Northeastern ILLINOIS UNIVERSITY

University Policy

Volume I1: Information Technology	**Multi-factor Authentication** **Interim Policy** **Effective Date:** 01/10/2022 **Date of Next Full Review**: 01/09/2023	**Responsible Office:** University Technology Services
Chapter 01: Acceptable Use		**Responsible Officer:** Chief Information Officer

POLICY STATEMENT

User accounts provide the basic first line of defense against unauthorized access and use of an organization's information resources. However, additional measures are necessary to protect against the increasing cyberattacks that target user accounts to compromise the security of data and IT resources. Multi-Factor Authentication (MFA) provides an additional layer of security to protect user accounts against compromise.

Multi-Factor Authentication is a tool that provides more control and assurance to user account owners by ensuring that all access authentication requests are verified by account owners before access to information resources is given. This is achieved by requiring extra verification from a user in addition to their user ID and password. The additional verification provided helps to protect the user's account should their password be compromised.

Northeastern Illinois University has implemented multi-factor authentication to further strengthen the access control to your information and the data and IT Resources (ITR) you use for work.

PURPOSE OF THE POLICY

The purpose of the policy is to set out the requirement and expectations for use of multi-factor authentication by faculty, staff, and third-party agents to protect their user accounts from being compromised and to safeguard the University's data and ITR.

WHO IS AFFECTED BY THIS POLICY

Faculty and staff (including third-party agents that access and use the University's data and ITR).

DEFINITIONS

Multi-factor Authentication (or two-factor authentication) is a tool that provides an additional layer of security when logging into an IT system. It works by requiring additional verification along with a user ID and password before access to data and/or IT resources is given. The additional verification provided helps to protect the user's account should their password be compromised.

REGULATIONS

- To protect the University's user accounts and to ensure that only authorized users have access to the University's data and ITR, faculty, staff, and third-party agents are required to use multifactor authentication.
- Users are required to follow the appropriate use of the University's multifactor authentication tool. See My Responsibilities for Use of MFA.
- Users are required to report any incidents relating to the use of the University's multifactor authentication tool as soon as possible to reduce the likelihood of any account compromise. University Technology Services should be contacted to report incidents and issues via helpdesk@neiu.edu or 773) 442-4357.

- Use of hardware (physical) token. If you are issued a hardware token as your multifactor authentication device, you may be required to purchase another hardware token device if the initial one is damaged or lost.

PROCEDURES

To enroll your smartphone to use the University's multi-factor authentication tool, follow the DUO Device Enrollment Instructions on the MFA web page. To request a DUO hardware token, please contact the Helpdesk at helpdesk@neiu.edu or call 773 442-4357.

RELATED POLICIES AND OTHER INFORMATIONAL MATERIAL

Acceptable Use of IT Resources

CONTACT INFORMATION

Please direct questions or concerns about this policy to:

Contact	Phone	Email
Chief Information Officer	(773) 442-4357	helpdesk@neiu.edu

DISCLAIMER

The University reserves the right to modify or amend sections of this policy at any time at its sole discretion. This policy remains in effect until such time as the Responsible Officer calls for a review. Requests for exception to any portion of this policy, but not to the policy statement, must be presented in writing to the Responsible Officer.