorized user may gain access to this stored information

2.3. The standard for the frequency of change of a password is as follows:

- All user passwords (i.e., network, email, portal, etc.) will be changed at least once every six months.
- All system-level passwords will be changed on a quarterly basis or more frequently as needed (i.e., suspected or confirmed information security breach, abnormal network activity, employee termination, etc.).

2.4. If an account or password is suspected to have been compromised, report the incident to the Vice President for Information Services and immediately change the password.

2.5. The Vice President for Information Services or his delegate may perform password cracking or guessing on a periodic or random basis. If a password is cracked or guessed during one of these scans, the user will be required to change it.

2.6. If the software and/or information system allows, the Vice President for Information Services will enforce password history (how many different passwords must be used before the user can reuse one of them); maximum password age (how long a password is good before a user is forced to pick a new one); minimum password age (how long a new password must be used before it can be changed); minimum password length (how many characters must make up the password); and password complexity requirements as detailed in this policy.

3. Exceptions. For systems and applications that have a maximum password length of less than eight characters, that maximum length will be set as the minimum accepted password length. All other exceptions must be approved by the Vice President for Information Services.

4. 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 must be reported to the Vice President for Information Services, who will investigate all such allegations of misuse with the assistance of Public Safety, Human Resources, Residence Life, and/or the appropriate office of the University. Penalties for faculty/staff violators may include: Suspension or termination of access to computer and/or network resources; disabling all computer and/or network services; suspension or termination of employment; and/or criminal and/or civil prosecution. Users of University computing facilities are subject not only to University policies, but also to applicable local, state, and federal laws.