Ohio Administrative Code

Rule 3349-9-18 Classification of university data systems.

Effective: May 27, 2019

(A) Purpose

To establish a classification framework based upon the sensitivity and regulatory requirements for safeguarding university data and systems.

(B) Scope

This rule applies to all university data and systems and to those responsible for classifying or using university data and systems.

(C) Definitions

(1) "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.

(2) "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).

(3) "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).

(4) "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.

(5) "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.

(6) "Internal university data" as defined within paragraph (D)(2)(a)(ii) of this rule.

(7) "Private university data" as defined within paragraph (D)(2)(a)(iii) of this rule.

(8) "Public university data" as defined within paragraph (D)(2)(a)(i) of this rule.

(9) "Record" refers to any document, device, or item, regardless of physical form or characteristic that is created, received by, or comes under the jurisdiction of an organization which serves to document the organization, its functions, rules, decisions, procedures, operations or other activities. University data may reside in university records, be used to produce university records, or may of itself be a university record.

(10) "Restricted university data" as defined within paragraph (D)(2)(a)(iv) of this rule.

(11) "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.

(12) "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.

(13) "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).

(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) Northeast Ohio medical university is committed to protecting the privacy of its students, faculty, and staff, as well as protecting the confidentiality, integrity, and availability of university data and systems that are important to the achievement of the university's mission and ongoing operations.

(b) The university uses risk assessment methodologies to translate university data and system considerations into an appropriate risk classification. This is done by assessing the adverse effects that could be expected by a loss of confidentiality, integrity, and availability of university data or systems and then determining a severity level for each resource. If a need for confidentiality, integrity, or availability is higher or stronger than the other two measures, the overall classification of that university data or system will reflect that highest or stronger need.

Example: if a specific university data was assessed with a high need for confidentiality, but low needs for integrity and availability, the university data will be classified based upon the high need for confidentiality (classifications further detailed below).

(c) Based upon the classification, authorization to access university data or systems will vary and security controls for access and protection will be applied, in accordance with the university's information technology rules.

(d) Proper classification is a prerequisite to enable compliance with legal and regulatory requirements, and university rules and procedures.

(e) Regardless of classification, university data may reside within university records, be used to

produce university records, or itself constitute a university record. University records are generally available to the public under the state of Ohio's public records law. Some records are protected by federal or state law or are otherwise exempt from disclosure.

(f) Any questions regarding the classification of university data and systems should be referred to the appropriate data steward, system steward, or to the office of compliance and risk management.

(2) Classification of university data

(a) The four university data classifications are, from least to most restrictive:

(i) Public

(a) Public university data is university data that is intended and accessible for public use and is not restricted by federal, state, local, or international regulations regarding disclosure or use.

(b) The potential loss of confidentiality, integrity, and availability of public university data could be expected to have no adverse effects on university operations, university assets, or individuals.

(ii) Internal

(a) Internal university data is university data used to conduct university business for which access must be guarded due to proprietary, ethical, or privacy considerations. This classification applies even though there may not be a civil statute requiring this protection. This university data is not intended for public dissemination, but its disclosure is not restricted by federal or state law or regulation.

(b) The potential loss of confidentiality, integrity, and availability of internal university data could be expected to have limited adverse effects on university operations, university assets, or individuals.

(i) The need for confidentiality is low/optional;

(ii) The need for integrity is low/optional as the university data is easily reproducible; and/or

(iii) The need for availability is low/optional as the university data provides an informational/non-critical service.

(iv) Access to and management of internal university data may only be available to users whose role, function, or assignment requires it.

(iii) Private

(a) Private university data is university data used to conduct university business for which access must be guarded due to legal, regulatory, administrative, and contractual requirements, in addition to proprietary, ethical, or privacy considerations.

(b) The potential loss of confidentiality, integrity, and availability of private university data could be expected to have serious adverse effects on university operations, university assets, or individuals.

(i) The need for confidentiality is moderate/recommended;

(ii) The need for integrity is moderate/recommended as the university data is internally trusted by or dependent on other university data or systems; and/or

(iii) The need for availability is moderate/recommended as the university data provides a normal or important service.

(c) Access to and management of private university data requires authorization and is only granted to those users as permitted under applicable law, regulation, contract, rule, and/or role.

(iv) Restricted

(a) Restricted university data is university data that requires the highest level of protection due to legal, regulatory, administrative, contractual, rule, industry standards, or rule requirements.

(b) The potential loss of confidentiality, integrity, and availability of private university data could be

expected to have severe or catastrophic adverse effects on university operations, university assets, or individuals.

(i) The need for confidentiality is high/required;

(ii) The need for integrity is high/required as the university data is internally trusted by or dependent on other university data or systems; and/or

(iii) The need for availability is high/required as the university data provides a critical or university-wide service.

(c) Access to and management of restricted university data is strictly limited and determined by data stewards, as unauthorized use or disclosure could substantially or materially impact the university's mission, operations, reputation, finances, or result in potential harm to members of the university community (e.g., identity theft).

(b) The classification of university data is subject to change as the attributes, considerations, or regulatory requirements of that data change.

(c) The following rules should be applied when classifying university data:

(i) When a set or collection of university data includes data of more than one classification, the set or collection of university data should be classified based on the most restrictive classification found in the set or collection.

For example, if a database contains both private and restricted university data, the database should be classified as restricted.

(ii) University data may be classified at a more restrictive classification; however, if this occurs, such data must meet the minimum-security measures for the more restrictive classification.

(3) Classification of university systems

(a) The three university system classifications are, from least to most risk:

(i) Low risk

(a) The system processes and/or stores public university data;

(b) The system is easily recoverable and reproducible; and/or

(c) The system provides an informational/non-critical service.

(ii) Moderate risk

(a) The system processes and/or stores internal university data;

(b) The system is internally trusted by or dependent on other university systems and its university data; and/or

(c) The system provides a normal or important service.

(iii) High risk

(a) System processes and/or stores private or restricted university data;

(b) System is highly trusted by or dependent on other university systems and its university data; and/or

(c) System provides a critical or university-wide service.

(b) University systems may be classified at a more restrictive classification; however, if this occurs, such systems must meet the minimum-security measures for the more restrictive classification.

(c) The classification of university systems is subject to change as the attributes, considerations, or regulatory requirements of those systems change.