Mike Ledgerwood <mike.ledgerwood@sunysb.edu>

11/29/2005 03:29 PM

To Mike Ledgerwood <mike.ledgerwood@sunysb.edu>

cc sdinkins@notes.cc.sunysb.edu, jolyon.jesty@stonybrook.edu, gzelinsky@notes.cc.sunysb.edu, Scott Sutherland

bcc

Subject Second Minutes of Senate Computing and Communication Committee

Please send me all revisions. Sorry for the length!!!

I am sending as both attachment and included in the e-mail.

P.S. Is either the 9th around 3 PM or the 16th possible for a last meeting?

Senateminutes22005.doc

University Senate Committee on Computing and Communications

Meeting minutes of Nov. 11th, 2005. Second meeting. Apologies for the length of the minutes.

The meeting came to order at 2:15 in the European Languages, Literatures, and Cultures Conference Room. Present: Lin, Rohlf, Cohen, Lagos, Ledgerwood and special invited guest: Rich Reeder, Stony Brook's Chief Information Officer. Two other members phoned/ wrote in questions for the meeting.

The Committee welcomed Rich and then proceeded to work its way through the minutes of the first meeting, getting comments from Rich on each item the committee addressed at that meeting.

1) The first item was the PR 109. Rich had sent the entire committee two documents before this meeting that outlined what is happening with questions of policy on computing. These items are attached at the end of the minutes. The committee's questions related to the need to have links to the laws mentioned in one of the attached items (Rich will look into have the links present on web site where the policy is listed) and whether the HIPAA privacy regulations would have to be enforced all over campus (no). In fact the new network being created for research faculty on East Campus who don't deal with patients should underline this fact. At the same time, it is also important to note that any machine with any patient information MUST be behind the hospital firewall/protection. An additional matter discussed was the fact that Notes, with its built-in security has to be used on clinical/patient computers. Notes also has built-in encryption for its forwarded mail as required by HIPAA.

As an aside, we had a report on the new HSC ARCAN network. It is in the last stages of being created. The first department to be on the network will be pharmacology with other departments to be added as soon as all works well with the first department. After entire departments are added, then it will be possible to discuss adding parts of departments, too.

3) In our continuing discussion of the need for more technology in

teaching classrooms Rich told us that soon there should be someone new responsible for addressing this question. He announced that a search has been approved for a new administrator who will take over Instructional Computing (since Nancy Duffrin is retiring), the Center for Excellence in Teaching and Learning (CELT, which has been without a director for several years) and also supervise Educational Technologies (Gary Van Sise's and Javitts Lecture Center's unit). The holder of this position will be a senior administrator and will report to both the CIO and the Provost. A search committee has now been formed and two of this committee's members (Rohlf and Ledgerwood) have been named to it. The first meeting of this committee will be on Dec. 7th. At that meeting a job description will be discussed as well as other aspects of the search.

4) Lin brought up the topic of the East Campus/West Campus divide over computer support, especially Notes support. Rich told us that he simply doesn't have the staff to do support for Notes for 3500 East Campus Notes users as well as West Campus. Given extra funds he could do more in the way of support for East Campus however, although he did note, again, that Notes differs from East to West Campus, including the need to have PH1 certification in East Campus Notes. The committee decided to send these minutes to Dennis Proul, East Campus CIO, to ask for his ideas on why there are so many complaints about computer support on East Campus, especially for Notes users, and so many complaints about the Help Desk as well.

5) We talked with Rich about what is happening with wireless on campus, including the status of the new Humanities Building. The new Humanities building should have wireless capability by January. Rich talked about other areas that might have wireless soon, such as the Wang Center and the SAC as well as more spots in the Library. The committee felt that expanding wireless was, generally, a good idea, especially since we will have a Center for Excellence in Wireless Computing soon. See the next item, too.

6) The committee continues to be very interested in seeing that a single, simple authentication procedure will be implemented for all campus computer users for Solar System, the libraries, virtual private networking (VPN) and wireless. Rich told us that a lot of progress has been made on this during the past year. In January services will be turned on for authentication using Microsoft's Active Directory (ADAM). Eventually there will be a master key for all authentication. This will be the SOLAR system ID and password. From that account users will be able to change passwords in the two other logins they will still have to use. They will still have to have a separate Notes login and password and a separate "Net ID" which they will use for VPN, library, wireless, and dial-in. Still, this is quite an improvement over the current situation. Rich did mention that one of the problems with this implementation is the number of users who use UNIX for mail or other authentication since the Microsoft application is not secure for them.

7) We did not discuss paying for a web site that would allow us to prove student plagarism. This is a subject to be discussed again.

8) Wei Lin again brought up the fact that faculty like him and some of the rest of the committee (as well as others not on the committee) would really benefit from the creation of something like a "Power Users Group". [Upon their agreement I can quote from e-mails that he and Charlie Bowman exchanged. Here is the text I would add if they

both agree, starting with Wei's questions. I would welcome any editing to this text as well:

{The first question is the sharing of client support knowledge base to the IT staff in campus departments. It will certainly help them to fix problems that already have solutions and relieve some load from client support. I have visited the client support website and found some technical information. But I feel they are more like FAQs. Do you have an internal knowledge base that can be shared?

The second question is the communication between the client support or DoIT and the departmental IT staff. Currently there is a USB tech support mailing list, which I am on, distributing updates from DoIT. However, it seems there is no efficient way for the departmental IT staff to communicate back directly to the client support. I am suggesting to make phone numbers, email addresses and support area of the client support staff available to the people on the USB tech support list. If this does not work out,, another alternative may be to provide the people on the mailing list priority access to support staff when they call 2-9800.

The third issue is if it is possible for DoIT to host technical brief meetings and invite the departmental IT staff on a regular base, e.g. quarterly or every semester. I think it will be a good opportunity for them to learn what campus computing resources are available and give feedback. The LDAP, which will be rolled out soon, will be a good topic of such meetings. This can also be a social event that the DoIT staff and departmental staff get to know each other.

Here is the answer from Charlie Bowman:

First, I want to say that I agree with all three issues that you have mentioned in your email. In my opinion they are issues that one would have a hard time arguing against. However, as with many issues at SBU, it comes down to a question of allocation of resources versus workload. I would welcome the opportunity to present to your committee my view of the management problems that, I believe, are unique to Client Support in this regard.

Knowledge sharing can and should be accomplished. At one time we did have a document database that was shared, however we also have a considerable amount of information that should not be shared. It became very time consuming to understand which was which and when to search what. So, we reverted to a secure database. I am searching for some software that might make web based knowledge sharing easy and simple to do. While some of the present offerings on the web are FAQs, others are full tutorials on certain subjects. It's a trade off based on whether we think the web user is just looking for one piece of information or an entire explanation.

Communication between DoIT and departmental IT staff can be improved. There are several means of communication that already exist. USB Tech Support consists of three public groups in notes (East Campus, West Campus

and Interested Parties). They are available for anyone to use, in and outside of Notes. SupportTeam@notes.cc.sunysb.edu as advertised on our web site under “Contact Us” is our mail in database for sending questions, solutions or requests to Client Support. Also on our web site is an automated “Submit a Help Request” link. All of these may be used to contact Client Support.

Our 2-9800 telephone number is the best way of contacting anyone in Client Support. Since all of out techs are called on to do site visits, or attend meetings, one is never certain as to the availability of any given tech at any particular time. There is one tech designated to be on phone support during the morning and afternoons. So, after the phone is answered by our students, the call can be directed to a tech designated for phone support at that given time. Our techs do specialize in certain areas so sometimes there is merit in contacting a particular tech. However, messages are taken by our students for anyone in Client Support and emailed to that tech. I am sure we could provide some procedure for departmental techs to identify themselves to our phone support for some kind of special handling of the call.

I have recognized the need for all of DoIT to communicate more often and more effectively with the University Community. I have written a position description for an individual that would coordinate DoIT’s communications. In addition to things such as newsletters and announcements, this person would also review University publications to make sure that they contain the correct instructions for using our IT resources. This effort is proceeding and has been endorsed by the CIO.

Technical Briefings. This is a good idea and I will work on this for the Spring ’06 semester. I know we are going to have a presentation from Microsoft about Windows Vista in March. That should be opened up to the entire campus. I recognize that there are other local issues that should be addressed also. Your last sentence brings me to a topic that is dear to me, “DoIT staff and Department staff get to know each other”. With the requirement for administrative passwords and increased security and patch maintenance on individual desktop workstations, it is very important to clearly define the responsibility for support. Both from the stand point of the provider as well as the requester. Client Support often receives calls from users that have no idea where or who placed that machine on their desktop. And, it is often the case that Client Support doesn’t know

either. And of course, there is the other approach to support that many Stony Brook users take. They call several support provides to see who gets there first. Many university web sites have pages that clearly indicate where support is supposed to come from. I would like to work to
that end and would certainly host such a page.

