(P109) Appropriate Use of Information Technology

User Standards in Support of P109

Policy on Use of Cable Television

(D100) Access to Institutional Data

(D101) Classification and Use of Information Assets

(D102) Network Security

(D103) Server Security

(D104) Workstation Security

(D105) Credential Security

(D106) Email

(D107) Information Security Governance

(D108) Information Security Program Roles and Responsibilities

(D109) Personnel Security Policy

(D110) Operational Management Policy

(D111) Stony Brook University Google Apps for Education Acceptable Use and Data Security Policy

(D112) Electronic Mail (Email) Retention Policy

(D120) Web Resources

(D121) Internet Videoconferencing and Virtual Meeting Rooms

(D123) Domain Name Policy

Plan to Combat Unlawful Distribution of Copyrighted Material

Faculty/Staff Personal Computer Policy

Acknowledgement and Compliance Statement

Re i ed Ma 17, 2012

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 Ď

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).

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). Knowing or reckless dis

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