P109.1. Scope

This Policy applies to all Users of IT Systems, including but not limited to University students, faculty, and staff. It applies to the use of all IT Systems. These include systems, networks, and facilities owned, leased, administered or otherwise provided by DoIT, as well as those owned, leased, administered or otherwise provided by any Stony Brook University (SBU) entity including but not limited to individual schools, departments, laboratories, etc., Use of SBU IT Systems, including activities using such IT Systems but performed on a privately owned computer that is not managed or maintained by SBU, is governed by this Policy.

P109.2. Policy Statement

The purpose of this Policy is to ensure an information technology infrastructure that promotes the basic missions of the University in teaching, learning, research, patient care, and administration. In particular, this Policy aims to promote the following goals:

A. To ensure the integrity, reliability, availability, and superior performance of IT Systems;
B. To ensure that use of IT Systems is consistent with the principles that govern use of other University facilities and services;
C. To ensure that IT Systems are used for their intended purposes; and to establish processes for addressing policy violations and sanctions for violators.
D. To outline the circumstances under which access or usage of campus IT Systems may be limited or restricted.

The SUNY Board of Trustees policy on Academic Freedom remains in full force and effect and is undiminished by this policy.

P109.3. Definitions

3A. IT Systems: These are the computers, terminals, printers, networks, online and offline storage media and related equipment, software, and data files that are owned, leased, administered, managed, maintained or otherwise provided by SBU. For example, IT Systems include but are not limited to institutional and departmental information systems, faculty research systems, desktop computers, the University's campus network, and University general access computer clusters (SINC sites).

3B. User: A "User" is any person, whether authorized or not, who makes any use of any IT System from any location. For example, Users include a person who accesses IT Systems in a University computer cluster, or via an electronic network.

3C. Systems Authority: The individual, subdivision, department or office to which Stony Brook University has delegated oversight of a particular system.

3D. Systems Administrator: Systems Authorities may designate another person as "Systems Administrator" to manage the particular system assigned to him or her. Systems Administrators oversee the day-to-day operation of the system and are authorized to determine who is permitted access to particular IT resources.

3E. Certifying Authority: This is the Systems Administrator or other University authority who certifies the appropriateness of an official University document for electronic publication in the course of University business.

3F. Specific authorization: This means documented permission provided by the applicable Systems Administrator.
P109.4. Policy Sections

4.A. Appropriate use of IT Systems

This Policy sets forth the general parameters of appropriate use of IT Systems. Faculty, students, and staff should consult their respective governing policy manuals and SUNY policies for more detailed statements on permitted use for their role within the community. In the event of conflict between IT policies, this Appropriate Use Policy will prevail.

4A.i. Appropriate Use. IT Systems may be used for any and all purposes pertaining to a user’s academic position and/or position related responsibilities and assignments with the exception of cases outlined below in Section 4.A.iii.. Use must also be consistent with all other applicable laws, rules and regulations and SUNY’s and the University’s policies and guidelines. All uses inconsistent with these objectives and requirements are considered inappropriate use and may jeopardize further access.

4.A.ii. Proper Authorization. Users are entitled to access only those elements of IT Systems that are consistent with their authorization. Use of University IT system is a privilege, not a right.

4.A.iii. Specific Proscriptions on Use. The following categories of use are inappropriate and prohibited:

4.A.iii.a. Use that impedes, interferes with, impairs, or otherwise causes harm to the activities of others. Users must not deny or interfere with or attempt to deny or interfere with service to other users in any way, including by "resource hogging," misusing mailing lists, propagating "chain letters" or virus hoaxes, "spamming" (spreading email or postings widely and without good purpose), or "bombing" (flooding an individual, group, or system with numerous or large email messages). Knowingly or recklessly distributing of unwanted mail or other unwanted messages is prohibited. Other behavior that may cause excessive network traffic or computing load is also prohibited.

4.A.iii.b. Use that is inconsistent with Stony Brook’s status as a public university. IT Systems may not be used for private and/or private commercial purposes or for financial gain, or other than for incidental personal use.

4.A.iii.c. Use of IT Systems in a way that suggests University endorsement of any political candidate or ballot initiative is also prohibited. The use of IT Systems shall be in accordance with SUNY and University policy on the use of University facilities for political purposes.

4.A.iii.d. Harassing or threatening use. This category includes, for example, display of offensive, sexual material in the workplace and repeated unwelcome contacts with another person.

4.A.iii.e. Use damaging the integrity of University or other IT Systems. This category includes, but is not limited to, the following activities:

4.A.iii.f. Attempts to defeat system security. Users must not defeat or attempt to defeat any IT System's security, for example, by "cracking" or guessing and applying the identification or password of another User, or compromising room locks or alarm systems.

4.A.iii.g. Unauthorized access or use. The University recognizes the importance of preserving the privacy of Users and data stored in IT systems. Users must honor this principle by neither seeking to
obtain unauthorized access to IT Systems, nor permitting or assisting any others in doing the same. Users are prohibited from accessing or attempting to access data on IT Systems that they are not authorized to access. Furthermore, Users must not make or attempt to make any deliberate, unauthorized changes to data on an IT System. Users must not intercept or attempt to intercept or access data communications not intended for that user, for example, by "promiscuous" network monitoring, running network sniffers, or otherwise tapping phone or network lines.

4.A.iii.h. **Disguised use.** Users must not conceal their identity when using IT Systems, except when the option of anonymous access is explicitly authorized. Users are also prohibited from masquerading as or impersonating others or otherwise using a false identity.

4.A.iii.i. **Distributing computer viruses.** Users must not knowingly distribute or launch computer viruses, worms, or other rogue programs.

4.A.iii.j. **Modification or removal of data or equipment.** Without specific authorization, Users may not remove or modify any equipment or data from IT Systems.

4.A.iii.k. **Use of unauthorized devices.** Users are expected to use caution when attaching any devices to IT systems at SBU. These devices may include but are not limited to external disks, printers, or video systems. Devices such as wireless routers which may potentially affect or disable University networks or broader access to University systems require DoIT authorization.

4.A.iii.l. **Use in violation of law.** Illegal use of IT Systems -- that is, use in violation of civil or criminal law at the federal, state, or local levels -- is prohibited. Please review University Copyright Policy P512.5 and other applicable policies.

4.iii.m. **Use in violation of University contracts.** All use of IT Systems must be consistent with the University's contractual obligations, including limitations defined in software and other licensing agreements.

4.A.iii.n. **Use in violation of University policy.** Use in violation of other University policies also violates this AUP. Relevant University policies include, but are not limited to, those regarding sexual harassment and racial and ethnic harassment, as well as University, departmental, and work-unit policies and guidelines regarding incidental personal use of IT Systems.

4.A.iii.o. **Use in violation of external data network policies.** Users must observe all applicable policies of external data networks when using such networks.

**4.B. Personal Account Responsibility.** Users are responsible for maintaining the security of their own IT Systems accounts and passwords. Any User changes of password must follow published guidelines for passwords. Accounts and passwords are normally assigned to single Users and are not to be shared with any other person without authorization by the applicable Systems Administrator. Users are presumed to be responsible for any activity carried out under their IT Systems accounts or posted on their personal web pages.

**4.C. Responsibility for Content.** Official University information may be published in a variety of electronic forms. The Certifying Authority under whose auspices the information is published is responsible for the content of the published document. Users also are able to publish information on IT
Systems or over Stony Brook's networks.

4.D. Personal Identification. Upon request by a Systems Administrator or other University authority, Users must produce valid University identification.

4.E. Conditions of University Access
The University reserves the right to examine, without user consent, material stored on or transmitted through its IT Systems if there is reason to believe that the standards for appropriate use in this policy are being violated or if required to carry on its operations. IT will seek review of the circumstances for access by the Office of General Counsel. Circumstances under which the University may exercise its rights include:

4.E.i. When necessary to identify or diagnose systems or security vulnerabilities and problems, or otherwise preserve the integrity of the IT Systems; or
4.E.ii. When required by federal, state, or local law or administrative rules; or
4.E.iii. When such access to IT Systems is required to carry out necessary business functions of the University; or
4.E.iv. When required to preserve public health or safety; or
4.E.v. When there are reasonable grounds to believe that a violation of law or a breach of University policy may have taken place and access and inspection or monitoring may produce evidence related to the misconduct; or
4.E.vi. For users who were members of the Stony Brook faculty or staff: when the User’s employment at the University has ended.

P109. 5. User access deactivations. In addition to accessing the IT Systems, the University, through the appropriate Systems Administrator, may deactivate a User’s IT privileges, whether or not the User is suspected of any violation of this Policy, when necessary to preserve the integrity of facilities, user services, or data. The Systems Administrator will attempt to notify the User of any such action.

P109.6. Use of security scanning systems. By attaching privately owned personal computers or other IT resources to the University's network, Users consent to University use of scanning programs for security purposes on those resources while attached to the network.

P109.7. Logs. Most IT systems routinely log user actions in order to facilitate recovery from system malfunctions and for other management purposes. Systems Administrators are required to establish policies and procedures concerning logging of User actions, including the extent of individually-identifiable data collection, data security, and data retention.

P109.8. Enforcement Procedures

8.A. Complaints of Alleged Violations.
If an individual has observed or otherwise is aware of a violation of this Policy, he or she may report any violation to the Systems Authority overseeing the facility most directly involved, or to the Chief Information Officer which must investigate the allegation and (if appropriate) refer the matter to University disciplinary and/or law enforcement authorities.

8.B. Disciplinary Procedures. Alleged violations of this Policy will be pursued in accordance with the appropriate disciplinary procedures for faculty, staff, and students.
8.C. Legal Liability for Unlawful Use. In addition to University discipline, Users may be subject to criminal prosecution, civil liability, or both for unlawful use of any IT System.

P109.9 Policy Development
This Policy shall be periodically reviewed and modified by the Chief Information Officer, in consultation with relevant SBU committees, faculty, students, and staff.