Access to Institutional Data  D 100

University data must be secured against unauthorized access, creation, modification or destruction to ensure its accuracy, integrity and availability. The value of University data is increased through its appropriate use; its value is diminished through misuse, misinterpretation, unnecessary restrictions to access and/or failure to maintain data quality.

The University’s Division of Information Technology ("DoIT") is committed to minimizing vulnerabilities that may result from compromised operating system integrity or application security problems, as well as protecting against the unauthorized disclosure or misuse of any information stored on any device connected to the University’s network infrastructure. To ensure the continued integrity of its information technology resources, the University may audit, inspect and/or monitor them, at any time.

Data requests:

Access to University data is governed by University policy as well as state and federal law. Requests for information from any source shall be referred as follows:

Freedom of Information Law:
University Records Access Officer, 291 Administration Bldg.

Court order or subpoena:
Office of University Counsel, 328 Administration Bldg.

Research data:
Office of the Vice President for Research, W-5530 Melville Library
Committee on Research Involving Human Subjects (CORIHS), W-5530, Melville Library. See generally University Policy 202R.

Quality-assurance research data:
Office of Institutional Research, 488 Administration Bldg.

Student data:
Office of the Registrar, 276 Administration Bldg.

Protected Health Information (PHI):
Health Information Management, MR-13, South Tower University Hospital

Employee data:
Human Resource Services, 390 Administration Bldg. or Hospital Human Resources, 3 Technology Drive, Suite 100
The following index lists some of the laws, policies and guidelines that regulate user access to data maintained on University networks, communication systems and computer resources.

Alumni/Donor data:
Office of the Vice President for Advancement, Administration Building
Stony Brook University Policies

Division of Information Technology
Information Technology Department
SUNYSB HIPAA Policy
SBUH Policies 0038, 5007
SBU Policies 105, 109, 507, 510, 512
SBU Student Conduct Code Article II A 6

State University of New York Policies

SUNY Policies & Procedures: Use of Facilities by Non-Commercial Organizations
SUNY Administrative Policy Item 007.1: State University Campuses or Facilities: Use of Computer Equipment or Services by Non-Affiliated Institutions and Organization
SUNY Administrative Policy Item 008: University Policy on the Use of University: Facilities by Non-Commercial Organizations: Attachment A
NYS Office for Technology: Technology Policy 97-1 Information Security Policy, Technology Policy 96-19 - Data Sharing Among Agencies

State and Federal Law

15 USC § 6801: Gramm-Leach-Bliley Act
17 USC § 101: Copyright Act
17 USC § 512: Digital Millennium Copyright Act
18 USC § 1030: Computer Fraud & Abuse Act
18 USC § 1302: Crimes (email fraud)
18 USC § 2252: Crimes (exploitation of minors)
18 USC § 2501: Electronic Communications Privacy Act
20 USC § 1232g: Family Educational Rights and Privacy Act
42 USC § 1320a: Health Insurance Portability and Accountability Act
42 USC § 2000e: Civil Rights Act
44 USC § 2901: Electronic Records Management Part 1234.28
NY Penal Code §§ 156, 170
NY Executive Law § 296
NY Public Officers Law §§ 84, 91

INQUIRIES/REQUESTS:

Office of the Chief Information Officer

ECC 231