UTICA
UNIVERSITY

Integrated Information Technology Services

POLICIES AND PROCEDURES

Multi-Factor Authentication Policy

POLICY:

Two-factor authentication is required for Utica University users to access protected network resources. The Office of Integrated Information Technology Services (IITS) will maintain and manage a list of services protected by a multifactor authentication process. This second authentication adds an extra layer of security if an account password is compromised and is used to restrict unauthorized access to the university network and resources. The Utica University IITS Helpdesk may issue a temporary bypass in case of a system failure.

SCOPE:

This policy applies to all Utica University faculty, staff, students, alumni, temporary employees, third parties, volunteers, and entities that have been granted access credentials and access those systems identified by IITS and protected by multifactor authentication

REASON FOR POLICY:

Single-factor authentication leaves accounts vulnerable if a password has been compromised. Adding an additional multifactor authentication method secures access to applications even if a password is compromised. Multifactor is required on all university applications that hold sensitive data as defined in the Data Security and Classification Policy.

DEFINITIONS:

Two-factor authentication adds a second layer of security to Utica University Accounts. Some services and websites refer to this second layer of security as two-factor authentication, 2FA, two-step authentication, two-step verification, or login verification. This second form of authentication helps to prevent unauthorized users from accessing an account, even if the password is compromised.

A **multifactor app** is available for phones and cellular-capable devices, both Apple and Android. It is free from the Apple App Store and Google Play Store. It allows the user to say “Yes” or “No” to any attempted login to their account for multifactor-protected services and thereby provides a second authorization factor for these services.

A **phone** is a device capable of receiving phone calls or text messages and can be a mobile phone or an office phone. It allows the multifactor system to contact a user by voice or text message to ask them to agree to any attempted login and thereby provides a second factor of authorization to services protected by two-factor authentication.

A **hardware token** is a small device that can generate a passcode which can be used as a second factor of authorization to services protected by two-factor authentication.

PROCEDURE:

- IITS will be responsible for provisioning required users into a multifactor authentication method for all required applications.
- Users will be responsible for downloading or setting up their multifactor authentication using instructions provided by the Office of Integrated Information Technology Services.
- Additional resources for Faculty or Staff who cannot use a mobile or office phone to complete their multifactor authentication are available by request from the IITS Helpdesk.
- Loss of a phone or other multifactor device must be reported to the Information Security Officer or the IITS Helpdesk as soon as possible.

RESPONSIBILITY:

The Information Security Officer is responsible for the annual review of this document. IITS will ensure the proper protections are in place based on the system. 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 University.

ENFORCEMENT:

Enforcement of Utica University 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 University acknowledges that University policies may not anticipate every possible issue that may arise. The University 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 University (i.e. President, Provost and Senior Vice President for Academic Affairs, Vice President for Financial Affairs, Senior Vice President for Student Life and Enrollment Management, or Vice President for Legal Affairs and General Counsel).

RESOURCES/QUESTIONS:

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

Please note that other Utica University 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 Pfannestiel, President Date

Effective Date:
Promulgated:

Last Revised:
Promulgated: