Ohio Administrative Code

Rule 3349-9-15 Information security.

Effective: May 27, 2019

(A) Purpose

Northeast Ohio medical university ("NEOMED") has instituted the following information security rule to establish the overarching, university-wide approach to information security and as a measure to protect the confidentiality, integrity and availability of university data and systems.

(B) Scope

This rule applies to university data and systems; university students, faculty, staff, and alumni; and authorized external users for legitimate university purposes (e.g., volunteers, tenants, vendors, contractors, consultants, guests and/or visitors).

(C) Definitions

(1) "Access control" refers to the process of regulating specific requests to obtain and use university data and systems.

(2) "Authorization" refers to the granting of permission to an identified individual to use university data or system(s) and to explicitly accept the risk to university operations, individuals, and assets based on extending such permission. Acceptance of authorization to use university data and systems establishes an obligation on the part of the individual to use those resources responsibly.

(3) "Availability" refers to the ensuring of timely and reliable access to and use of data or systems. Additionally, it describes the importance of access when the data or system is needed, and the impact on the organization if it is not available. A loss of availability is the disruption of access to or use of data or systems (e.g., hard drive failure, destruction of a system, system unresponsiveness, denial of service attack).

(4) "Confidentiality" refers to the preservation of authorized restrictions on data access and disclosure, including means for protecting personal privacy and proprietary data. A loss of confidentiality is the unauthorized disclosure of data (e.g., compromised by hackers; released or published publicly without authorization).

(5) "Data" refers to any instance of information, regardless of form or storage medium, that is categorized by an organization or by a specific law or regulation.

(6) "Information security" refers to the protection of university data and systems from unauthorized access, use, disclosure, disruption, modification and destruction with the intent to provide confidentiality, integrity and availability to such data and systems.

(7) "Integrity" refers to the guarding against improper data or system modification or destruction and ensuring authenticity and non-repudiation in the use of data or systems. A loss of integrity is the unauthorized modification or destruction of data or systems where such resources can no longer be trusted for use, are not complete, or incorrect.

(8) "Risk," with respect to the university, refers to the effect of uncertainty, either negative or positive, on the university's strategy and its strategic objectives.

(9) "Security incident" refers to an adverse event that results in a suspected or known unauthorized disclosure, misuse, alteration, destruction, or other compromise of university data or systems. A security incident is caused by the failure of a security mechanism or an attempted or threatened breach of these mechanisms through nonelectronic means (e.g., a violation of applicable university rules, mishandled documents, the theft or loss of a system, verbal or visual disclosure of personal information) and electronic means (e.g. hacking, malware, ransomware, phishing).

(10) "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. Example of systems are, but not limited to: desktop, laptop, or server computers; mobile devices (e.g., iphones; ipads; android; blackberry) to the extent that they interact with university data and systems, such as university email; university network(s); software; applications; and databases.

(11) "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 section 149.43 of the Revised Code).

(12) "University account" refers to a user's username and password combination for a university system (e.g., university email).

(13) "University email", also known as "NEOMED email", refers to the university's approved microsoft-based email system used to transmit and receive electronic messages.

(14) "User" refers to any individual or entity that has received authorization, if applicable, to access university data or systems.

(D) Rule statement

(1) Overview

(a) The ability for the university to meet the regular needs of its academic, administrative, and research communities is facilitated, in large part, by using university data and systems. While these technologies are important assets of the university and are fundamental to the carrying out of its mission, they also introduce risk, which are increasing in both number and variety (e.g., phishing, identity fraud, misuses of university data and systems). As a result, the university has established an overarching information security rule to serve as the basis for the safeguarding of its data and systems.

(b) NEOMED will ensure that users are aware of their specific information security responsibilities in the use and management of university data and systems. By being aware, NEOMED expects users to use appropriate physical, electronic, and procedural safeguards to protect the confidentiality, integrity and availability of university data and systems, as outlined herein and throughout the university's information technology rules and procedures. While the safeguards utilized by the university are expansive and thorough, the university cannot guarantee absolute security; therefore, all users share responsibility to minimize risk and to secure university data and systems within their control. Any suspected misuse or other information security incidents must be reported, in accordance with the

information security incident response plan rule.

(c) This overarching rule is supplemented and supported by other information technology rules and procedures that are created to support information security elements not outlined herein. All information security rules and procedures shall ensure compliance with all applicable federal and state security-related laws and regulations. These rules and procedures shall consider risk within their design and be written to recognize the risk severity and resource constraints of university.

(2) Information security elements

The following is an overview of the overarching components that provide the basis for the university's information security measures and corresponding safeguarding requirements. These components are adapted from the national institute of standards and technology (NIST) risk management framework and corresponding NIST security controls which are further developed within other university information technology rules and procedures.

(a) Confidentiality, integrity and availability: the university shall ensure that its information security rules and procedures address the basic security elements of confidentiality, integrity, and availability.

(b) Management and governance: the university shall implement an institutional governance structure for the management of its information security framework.

(c) Classification of university data and systems: the university shall implement classification requirements that protect university data and systems in the most appropriate manner.

(d) Risk management: the university shall apply risk management procedures to make informed decisions on appropriate information security safeguards and to aid in designing and implementing any additional information technology rules and procedures.

(e) Access control and authorization: the university shall implement information security rules and procedures regarding access control and authorization required to protect university data and systems.

(f) Audit logging: the university shall implement an information security audit logging capability for

university systems, including computers and network devices.

(g) Identify, protect, detect, respond, and recover: information security rules and procedures shall include methods to identify, protect against, detect, respond to, and recover from threats and vulnerabilities to university data and systems.

(h) Rule and procedure management: rules and procedures created to supplement and support this overarching information security rule shall be reviewed by university information security personnel before being installed. These rules and procedures will be implemented with consideration of the business impacts and resource constraints for all university areas tasked with their implementation.

(3) Enforcement

(a) The university respects the privacy of individuals and keeps university data on university systems as private as possible. The university also does not generally monitor university email, systems, and university data stored on university systems or traversing the university's network; however, the university reserves the right to monitor, access, and disclose university data created, sent, received, processed, or stored on university systems to protect the confidentiality, integrity, and availability of university data and systems or for any reason to ensure compliance with university rules and federal, state, or local laws and regulations. University personnel will have the right to review and/or confiscate any university equipment connected to or using university data and systems. University personnel also reserve the right, without notice, to limit or restrict any individual's university data and systems access and to inspect, remove, or otherwise alter any university data or system that may compromise the information security of the university. University data and systems are the property of NEOMED and not the personal property of the individual.

(b) Access to university data and systems is a privilege that is granted by the university; therefore, non-compliance or violation of related university rules may result in disciplinary action, which could include, but is not limited to: suspension or loss of the user privileges related to university data and systems; mandatory information security training; written warnings, suspension with or without pay, or termination; or any other remedy available by law.

(c) The university will not defend or indemnify any user who utilizes university data and systems for

an unlawful purpose or in contravention of university rules.