Multifactor Authentication Policy

1.0 Purpose

The purpose of this policy is to provide guidelines for Multifactor Authentication (MFA) connections to the Northwestern State University (NSU) network and information systems. This policy is designed to minimize the potential security exposure to Northwestern State University from damages which may result from unauthorized use of University resources and to add a layer of security to individual users from compromised credentials.

2.0 Policy

It is the policy of NSU that any off-campus access to the University's network or computer systems require the use of the University's Multifactor Authentication provider along with the traditional username and password. MFA is required on all new accounts created. Previously set up accounts will be temporally grandfathered in as MFA is implemented. MFA is required on any externally exposed application, whether in house or third party.

3.0 Responsibilities

It is the User's responsibility to promptly report compromised credentials or lost MFA devices to Information Technology Services.

4.0 Miscellaneous

NSU recommends use of the Microsoft Authenticator app for mobile devices. Receiving an SMS text message or a phone call from Microsoft to complete the authentication process is also supported.

5.0 Exceptions to Policy

There may be situations in which a member of the university community has a legitimate need to utilize university technology resources outside the scope of this policy. Information Technology Services may approve, in advance, exception requests based on balancing the benefit versus the risk to the University.