Title: **Information Security Program Administration Policy**	**Policy Category:** **Risk Management & Security**
Issuing Authority: **President**	**Responsibility:** **Enterprise Risk Management & Information Security Program Council**
Publication Date: **11/18/2022**	**Next Review Date:** **11/18/2025**

Printed copies are for reference only. Please refer to the electronic copy for the latest version.

Policy Statement/Background:

Stony Brook University (SBU) is committed to safeguarding **Sensitive Information** and **Sensitive Systems**. An Information Security Program will be leveraged to balance the need for securing information assets against its ongoing operational needs.

Scope

This policy applies to all Stony Brook University departments and community members using information created or collected through a function of the University. Stony Brook Medicine, FSA, Research Foundation, and the Stony Brook Foundation will coordinate with the **Information Security Program Council (ISPC)**, but may maintain additional policy, procedure, security controls and documentation that do not conflict with policy and procedure published by the University or the **ISPC**.

Policy:

Information Security Goals

Pursuant to federal and state laws and SUNY policy, SBU must maintain an effective and comprehensive information security program (**Program**) that addresses the full range of information security issues that affect the

University. The **Program** will implement an Information Security Program according to industry standards. In so doing, the **Program** will:

- Lead and assist the workforce in preserving the confidentiality, integrity, and availability of Sensitive Information;
- Give special attention to preserving the confidentiality of information that bears directly on the privacy, health, and property rights of persons with whom SBU has business transactions, including students, employees, alumni, applicants, patients, contractors, vendors, and customers;
- Lead and assist the workforce in protecting Sensitive Systems; and
- Engage all employees, as appropriate to their roles, in actively anticipating and addressing threats and hazards to the security of Sensitive Information and Sensitive Systems.

Responsibility for Information Security

Pursuant to industry standards, the University's senior leadership must:

- Oversee the **Program's** implementation;
- Identify, authorize, and require specific individuals to implement the **Program;** and
- Ensure individual managers are assigned ownership and stewardship responsibilities for critical information assets.

All employees, as appropriate to their jobs, must treat **Sensitive Information** and **Sensitive Systems** in accordance with the principles and procedures established by the **Program**.

All supervisors must implement and monitor procedures, as appropriate to their business units' work, to support and encourage the proper treatment of **Sensitive Information** and **Sensitive Systems.**

The **ISPC** has been identified and authorized to implement the Program and publish related policy, procedure and standards. Individual membership will be maintained in a separate document.

Set of Information Security Policies

Stony Brook University must maintain a comprehensive set of information security policies governed by the **Program**. Additionally, SBU will promulgate to appropriate audiences each of the policies in this set and educate workers regarding the content and intent of the policies.

Waivers and Exceptions

Any waiver of requirements set forth in these policies must be established through formal procedures, documented by the **ISPC**, which justifies the waiver based on risk and business value and define either an acceptable period for expiration of the waiver or process for renewal consideration.

Definitions:[1]

Access: relating to information – to view, read, decrypt, share, speak aloud, listen to, create, collect, store, move, copy, transmit, or delete. Relating to objects, such as Sensitive Systems – to touch, log into, modify, configure, move, remove, steal, destroy.

Active: relating to information – having authorization to access or modify information. Relating to objects, such as Sensitive Systems – having authorization to access or modify the system configuration or operating system.

Approved: relating to information and system security procedures – written in the University's policies or procedures, or accepted by management through precedent and long-standing, operationally required practice, where such practice does not conflict with written policy and procedure.

Authorization: formal permission provided to an individual with the knowledge and approval of the director of a department that is authorized to give such permission.

Breach Notification: the procedures to notify persons that their personal information was or might have been acquired by a person without authorization. Such procedures are legally required by many jurisdictions including New York State.

Container: relating to information – a structure that can hold a physical or digital representation of information (i.e., data), such as a computer, database, computer folder, building, room, paper file cabinet.

Department: a University functional office.

[1] Not all terms defined in this policy are used herein, but may be used in other related policies.

Departmental SI Declaration: a chart maintained by a SI Department that shows which SI Categories are active in which of its business functions.

Departmental Workforce Inventory: a chart maintained by a department that shows which workers, if any, are active with which SI Categories.

Information Security Program: a formal management function, with written goals and charges, that seeks to address the full range of information security issues that affect the organization and seeks to align its practices with applicable laws, regulations, policies, and standards of practice.

Information Security Program Council (ISPC): the people and associated procedures that administer the Program.
Modify: as related to information – to alter, encrypt, distort, deface, delete, hide or otherwise block access.

Personally Issued Technology (Technology): the University's information and communication technology as it is issued (assigned or made available) to individuals for conducting the University's business.

Program: the Stony Brook University Information Security Program, which includes efforts put forth by the ISPC and efforts employed by Stony Brook Medicine, FSA, Research Foundation, Stony Brook Foundation, and the Computer Science Department.

Program Document: a formal, published document maintained and used by the Program.

Program Library: a formal location for Program Documents.

Public Information: SE Information that is presented in an approved medium that intentionally enables the public to access it, although usually not to modify it.

SE Information: SUNY Entity information. Information created or collected through a function of the University.

SE System: SUNY Entity system. A computer or network-based system, including applications and databases, operationally managed by a University function.

Sensitive Information (SI): SE Information subject to security controls overseen by the Program.

Sensitive Information Department (SI Department): a department that is active with one or more SI Category.

Sensitive Information Category (SI Category): category of Sensitive Information defined in policy using operational details meaningful to the University's operations in order to assist managers in identifying instances of the information.

Sensitive Information Worker (SI Worker): an employee that is active with SI.

Sensitive System (SS): SE system subject to security controls overseen by the Program.

Sensitive System Category (SS Category): category of Sensitive System defined in procedure using operational details meaningful to the University's operations in order to assist managers in identifying instances of such systems.

Sensitive System Worker (SS Worker): an employee that is active with SS.

User: anyone, whether an employee or not, who has been granted permission to use the University's Personally Issued Technology (Technology).

Virtual: as related to digital structures (images, files, and containers); as presented or simulated for an audience, consumer, user, etc., regardless of the underlying construction.

Contact:

Additional information about this policy is available here:

Enterprise Risk Management
180 Administration Building
Stony Brook, NY 11794
(631) 632-9500

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

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

- SUNY Policy 6900: Information Security
- Stony Brook Cybersecurity Website