NEOMED OPERATIONAL POLICY	Policy No: 3349-OP-327
OPERATIONAL POLICY TITLE: Multi-Factor Authentication	EFFECTIVE DATE: June 1, 2021
RESPONSIBLE DEPARTMENT: Information Technology	Approval Authority: VP for Operations and Finance Responsible Office: Operations and Finance

(A) PURPOSE

The purpose of this policy is to define access requirements to NEOMED systems using Multi-Factor Authentication ("MFA"). This policy is designed to minimize the potential security exposure to the University from damages that may result from the unauthorized use of University resources.

(B) SCOPE

This policy applies to all individuals who have a NEOMED email account as well as any University System that is protected with Multi-Factor Authentication. University Systems requiring the use of MFA may include, but are not limited, to the NEOMED Virtual Private Network (VPN), Systems utilizing single sign-on (SSO), System administration tools, and privileged accounts.

(C) DEFINITIONS

(1) "Multi-Factor Authentication" refers to a method of access control in which an individual is granted access only after successfully presenting at least two, distinct pieces of evidence when logging into an account. The pieces of evidence fall into any of these categories: something you know (like a password or PIN), something you have (like a smart card), or something you are (like your fingerprint).

(2) "System" refers to an information technology resource that can be classified, may have security controls applied, and are organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of University Data.

(3) "Technology" refers to the broad term used to describe the aggregation of University Data, Systems (cloud-based, externally hosted, on-site), technology services, the University network, or any other device that may affect the security of the University's technology environment.

(4) "University Data" refers to Data that is created, collected, stored, and/or managed in association with fulfilling the University's mission or its required business functions. University Data may or may not constitute a Public Record (as defined within Ohio Revised Code §149.43).

(5) "Virtual Private Network" ("VPN") refers to a method employing encryption to provide secure access to a remote computer over the Internet.

NEOMED OPERATIONAL POLICY	Policy No: 3349-OP-327
OPERATIONAL POLICY TITLE: Multi-Factor Authentication	EFFECTIVE DATE: June 1, 2021
RESPONSIBLE DEPARTMENT: Information Technology	Approval Authority: VP for Operations and Finance Responsible Office: Operations and Finance

(D) POLICY STATEMENT

(1) Individual Requirements and Registration

(a) To access University Systems protected with MFA, individuals who have a NEOMED email account are required to complete the MFA enrollment process, wherein the individual registers authentication methods and devices. If an individual does not register for MFA, that individual will not be permitted access to University Systems protected with MFA.

(i) The MFA enrollment first time setup guide and additional instructions for changing authentication methods can be found at https://www.neomed.edu/mfa.

(ii) A hardware token is available for individuals on a case-by-case basis and is only granted for exceptional cases. The hardware token will be provided and managed by the University. If an individual cannot use any of the authentication methods, please contact the NEOMED Help Desk at help@neomed.edu or extension 6911.

1. All requests will be reviewed by Information Technology ("IT") personnel before a hardware token is issued.

2. Individuals that are granted access to a hardware token are responsible for safeguarding the University token from loss or theft. A charge of $50.00 will be applied if a hardware token needs replaced.

(2) Frequency of User Challenges

(a) The frequency of user challenges depends on the application being protected by multi-factor authentication. User challenge intervals for systems and services protected by multi-factor authentication vary.

(3) Off-Hours and Emergency Access to Protected Data

(a) NEOMED IT shall maintain internal procedures for processing emergency access requests if issues arise with the MFA process. Individuals should contact the NEOMED Help Desk for such requests.

(4) Lost or Stolen Devices

(a) If an individual's registered device is lost or stolen, or the individual has reason to suspect their NEOMED account credentials have been

compromised, the individual should contact the NEOMED Help Desk at help@neomed.edu or extension 6911 as soon as possible.

(5) Unauthorized Access

(a) Individuals may not attempt to circumvent login procedures, including MFA, on any University system or otherwise attempt to gain unauthorized access to University information resources. Attempts to circumvent login procedures may subject the individual to disciplinary action including, but not limited to, suspension of the individual's access to the information resources. Financial losses incurred due to the use of MFA circumvention techniques are the responsibility of the individual, and the University may seek financial restitution from individuals who violate this policy.

(b) Individuals may also be subject to other possible consequences under existing University policies and federal, state, or local laws, particularly those related to computer crime and copyright violation.