DATA CLASSIFICATION POLICY

Policy Title:	**DATA CLASSIFICATION POLICY**
Policy Number:	**32-02**
Approval Date:	**1-19-2023**
Responsible Office:	**Office of Information Technology**
Responsible Executive:	**Vice President for Operations and Chief Strategist for Institutional Effectiveness**

Applies to: University Community

POLICY STATEMENT

Any person who uses, stores, maintains, or transmits University data has the added responsibility of safeguarding that data. The first step in establishing the appropriate safeguards for University data is to establish a framework to categorize the data based on its sensitivity and then to define the required level of security and control needed for each category. Data classification is a method of assigning data sensitivity based on an established rubric or data characteristics. Once classified, data can be controlled and secured based on its classification. The purpose of this policy is to establish the framework or rubric for classifying the University's institutional data. This Policy supersedes the University policies ADMINISTRATIVE POLICY # 32 – 8 – 4 (2014) IT System and Data Sensitivity Classification and ADMINISTRATIVE POLICY # 32 – 8 – 5 (2014) Sensitive IT System Inventory and Definition.

TABLE OF CONTENTS

DATA CLASSIFICATION POLICY

DEFINITIONS

Data Classification: In the context of information security, it is the assignment of a specific level of sensitivity to data based on the impact to the University should the data be disclosed, altered, or destroyed without authorization.

Data Element: A combination of characters or bytes (in electronic record keeping) referring to one discrete item of information such as name, address, or age.

Data Owner: A business lead responsible for the evaluation and classification of data and how data can be used, stored, shared, and transported.

Data Users: Faculty, staff, students, and others who have been authorized to access/use Norfolk State University's data resources, i.e., contractors, interns, volunteers etc.

Institutional Data: Recorded information that documents a transaction or activity by or with any appointed board member, officer, or employee of the Norfolk State University. The recorded information is an institutional record, regardless of physical form, if it is produced, collected, received, or retained in pursuance of university legal obligations or as the result of conducting university business. Institutional records include but are not limited to personnel, student, financial, patient, and administrative records. Record formats include but are not limited to email, electronic databases, files, both paper and electronic, audio, video, and images (regardless of the medium).

Personally Identifiable Information: Personally identifiable information (PII) is defined as information that describes, locates, or indexes anything about an individual including financial transactions, social security numbers, medical history, ancestry, religion, political ideology, criminal or employment records and photographic images which contain identifying characteristics.

CONTACT(S)

The Office of Information Technology (OIT) officially interprets this policy. OIT is responsible for obtaining approval for any revisions as required by BOV Policy # 01 (2014) *Creating and Maintaining Policies* through the appropriate governance structures. Questions regarding this policy should be directed to OIT.

STAKEHOLDER(S)

All users of Norfolk State University resources

POLICY CONTENTS

Data security measures must be implemented commensurate with the sensitivity of the University data and the potential risk to the University if said data is compromised. It is the responsibility of

the applicable Data Owner to evaluate and classify the University data for which he/she is responsible according to the classification system adopted by the University and described below. If a University data resource is comprised of data which has more than one level of sensitivity, all data shall be classified at the higher sensitivity level.

Once data is classified according to the system below, the controls defined in the Data Classification Matrix are to be enforced.

Data Classification Categories

Sensitive Data: Restricted data with the highest security\privacy requirement. Unauthorized disclosure of Sensitive data will have a catastrophic impact on the University or the University community. Sensitive data includes information protected by federal, state, or local laws and also regulations or industry standards, such as GLBA, HIPAA, HITECH, PCI-DSS and major identifiers such as Social Security Number, Passport Number, or Driver's License Number.

Confidential Data: Data that is protected by statutes, regulations, University policies or contractual language but if disclosed without authorization would not have the same catastrophic impact to the University as the unauthorized disclosure of sensitive data. Examples include grades and GPA, class schedule, class roster, transcripts, student health records not covered under HIPAA, and student conduct records.

Internal Data: Data that must be protected from unauthorized disclosure but has limited adverse impact on the University or community should it be disclosed. This includes Virginia HB 1 directory information and certain business information. Examples include internal business documents under NDA, internal intellectual property, some University financial data, and certain FERPA directory information such as name, date of birth, photograph, major field of study, and compilations of student email addresses.

Public Data: Data that is explicitly or implicitly approved for distribution to the public without restriction and disclosure of said data has little to no impact to the University or its community. Examples include enrollment numbers ready to be published, business process documents, and public reports.

Data Classification System

Data Owner Classification: Involves classifying data or data files according to a manual judgment by a knowledgeable user. Individuals who work with specific data or documents can specify data or document sensitivity. Sensitivity can be established when new data is introduced to a system, when a file or document is created, after a significant edit or review of a system, file, or document, or before data is released.

EDUCATION AND COMPLIANCE

The Director of IT Security (or designee) is responsible for official interpretation of this policy and providing education to the University community. Questions regarding the application of this policy should be directed to the Office of Information Technology. The Director of IT Security reserves the right to revise or eliminate this policy.

Violations of this policy will be addressed in accordance with the appropriate level of disciplinary action determined on a case-by-case basis by the appropriate Vice President or designee, with sanctions up to or including termination or expulsion from the University depending on the severity of the offense.

PUBLICATION

This policy shall be widely published and distributed to the University community. To ensure timely publication and distribution thereof, the Responsible Office will make every effort to:

- Communicate the policy in writing, electronic or otherwise, to the University community within 14 days of approval;
- Submit the policy for inclusion in the online Policy Library within 14 days of approval;
- Post the policy on the appropriate website; and
- Educate and train all stakeholders and appropriate audiences on the policy's content, as necessary. Failure to meet the publication requirements does not invalidate this policy.

REVIEW SCHEDULE

- Next Scheduled Review: 01/19/2029
- Approval by, date: President, 01/19/2023
- Revision History: 01/19/2023,01/19/2026
- Supersedes: ADMINISTRATIVE POLICY # 32 – 8 – 4 (2014) IT System and Data Sensitivity Classification and ADMINISTRATIVE POLICY # 32 – 8 – 5 (2014) Sensitive IT System Inventory and Definition policies.

RELATED DOCUMENTS

32-01 - Acceptable Use of Technological Resources
https://www.nsu.edu/policy/admin-32-01.aspx

38-10 - Information Security Policy
https://www.nsu.edu/policy/bov-38-10.aspx

Data Classification Matrix (In Development)

Virginia Department of Human Resources Management Policy 1.60 Standards of Conduct:
https://www.dhrm.virginia.gov/docs/default-source/hrpolicy/pol1_60.pdf?sfvrsn=2