# Ohio Administrative Code

## Rule 3337-93-01 Data classification.

Effective: June 30, 2016

The version of this rule that includes live links to associated resources is online at

https://www.ohio.edu/policy/93-001.html

(A) Overview

This policy establishes that all information assets will be classified according to their confidentiality, integrity and availability. This policy sets forth procedures based on those classifications so that the university can protect each asset in an appropriate manner.

This policy is based on federal information processing standards (FIPS) publication 199, "Standards for Security Categorization of Federal Information and Information Systems" and the corresponding NIST special publication, 800-53 revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations."

Key elements of this policy are the appointment of data stewards and the classification of data elements or data assets.

(B) Security objectives

As part of the university's data classification scheme, data will be classified, in terms of security, as high, medium, or low in three areas:

(1) Confidentiality

"Confidentiality" refers to the requirement and need for preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. Examples include student social security numbers, which require a high level of confidentiality; the contents of university work emails, which require a medium level of confidentiality; and the university's "front door" web pages, which require a low level of confidentiality.

(2) Integrity

"Integrity" refers to the necessity of guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. Student grades and university financial data are examples of data that requires a high degree of integrity.

(3) Availability

"Availability" refers to the requirement to ensure timely and reliable access to and use of information. Medical information, such as an individual's potential allergic reactions to certain drugs, is an example of data that has a requirement for a high degree of availability.

(C) Potential impact

(1) High

Failure to meet this particular security objective could pose a significant threat to: reputation, university mission, intellectual properties, legal compliance, financial health, or life or liberty. Information exempted from the "sunshine" laws usually has a high degree of confidentiality. Information regarding grades, confidential or proprietary research, health care, or personal financial information typically requires a high degree of integrity.

(2) Medium

Failure to meet this particular security objective could pose a moderate threat to: reputation, university mission, intellectual properties, legal compliance, financial health, or life or liberty. Typically, items in this classification are subject to release under the "sunshine" laws.

(3) Low

Failure to meet this particular security objective could pose little or no threat to: reputation, university mission, intellectual properties, legal compliance, financial health, or life or liberty. A low degree of confidentiality is typically used for information that is intended for public consumption.

(D) Data stewards

The data steward is the individual whom the university has identified as being responsible for the quality and utility of data elements. A primary duty of the data steward is to ensure that all data for which the steward has responsibility is properly rated and classified. The data steward is responsible for ensuring that a particular data element remains useful for the university, and that data is made available to appropriate parties as defined by role.

A data steward must be identified for all data elements that have a medium or high potential impact. The data steward works with Ohio university to ensure that the right policies, procedures, and operating practices are in place to protect the data element.

(E) University information security officer

The director of information security, fulfilling the role of university information security officer, is tasked to coordinate, develop, implement, and maintain an organization-wide information security program. This includes responsibility for the overall information risk posture of the university, and ensuring that the security objectives listed in this policy are adequately addressed.

(F) Procedures for levels of data

All institutional data shall be rated according its criticality in the dimensions of confidentiality, integrity, and availability. These ratings will occur over time, starting with those data elements that pose the greatest risk to the university, or that have the greatest compliance requirements.

A list of data elements with their corresponding data classification ranking will be generated by the information security office through collaboration with university parties, including at a minimum the listed reviewers of this policy, and approved by the Ohio university president and executive staff.

Those officially classified data sets and guidance for the different levels of data, including notation and suggested methods of protection will be included at https://www.ohio.edu/oit/security/Data-Classification.cfm.

The following policies apply to data elements at these particular levels. If a particular data element has a combination of ratings, the highest rating will take precedence. Failure to adhere to the following shall also be considered to be a violation of policy 91.003 and may result in disciplinary action.

(1) High

User roles or systems handling data with a high classification shall be reviewed and approved by the appropriate data steward, information security office, and chief information officer on an annual basis with appropriate input from interested parties throughout the university. Those systems and business processes surrounding the data elements shall be reviewed prior to being put into production, or containing sensitive information, and thereafter on an annual basis, by the information security office, to ensure that security controls are adequate.

(2) Medium

User roles or systems handling data with a medium classification shall be reviewed and maintained by the information security office, appropriate data steward, and supervisor or department head as appropriate. Those systems and business processes surrounding the data elements shall be reviewed on a periodic, sequential basis by the information security office, to ensure that security controls are adequate.

(3) Low

User roles or systems handling data with a low classification shall be reviewed and maintained by the appropriate supervisor or department head as appropriate. Guidelines for best practices in handling this classification of data will be provided by the information security office upon request. A security review of systems with a low security rating will be done by the information security office at the request of the department as time and resources allow.

The version of this rule that includes live links to associated resources is online at

https://www.ohio.edu/policy/93-001.html