Title: Policy on Data and Data Access	**Policy Category:** Information Technology
Issuing Authority: Educational and Institutional Effectiveness	**Responsibility:** Data Governance Council
Publication Date: 03/23/2023	**Next Review Date:** 03/23/2026

Policy Statement/Background:

This policy replaces former Division of Information Technology policies D100 Access to Institutional Data, D101 Classification and Use of Information Assets, and D109 Personnel Security Policy.

Policy:

University Data is information collected or created through a function of the University. Stony Brook University owns University Data.

Access to University Data requires a legitimate educational or institutional purpose. Access is limited to the minimum data needed to accomplish this purpose with reasonable technical and administrative burden and in compliance with applicable statutory and regulatory requirements.

Roles & Responsibilities

All Data Assets of the University fall under the purview of Data Trustees. Data Trustees have the ultimate responsibility for designated Data Assets, including the security, confidentiality, integrity, usability, retention, and disposition of University Data. Data Trustees delegate care and management of University Data to Data Stewards.

Data Stewards are responsible for the development, maintenance and management of policies and procedures for one or more Data Assets (effective 6 months from the publication of this policy). This includes keeping an inventory of Data Asset contents, implementation of consistent data standards; maintenance of a data dictionary; and communication of data governance policies, procedures, and

practices.

For Data Assets in their care, Data Stewards shall develop appropriate access controls, as technically and operationally feasible, consistent with the data's confidentiality, sensitivity and use. They will create and maintain written procedures for routine and non-routine access for Data Assets in their care, as well as written procedures for user management. Such procedures must be consistent with Stony Brook's [Sensitive Information Classification Policy](#) and contain a description of how users are managed, including: how users are added, removed, granted special privileges, and periodically reviewed to ensure access is appropriate. Access procedures may place stipulations on how data are used, stored, re-disclosed, or re-purposed. Procedures must be approved by the Data Trustee and reviewed no less than every three years. The Data Governance Council maintains guidelines to help Data Stewards develop reasonable and consistent procedures for data access.

Data Custodians implement and enforce security and access rules and policies established by Data Stewards and the University at-large (effective 9 months from the publication of this policy). They grant and remove access to specific users and/or data, follow prescribed data handling procedures, and comply with federal and state laws and regulations and University policies for the data in their custody.

Routine Access

Procedures for routine access include how access is evaluated and granted for an employee, as well as a persistent or episodic connection to another internal or external data system. Access to data is granted to employees whose job responsibilities require ongoing access to the data. Persistent or episodic connections of Data Assets to internal or external systems must include an evaluation of the extent to which access will advance the mission of Stony Brook University, the cost of administrative burden, the risk to individual privacy, and the risk to the University of extending access to the data. Connections to external systems are subject to Stony Brook's cybersecurity policies and procedures. The Data Trustee is the final arbiter for approval of access.

Non-routine Access

Non-routine access to University Data also requires a legitimate educational or institutional purpose and may also require consideration of additional criteria. Stony Brook University releases University Data and information to comply with federal, state, and local laws and regulations; meet requirements of the SUNY system; and advance the mission of Stony Brook University. Requests for non-routine access are reviewed on a case-by-case basis, in accordance with the area's procedures for data access. These criteria include the extent to which access will advance the mission of Stony Brook University, the cost of administrative burden, the risk to individual privacy, and the risk to the University of extending access to the data. Non-routine access to University Data must have a time limit, a plan to store data securely and appropriately, appropriate restrictions on subsequent disclosure, and a

requirement to destroy local copies of data in an approved fashion. The Data Trustee is the final arbiter for approval of access.

Formal requests to access University Data made through legal proceedings or the New York Freedom of Information Law are subject to statutory and regulatory requirements.

Definitions:

Data Assets: information-based resources of significant scope, comprised of University Data. Data assets include repositories of University Data, systems housing university data, and services that host University Data.

Data Custodians: employees responsible to implement and enforce security and access rules and policies established by Data Stewards and the University at-large. Data Custodian responsibilities may be assumed by Data Stewards as appropriate.

Data Stewards: designated by a Data Trustee to develop, maintain, and manage policies and procedures for one or more data assets. Data Stewards may also assume responsibilities as Data Custodians as appropriate.

Data Trustees: senior leaders of the University at the level of Vice President, Vice Provost, or higher who have responsibility for designated data assets.

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

Contact:

Additional information about this policy is available here:

Office of Institutional Research, Planning, and Effectiveness
315 Administration Building
Stony Brook, NY 11794
(631) 632-6210

Relevant Standards, Codes, Rules, Regulations, Statutes and Policies:
- [Family Educational Rights and Privacy Act (FERPA)](#)
- [Gramm-Leach-Bliley Act](#)
- [Health Insurance Portability and Accountability Act](#)
- [Information Security Program Administration Policy](#)
- [Sensitive Information Classification Policy](#)