I hope this answers some of your questions. As stated above, I would welcome the opportunity to discuss any of these answers with the Committee.

9) Stephanie Dinkins again brought up questions about the faculty addendum which the Provost requires faculty to do to be considered for merit raises. She and others questioned why it had to be entered via Lotus Notes user name and password. Rich responded that this was still a question of authentication. When informed that faculty and chairs did not know if an addendum had even been filed since there was no note of confirmation, he explained that the addendum did not work like a typical web site for ordering items. Instead, the user was populating a data file with all of the information supplied. All of the data, once saved, was saved permanently. So, a user who entered data and saved it had an updated addendum file, even without knowing it. Still, the committee explained that a user, especially someone not familiar with data files and Notes, would not know that he or she had actually created a file to satisfy the Provost's demand that a file exist for a merit pay raise. The committee, humorously, discussed what kinds of buttons and responses needed to be created by DoIT to help faculty realize they actually had a file for raises.

10) Ledgerwood mentioned that he had been contacted by UMass Amherst concerning their difficulties with PeopleSoft and agreed to answer questions by their Senate Committee (equivalent to this committee). Rich agreed to help with this if needed. Jim Rohlf talked about his knowledge of the people at Amherst.

11) Finally Ledgerwood read an article in the NY Times after the meeting where colleges are now going to be forced to do more to help the government be able to spy on Internet users and how colleges are resisting the cost of this new initiative as well as questioning its utility. Rich gave a very detailed response explaining why this is a very important issue. He told us that if the most draconian bill, the Communications A? Law Enforcement Act, is passed in Congress it would require SBU to replace all of its networking, all the way down to routers and switches and would have to spend millions of dollars. He told us that a lot of groups, including EDUCAUSE, are working very hard to defeat this measure.

After all of these items of old business, the committee will have to consider two items of new business at its next meeting.

The first item involves the library, privacy issues, and records purging. The second is the reinvigoration of the Provost's Task Force on Technology and whom we should nominate for that committee. One of its first topics will be classroom technology at all three campuses, here, Manhattan, and Southampton.

Respectfully submitted to the committee,

Mike Ledgerwood, Chair.

Attached item 1:

SUSB HIPAA Information and Communication Infrastructure Security and Privacy Policy

PURPOSE

The purpose of this policy is to establish direction, procedures, and requirements to ensure the appropriate protection of the Stony Brook University (herein after referred to as the University) information, and infrastructure systems as relates to Protected Health Information [PHI] and the HIPAA Regulations for Security (CFR 45 Parts 160,162 and 164, February 20, 2003) and Privacy Standards (45 CFR Parts 160 through 164, August 14, 2002).

This policy is intended to emphasize for University workforce members the necessity of PHI security and privacy in the various communication and information system environments and their role in maintaining security and privacy of same. The policy will also assign specific responsibilities for the provision of PHI data and PHI security and for the security of the various infrastructure environments. This policy is also intended to conform to federal, state and local regulations and statutes affecting the security and privacy of PHI.

SCOPE

This policy applies to all University workforce members, including employees, students, medical staff, trainees, volunteer staff, contractors, consultants and other representatives, including those affiliated with third parties who access University Computing Systems and University Computer Network Systems which contain PHI (herein after referred to as University workforce members). It applies equally to all computer systems, networking systems, physical medical records (including wireless), firewalls, servers, peripheral equipment, workstations, personal computers (desktop and portables), personal data assistants (PDA’s), including wireless PDA’s, within the University. Network and computer resources include PHI data, PHI printouts, PHI software (applications and databases), PHI hardware, facilities and telecommunications that permit access to PHI.

POLICY

It is the policy of the University to prohibit unauthorized access, disclosure, use, duplication, modification, diversion, destruction, storage, . loss, misuse, or theft of medical (hard copy or electronic) records, information, software or hardware as relates to PHI. Any such unauthorized activities or misuse will be cause for disciplinary action to be taken to the fullest extent of the law, in accordance with university policies and collective bargaining agreements when applicable.

POLICY CROSS-REFERENCE: University Policy 109R and related SUSB , SBUH, HSC and LISVH HIPAA policies.

DEFINITIONS

Access:

The ability of clinical and technical users with authorization and a need to know to access systems and medical records (in either physical and electronic format) which contain PHI or the ability of University workforce members that work in various areas to have contact with PHI.

RISK MANAGEMENT AND OVERSIGHT

The University will have in place a formal structure that will govern risk management and assessment of the University PHI data management structure. This structure will have oversight of the privacy and security (hard copy and electronic) of the University PHI and communication infrastructure environment that stores or transmits such information.

EMPLOYEE RESPONSIBILITY

Users:

Users are expected to follow all policies and procedures related to PHI security and privacy of medical record data in both physical and electronic format. University workforce members will comply with policies and procedures at the University (global) and departmental (local) levels for security of printing, copying and faxing PHI. This includes transmission, viewing and distributing PHI. University workforce members are expected to not only be aware of all existing security and privacy policies, but also to comply with all future policy changes as they arise. Only authenticated University workforce members will be given access to the communication infrastructure as relates to PHI in a capacity limited to meet the ability to perform their duties appropriately and with a need to know level of access only. All University workforce members who have been determined to no longer need access to the communication infrastructure or specific areas of the network and applications will be removed from access lists, including terminated employees, employees on extended leave, retired or transferred employees with new duties and responsibilities. All University workforce members with PHI access capabilities must attend HIPAA specific training sessions which will provide information on current policies, procedures and regulations relating to PHI security and privacy compliance.

Confidentiality:

The University, in accordance with Federal and State laws, is required to protect and preserve the confidentiality of PHI. All University workforce members must sign a Workforce & Electronic Information Confidentiality Acknowledgement Statement to be granted access honoring all the legal and ethical requirements for protecting and preserving the confidentiality and privacy of patients at the SUSB Infirmary, University Hospital and LISVH. This includes pre-employment and any subsequent additional requirements or changes in access to PHI either for hard copy or electronic format.

Administrators/Department Heads:

Administrators and Department Heads are responsible for ensuring that PHI data privacy and information security measures are being followed for their areas. They must maintain a current working knowledge of the University policies pertaining to PHI security and privacy and identify necessary process improvement changes when new policies are approved.

The Department Head is responsible for ensuring the PHI security and privacy of all department/agency data stored as either physical paper records or electronic records on departmental computer servers. Department Heads will work with the appropriate network and information security administration to ensure PHI security. The Department Head may assign responsibility to someone within the department/agency who will oversee the day-to-day implementation of the PHI security and privacy policies and procedures for their departments. Department Heads must ensure that all employees in their

area of responsibility are trained in the most current University policies and procedures as relates to PHI security and privacy. Department Heads will ensure that all employees under their supervision will have appropriate access to PHI and will review such on a regular basis.

The Information Security Officer:
The designated Information Security Officer of each University division is responsible for oversight and monitoring maintenance and compliance of the University PHI systems as outlined in the Health Insurance Portability and Accountability Act, Security Standards, Feb. 20, 2003, 45 CFR Part 164.308. (This position may be assigned at the University or at divisional levels.)

Privacy Officer:
The Privacy Officer of each University division is responsible for overseeing the development and implementation of policies, procedures and systems for protecting the privacy of protected (PHI) health information maintained by that University division or its business associates that has the potential to reveal the identity of patients as per HIPAA Privacy Standards (45 CFR Parts 160 through 164, August 14, 2002). (This position may be assigned at the University or at divisional levels.)

Security Committee:
A committee will be established to monitor the electronic security structure of the University, and interpret and implement changes in applicable regulations. To further the protection of the University PHI infrastructure, the committee will consist of not only the Information Security Officers but representatives from all local University divisions that have access or input capabilities to PHI, and any other relevant department(s). This committee will authorize appropriate audits and maintain records for compliance with this policy and SUSB, SBUH, HSC and LISVH policies that relate to PHI and the security of systems.

Privacy Committee:
A committee will be established to monitor HIPAA Privacy compliance and will interpret and implement changes in applicable regulations. The committee will also review new or revised health care laws, regulations and standards pertaining to the privacy of PHI, to determine whether the establishment of new policies and procedures or modification of existing policies and procedures are needed. To further the protection of PHI the committee will consist of representatives, as necessary, from all University divisions that have access or input capabilities to PHI, as well as other relevant department. The committee will review suspected violations and/or incidents on a case–by-case basis.

FUNCTIONAL REQUIREMENTS
Authentication:
The ability to authenticate the users of every University computer network and application that accesses PHI is required. No application or hardware that prevents authentication and identification of users on the University network infrastructure will be permitted. All users on the University computer network will be authenticated by a Human Resources personnel database, i.e., PeopleSoft and/or the Medical Staff Directory. Authentication will allow access to systems with PHI by role and on a need to know basis and will be verified by a

department director/manager. Access levels to systems with PHI will be managed by the appropriate System Administrator and an alternate.

Access:

Access is the ability of an authenticated user to access systems with PHI. Methods of access will be by a unique user name (alternate methods such as biometrics or tokens can be used) for identifying and tracking. All passwords words used by a user will consist of a minimum of eight alpha/numeric characters and will be changed on a regular basis, but not to exceed 120 days. System administrator passwords will be changed on a regular basis, but not to exceed 60 days.

Acceptable Use:

The PHI communication infrastructure and physical records are the property of the University and the governance of its use are restricted to further the legitimate interests of the University. Actions and activities that directly or indirectly threaten the integrity of the University PHI communication infrastructure, including circumvention of established security mechanisms, constitute a violation of this policy. Any violation of this acknowledgement or University policies and procedures is strictly prohibited and will be subject to disciplinary action and/or dismissal.

Physical/Technical Security:

Servers, networking equipment and other computers storing or transmitting University PHI data and physical records must be located in secured areas. Access is restricted to authorized personnel. PHI data will be backed up appropriately and tested to ensure the back up is an exact copy as per University policies. Any PHI that is on electronic or magnetic media will be controlled to prevent unauthorized access and will be destroyed in an appropriate manner as per University policies. Additional measures for the safeguarding of PHI, such as the development of individual system disaster recovery plans, firewalls, intrusion detection systems, virus and other intrusion scanning, use of UPS (Uninterruptible Power Supplies) and offsite storage of backups, will be implemented as required in the HIPAA Security regulations.

Authorization for Services on the Internet/Network:

The Communication Infrastructure Security Committee must approve all services that will be made available on the Internet. All servers connected to the University network system must be documented appropriately. Any unauthorized servers on the University network system will be disconnected and appropriate disciplinary action will be taken. The latest encryption technology will be utilized for all University network system communications by external vendor services, business associates/partners and individuals with access to PHI.

Training/Orientation:

All departments will provide appropriate staff training. The University will provide HIPAA training sessions, as needed, for all workforce members.

Updated Software:

Software used on the PHI communication infrastructure will be kept current through the use of the latest version(s) that have the most current updates, service packs or “patches”. New versions of software, especially operating systems, will not be supported by the University until a determination of the acceptability of the PHI

security of that software is determined. SUSB and SBUH Information Security Administration, together with the appropriate network/client support, will review all new applications that effect PHI. System administrators will maintain a record of the most current updates, service packs or “patches”.

Waste Disposal:
All departments must prevent the disposal and destruction of PHI that may directly or indirectly breach PHI confidentiality. Examples include unsecured disposal of hard copies of medical records, computer media, or documents containing network IP addresses, or usernames and passwords. Disposal of sensitive documentation and storage media will follow applicable University policy.

Verbal Security Breaches/Social Engineering:
All University workforce members who have access to the PHI network shall communicate sensitive information about the network only to appropriate personnel. Release of such information in any form to individuals not properly identified is a violation of this policy.

Minimum Necessary Standards:
All University workforce members are expected to limit their use and disclosures of PHI. Requests for PHI should be kept to the minimum amount of information necessary to perform their duties. Each department will implement policies and procedures, identifying the persons, or groups of persons within the department who will be permitted to access and use PHI to carry out their respective duties. Departmental policies should specify what categories of PHI each person or group may access and use and under what conditions. The determination should be consistent with individual job responsibilities. For example, individuals involved in treatment may be permitted to access the entire record as needed. As a guide for assigning access levels, the following factors should be considered:
1. Who may access the PHI?
2. Which types of PHI may be accessed?
3. In the record of which patients?
4. During what time period or for what activities?
There must be a specific justification for using or requesting the entire physical medical record or accessing the entire electronic medical record.

