Title: **Sensitive Information Classification Policy**	**Policy Category:** **Risk Management & Security**
Issuing Authority: **Enterprise Risk Management**	**Responsibility:** **Information Security Program Council & Data Governance Council**
Publication Date: **11/15/2022**	**Next Review Date:** **11/15/2025**

Policy Statement/Background:

Stony Brook University is committed to the confidentiality, integrity, and availability of information important to the University's mission. University Data fall into one of three categories described in this policy. Data must be protected using the appropriate security measures consistent with the minimum standards for the classification category, where available.

Scope

This policy applies to all members of the university community, including West Campus, East Campus, Stony Brook University Hospital, the Long Island Veterans Home, Stony Brook Southampton Hospital, Stony Brook Eastern Long Island Hospital, and other units as may come under management of the University, as well as to third parties who handle University Data.

Policy:

Stony Brook classifies physical and electronic data into three risk-based categories for the purpose of determining access, permissions, and security precautions. This policy facilitates applying the appropriate security controls to University Data and assists data caretakers in determining the level of security required to protect data on the systems for which they are responsible.

All University Data fall into one of the three categories. Based on the data classification, individuals who use University Data are required to implement approved minimum-security standards, where available, for protecting the data. The standard for protecting the data becomes more stringent as the risk from disclosure increases.

University business processes must treat data according to this policy. Data that are personal to the operator of a system and stored on a university information technology (IT) resource as a result of incidental personal use are not considered University Data. University Data stored on non-university IT resources must still be verifiably protected according to respective minimum-security standards.

All data classified as Category 2 or Category 3 as described below are considered to be sensitive information (SI). Systems that store, transmit, or process SI are considered to be sensitive systems (SS).

Data Classifications

Data Risk Classification Category	**Category 3**
Risk to University from Disclosure	*High*
Definition	• The loss of confidentiality, integrity, or availability of the data or system would likely have a significant, adverse impact on the University's mission, safety, finances, or reputation. • Protection of the data is required by law/regulation or contractual agreement, or is otherwise highly sensitive. • Category 3 data includes private information defined in the New York State Security and Breach Notification Act. To this list University policy adds large sets of Category 2 records (1,000+ records). • Category 3 data may be exempt from disclosure/release under the New York State Freedom of Information Law (FOIL). • Data in this category often have mandatory notification requirements in the event of inadvertent disclosure.
Examples	• Social security number (SSN) • Driver license number • State-issued non-driver ID number • Bank/financial account number • Credit/debit card number (CCN) • Protected Health Information (PHI) • Passport number • University I.T. authentication credentials • Export controlled data • Large (1,000+ records) data sets of Category 2 records, including education and employee records

Data Risk Classification Category	**Category 2**
Risk to University from Disclosure	*Moderate*
Definition	• The loss of confidentiality, integrity, or availability of the data or system could have an adverse impact on the University's mission, safety, finances, or reputation. • Protection of data may be required by law/regulation or contract. • Includes University Data not identified as Category 3 data and protected by state and federal laws and regulations. This includes FERPA-protected student records and records that are specifically exempted from the disclosure requirements of New York State FOIL. • Data qualified to be released under the NY FOIL is not, by definition, exempt from classification as Category 2. • Data in this category must be protected to ensure that it is not inadvertently or unnecessarily disclosed.
Examples	• Small sets of education and employee records (under 1,000 records) • Personal information of employees and affiliates (salary, personnel files, disciplinary actions, home address) • Law enforcement investigation data, judicial proceedings data includes student disciplinary or judicial action information • Public safety information • IT infrastructure data • Collective bargaining negotiation data, contract negotiation data • Trade secret data • Protected data related to research • University intellectual property • University proprietary data • Data protected by external non-disclosure agreements • Inter- or intra-agency data which are not: statistical or factual tabulations; instructions to staff that affect the public; final agency policy or determination • Audit data • Licensed software • Nonpublic intellectual property • Documents protected by attorney-client privilege

Data Risk Classification Category	**Category 1**
Risk to University from Disclosure	*Low*
Definition	• Includes University Data not included in Category 3 or Category 2 and data that are intended for public disclosure. The loss of confidentiality of this data or the systems containing it would have insignificant impact on the University's mission, safety, finances, or reputation. • This category includes general access data, such as that available on unauthenticated portions of the University's website. • Public data have no requirements for confidentiality; however, systems housing the data should take reasonable measures to protect its integrity and availability.
Examples	• General access data, such as that on unauthenticated portions of the institution's website • Select HR directory information (name, department, position title, campus address) • Statistical information released to federal, state or other agencies for public disclosure

Definitions:

University Data: information collected or created through a function of the university.

Sensitive Information (SI): data classified as Category 2 or Category 3 as described in this policy.

Sensitive Systems (SS): systems that store, transmit, or process sensitive information.

Contact:

Additional information about this policy is available here:

Information Security Program Council (ISPC)
ISPC@stonybrook.edu

Relevant Standards, Codes, Rules, Regulations, Statutes and Policies:

- Data Classification Security Standards
- Information Security Program Administration Policy
- New York State Breach Notification Law
- SUNY Policy 6900: Information Security