Integrated Information Technology Services

POLICIES AND PROCEDURES

Computer Passwords

POLICY:

Passwords are required for accessing all Utica College computers, networks, systems, and infrastructure.

Passwords are administered by the IITS Infrastructure Department. A password is required for all users using network resources in computer labs, offices, and other campus locations.

Passwords' length and complexity vary by system, and are required to contain a combination of uppercase letters, lowercase letters, numbers, and special characters. Generally, passwords must be changed every 120 days, and users may not reuse a previously used password.

Unless the user is unable, the user is responsible for changing the password**.** The Computer Help Desk will not change any password or provide temporary passwords over the phone without sufficient user authentication based on the account the user is trying to access.

Passwords must not be stored electronically in plain-text, unprotected documents. Writing down a password is also discouraged. If it is necessary, passwords may be stored in locked drawers or in personal possessions (e.g., purses, wallets, etc.). They must not be stored in the same location as the username.

All passwords are considered sensitive, confidential UC information and therefore must be protected as such and stored accordingly.

SCOPE:

This policy applies to all UC faculty, staff, students, alumni, temporary employees, third parties, volunteers, and entities that have been granted an approved set of access credentials.

REASON FOR POLICY:

It is imperative that the College have established security policies in order to ensure stable computer and network resources.

DEFINITIONS:

User Account: These accounts must have strong passwords consisting of least eight characters, and they must change every 120 days. Examples of user accounts include Banner, computer login, network access, and email access.

Admin Account: These accounts are required to perform certain tasks that the general Utica College user population would not need to perform. These tasks require elevated access rights, and thus must be protected more so than a standard user. While the standard user has the rights to check his or her own email, the email admin user has the ability to add/remove users, apply security patches, and recover from attacks/or natural disasters. User account passwords must be strong, consisting of at least eight characters, and must change every 90 days. Examples include Root and Administrator accounts.

Service Account: Service accounts are used by computer programs within a system, not by end users. These accounts require complex passwords that must be greater than 32 characters in length and consist of uppercase letters, lowercase letters, numbers, and special characters. Complexity varies based on what character set each system can accept.

PROCEDURE:

- All service account passwords will be stored on an encrypted thumb-drive stored in a secure location.
- Admin account passwords will be stored on paper in a sealed envelope at a secure location; only authorized IITS personnel will know this location.
    - The authorized supervisor is responsible for the safe storage, retrieval, and dissemination of top-level passwords.
    - In the event of an emergency when the supervisor of the system in question is not available, the Chief Information Officer and Vice President for Technology (CIO) may provide access to this location.
    - If the CIO is not available, the available directors shall make this decision.
- A simple alerting system or procedure will remind users when to change passwords.
- Users can change passwords by going to http://password.utica.edu.
- If a user fails to change the password within 15 days of notification, access will be denied until the password has been changed.
- If the user is unable to change his or her own password, the Computer Help Desk may be able to issue a temporary one. For more information, contact the Computer Help Desk.

RESPONSIBILITY:

The CIO is responsible for the annual review of this document. IITS will ensure that the proper protections are in place based on the system in question. The CIO and those designated are responsible for following the policy defined in this document. Exceptions to this policy must be approved by the President of the College.

ENFORCEMENT:

Enforcement of Utica College policies is the responsibility of the office or offices listed in the "Resources/Questions" section of each policy. The responsible office will contact the appropriate authority regarding faculty or staff members, students, vendors, or visitors who violate policies.

Utica College acknowledges that College policies may not anticipate every possible issue that may arise. The College therefore reserves the right to make reasonable and relevant decisions regarding the enforcement of this policy. All such decisions must be approved by an officer of the College (i.e. President, Provost and Vice President for Academic Affairs, Executive Vice President and Chief Advancement Officer, Vice President for Financial Affairs, or Vice President for Legal Affairs and General Counsel).

RESOURCES/QUESTIONS:

For more information, contact the Utica College Computer Help Desk, which can be reached via telephone at (315) 792-3115. See also the Responsible Use of College Computing Resources policy.

Please note that other Utica College policies may apply or be related to this policy. To search for related policies, use the Keyword Search function of the online policy manual.

_____ _____

Todd S. Hutton, President Date

Effective Date: February 13, 2013
Promulgated: September 22, 2013

Last Revised:
Promulgated: