Multi-Factor Authentication Requirement Policy

Policy/Procedure

PURPOSE

The purpose of this policy is to define the requirements for access to Dickinson College's Microsoft Office 365 services from off campus. This policy is designed to minimize the potential security exposure to Dickinson College from damages which may result from unauthorized use of college services. Multi-factor authentication (MFA) adds a layer of security which helps deter the use of compromised credentials.

SCOPE

This policy applies to all members of the Dickinson College community who may require remote (off campus) access to email and the other services within the college's MS Office 365 environment. There may be extraordinary instances when a member has a legitimate need to use the college's services outside the scope of this policy. The VP and CIO of IS and the Director of Infrastructure and Information Security must approve, in advance, exception requests based on the balancing of the benefit versus the risk to the college. Exceptions for individuals with disabilities will be addressed on an individual bases in consultation with HR Services and the office of Access and Disability Services (ADS).

USER REQUIREMENTS

All members are required to register their user credentials for remote access to the college's MS Office 365 environment. If a community member does not register their user credentials, they will not be permitted remote access to the college's MS Office 365 service. Information for selecting a verification method can be found by using the following link:
https://www.dickinson.edu/mfa

There are 3 primary verification methods available to all members:

1. Microsoft Authentication App or the Google Authentication App. These Apps can easily be downloaded to a device and allow for a "challenge response" or a six-digit code input within the App.
2. A phone call to any 10-digit phone number.
3. A text message to your cell or smart phone.

A digital token is available for members on a case by case basis. The use of a digital token will only be granted for exceptional cases. The token will be provided and managed by the college. If a member can't use any of the 3 primary verification methods, please contact the Helpdesk at helpdesk@dickinson.edu or x1000 to request the use of a college provided digital token. All requests will be reviewed by the Director, Infrastructure Systems and Information Security before any digital tokens are issued.

LOST OR STOLEN DEVICE
All lost or stolen devices should be reported immediately to the LIS Helpdesk at helpdesk@dickinson.edu or x1000, so that device may be denied access to the college's MS Office 365 services.

Individuals that are granted access to a digital token are responsible for securing the token to safeguard its loss or theft. A replacement charge of $50.00 may be applied for any lost or stolen digital token.

Related Information

History/Revision Information

Responsible Division/Office: IS/User Services

Effective Date: 3/19/2019

Last Amended Date: 6/5/2022

Next Review Date: 6/5/2024

Also Found In: