XAVIER UNIVERSITY

Information Classification Policy

Effective: 4/20/2020

Last Updated:

Responsible University Office: Information Technology

Responsible Executive: Associate Provost and Chief Information Officer

Scope: This policy applies to all University owned information that is present on or transmitted through University owned systems and networks. University owned information assets can take the form of electronic and hard copy information.

A. REASON FOR POLICY

This policy ensures that data is identified, classified, labeled, and properly handled and protected in accordance with its importance and potential impact to Xavier University. Information must be properly handled throughout the entire lifecycle, from creation to disposal. The importance of information varies and therefore requires different levels of protection.

B. POLICY

1. The XTC Data Governance Subcommittee will oversee the data classification initiative in accordance with the XTC Data Governance Subcommittee Charter.
2. Data classification indicates the level of impact to Xavier University if the confidentiality, integrity, and/or availability is compromised. If the appropriate classification of a data asset is not obvious (e.g. not dictated by specific laws and regulations), consider the classification definitions as a guide to effectively classify the asset. All data will be classified commensurate with this policy.
3. Xavier University staff, faculty, non-employee associates, volunteers, students and any other authorized users that access data stores, information in any medium, and/or information systems and applications will comply with the Minimum Safeguard Standard.
4. Any Xavier University staff, faculty, non-employee associates, volunteers, students or authorized users who have violated this policy may be subject to disciplinary action, as outlined in the faculty, staff, or student handbooks. Unauthorized disclosure of

regulated data, such as personally identifiable information, may lead to legal repercussions.

C. DEFINITIONS

Public: Public information is defined as information that is generally available to anyone within or outside of the University. Access to this information is unrestricted and may be shared internally or externally without prior approval. Public information includes, but is not limited to, marketing materials, public web site contents, University statistics or any other information that has been approved by management for public release.

Internal use: Internal use information is defined as University information that is to be used within Xavier. Access to this data may be limited to specific departments and cannot be distributed outside of Xavier. Internal use information is less sensitive than Confidential information, but if exposed could have an adverse impact to the University. Internal use information includes but is not limited to strategic plans or other non-public information as dictated by the Data Custodian. All information not otherwise classified will be assumed to be internal use. Users may not disclose internal use information to anyone who is not an authorized user without prior consent of the Data Custodian.

Confidential: Confidential information is defined as personal or University information that may be considered potentially damaging if released and is only accessible to authorized users. Confidential information includes, but is not limited to, medical/health information, legally privileged information, contractual information, payment card information, personally identifiable information, protected health information and protected student information. Users may only share confidential information with people that require the information to perform their job. Sensitive HIPAA and FERPA information are considered confidential and should only be shared on an as needed basis and in compliance with any applicable laws.

Export Controlled: As a means to promote national security, the U.S. Government controls export of sensitive data, equipment, software and technology. This data is labeled Export Controlled. Users of Export Controlled data must follow all the safeguards for Restricted data plus additional safeguards as directed by The Data Trustees, Stewards, and Custodians of systems and applications that have Export Controlled data. The Custodians are responsible to identify appropriate additional safeguards.

Data Stewards: Data Stewards have operational planning and policy level responsibility for data within their functional areas. They assign individuals to serve as a Data Custodian from their area. In coordination with Data Custodians they implement and apply safeguards that meet or exceed the minimum safeguards of each data classification.

Data Custodians: A Data Custodian is the individual authorized by the appropriate Data Steward to be responsible for management of data which includes maintaining and controlling data quality as well as granting inquiry, entry and updating data privileges within their respective area of responsibility. Data Custodians must be and serve as the departmental data liaison for their specific area.

Data Custodians are responsible for the accuracy and completeness of data and responsible for the maintenance and control of data validation and rules tables. These tables, and processes related to their use, define how business is conducted at Xavier University. The Data Custodians are responsible for access control data within his/her charge. They make data available to others for the use and support of the office or department's functions.

XTC Data Governance subcommittee: Subcommittee to the XTC, responsible for establishment of data governance standards for all data at Xavier including establishment and enforcement of Banner as the Primary System of record. The XTC Data Governance Subcommittee is the body that reviews and approves how data is processed and stored at Xavier University.

Xavier Technology Committee (XTC): The Xavier Technology Committee (XTC) provides Information Technology (IT) governance for Xavier University.

D. PROCEDURES

1. Banner and Auxiliary Software Data Custodians will ensure that all Internal Use and Confidential data is appropriately identified and documented. This includes restrictions on e-mail or physical mail redistribution as outlined in the Minimum Safeguard Standards. Contact the Director of Information Security for details.
2. Any exception to this policy must be approved by the XTC Data Governance Subcommittee in writing.

E. EXHIBITS

Minimum Safeguard Standards

F. HISTORY

Updated 2/7/2020

Other applicable policies and/or resources:

Information Security Policy
Acceptable Use Policy