Public Viewing/Hearing
Many customary health care communications and practices play an important role in ensuring that patients receive prompt and effective health care. Due to the nature of these communications and practices, as well as the various environments in which patients receive health care services, the potential exists for PHI to be disclosed incidentally. For example, an Infirmary, Hospital or LISVH visitor may overhear a health care provider’s confidential conversation with another provider or patient. The Privacy Rule permits certain incidental uses and disclosures of PHI when the University has in place reasonable safeguards and minimum necessary policies and procedures to protect an individual’s privacy. Reasonable safeguards for University workforce members include:
· Speaking quietly or talking apart from others when discussing a patient’s condition with family members in semi-private patient rooms and waiting rooms;
· Isolating or locking file cabinets or records rooms;
· Isolating or screening from public view and access computer terminals, printers and fax machines containing PHI;

· Providing additional security, such as ID and passwords on computers maintaining PHI;
· Safeguarding PHI from inappropriate public viewing and hearing and refraining from discussing PHI in public areas, such as elevators or reception areas, unless doing so is necessary to providing treatment to patients; and
· Ensuring that confidential databases are exited upon leaving workstations so that PHI is not left on a computer screen where it may be viewed/accessed by individuals who are not authorized to see the information.

Incident Reporting:
All reports of incidents of HIPAA PHI violations will be reported to the appropriate SBU business unit Privacy Officer. Privacy violations will be appropriately reported up the chain of command. Electronic PHI Security violations will be reported to the appropriate SBU Information Security Administration unit for the University and University Police in accordance with policy. Warnings and reports of external PHI security threats will be monitored and distributed by each University division. All hardware will be handled in accordance with incident reporting and investigation policies. All PHI violations will be properly investigated and reported.

PENALTIES
The University will not tolerate the intentional or unintentional breach of PHI security. All violations will be penalized according to policy with respect to the type of violation. Any violation of this policy or other applicable University division policy or procedure is strictly prohibited and will be subject to disciplinary action and/or dismissal and could include additional penalties in accordance with federal, state and local laws.

Forms: Workforce & Electronic Information Confidentiality Acknowledgement Statement

Attached item 2:

USE OF INFORMATION TECHNOLOGY P 109

Issued by: Office of the President
Replaces: Policy 109, April 2001.
Approved:

Application. This policy applies to all users of any University network, communication system or computer resource. Guidelines adopted by a division or department to meet specific academic or administrative needs must comply with this policy and with policies on the use of University information technology resources established by the University Division of Information Technology and Hospital Information Technology Department.

Purpose. Information technology resources are provided by the University to support its education, research, public service and health care missions. Use of campus computing and network information resources is a privilege. Accordingly, all users of University networks and computer resources are responsible for the

proper use and protection of those resources.

Access / Usage.

Computer accounts and passwords are assigned to individual users for University-related purposes. Account access may not be shared.

Improper usage may include, but is not limited to: the misuse of or unauthorized access to network or electronic data in any form; the use of another's password or account; circumventing network security measures; the use of University data, networks or computer resources for private, commercial or political purposes; harassment or defamation; the unauthorized alteration of electronic files; disruption or interference (hacking / spam / viral programs); software license or copyright violations; violations of state or federal law.

To ensure the continued integrity of its information technology facilities and controls, the University may audit, inspect and/or monitor network usage, at any time, without notice.

The University may also restrict unlimited electronic access. If an imposed limitation interferes with a user's bona fide educational, research or health care activity, the user may direct a written request for a waiver to his or her Department Chair, who shall, on approval, forward the request to the appropriate administrative officer for review. The University reserves the right to limit the use of information technology resources based on institutional priorities, technical capacity and fiscal considerations.

Misuse of the University's information technology resources is subject to disciplinary and/or legal action.

Inquiries/Requests

Division of Information Technology
Office of the Chief Information Officer
Room 231, Educational Communications Center
(631) 632-9085

Information Technology Department (Hospital & Medical Center)
Office of the Chief Information Officer
L4-215 Health Sciences Center
(631) 444-2249

Related Policies

Division of Information Technology (link)
Information Technology Department (link)
NYS Office of Technology Policy 97-1
SUNY Administrative Procedures 007, 008
SBUH Policies 0038, 5007
SBU Policies 105, 507, 510, 512
SBU Student Conduct Code Article II A 6

Related Laws

17 USC § 101: Copyright Act
17 USC § 512: Digital Millennium Copyright Act (protects electronic text, graphic files, commercial software and audio and video files).

18 USC § 1030: Computer Fraud & Abuse Act (protects computer and data integrity)
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

NY Penal Code §§ 156, 170 (computer crimes; forgery)
NY Executive Law § 296 (Human Rights Law)
NY Public Officers Law §§ 84, 91 (FOIL, Personal Privacy)