

Information Sensitivity Policy

1.0 Purpose

The Information Sensitivity Policy is intended to help employees determine what information can be disclosed to non-employees, as well as the relative sensitivity of information that should not be disclosed outside of SUNY Stony Brook CS department without proper authorization.

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via any means. This includes: electronic information, information on paper, and information shared orally or visually (such as telephone and video conferencing).

All employees should familiarize themselves with the information labeling and handling guidelines that follow this introduction. It should be noted that the sensitivity level definitions were created as guidelines and to emphasize common sense steps that you can take to protect SUNY Stony Brook CS department Confidential information (e.g., SUNY Stony Brook CS department Confidential information should not be left unattended in conference rooms or in a printer room).

Please Note: The impact of these guidelines on daily activity should be minimal.

Questions about the proper classification of a specific piece of information should be addressed to your manager, group leader, lab manager or committee chairperson. Questions about these guidelines should be addressed to Director of Labs or Chairperson.

2.0 Scope

All SUNY Stony Brook CS department information is categorized into two main classifications:

- SUNY Stony Brook CS department Public
- SUNY Stony Brook CS department Confidential

SUNY Stony Brook CS department Public information is information that has been declared public knowledge by someone with the authority to do so, and can freely be given to anyone without any possible damage to SUNY Stony Brook CS department.

SUNY Stony Brook CS department Confidential contains all other information. It is a continuum, in that it is understood that some information is more sensitive than other information, and should be protected in a more secure manner. Included is information that should be protected very closely, such as trade secrets, development programs, potential job offerings, student grade and ID mappings, student social security numbers, disciplinary proceedings and other information integral to the success of our department. Also included in SUNY Stony Brook CS department Confidential is information that is less critical, such as department information, personnel information, etc., which does not require as stringent a degree of protection.

A subset of SUNY Stony Brook CS department Confidential information is "SUNY Stony Brook CS department Third Party Confidential" information. This is confidential information belonging or pertaining to another corporation which has been entrusted to SUNY Stony Brook CS department by that company under non-disclosure agreements and other contracts. Examples of this type of information include everything from joint development efforts to vendor lists, customer orders, and supplier information. Information in this category ranges from extremely sensitive to information about the fact that we've connected a supplier / vendor into SUNY Stony Brook CS department's network to support our operations.

SUNY Stony Brook CS department personnel are encouraged to use common sense judgment in securing SUNY Stony Brook CS department Confidential information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their manager

3.0 Policy

The Sensitivity Guidelines below provides details on how to protect information at varying sensitivity levels. Use these guidelines as a reference only, as SUNY Stony Brook CS department Confidential information in each column may necessitate more or less stringent measures of protection depending upon the circumstances and the nature of the SUNY Stony Brook CS department Confidential information in question.

3.1 Minimal Sensitivity: General department information; some personnel and technical information

Marking guidelines for information in hardcopy or electronic form.

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential".

Marking is at the discretion of the owner or custodian of the information. If marking is desired, the words "SUNY Stony Brook CS department Confidential" may be written or designated in a conspicuous place on or in the information in question. Other labels that may be used include "SUNY Stony Brook CS department Proprietary" or similar labels at the discretion of your individual committee or group. Even if no marking is present, SUNY Stony Brook CS department information is presumed to be "SUNY Stony Brook CS department Confidential" unless expressly determined to be SUNY Stony Brook CS department Public information by a SUNY Stony Brook CS department employee with authority to do so (e.g. Chairperson, committee chairperson, group leader, lab manager).

Access: SUNY Stony Brook CS department employees, contractors, people with a business need to know.

Distribution within SUNY Stony Brook CS department: Standard interoffice mail, approved electronic mail and electronic file transmission methods.

Distribution outside of SUNY Stony Brook CS department internal mail: U.S. mail and other public or private carriers, approved electronic mail and electronic file transmission methods.

Electronic distribution: No restrictions except that it be sent to only approved recipients.

Storage: Keep from view of unauthorized people; erase whiteboards, do not leave in view on tabletop. Machines should be administered with security in mind. Protect from loss; electronic information should have individual access controls where possible and appropriate.

Disposal/Destruction: Deposit outdated paper information in trash bins on SUNY Stony Brook CS department premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.

Penalty for deliberate or inadvertent disclosure: Not limited to loss of committee or group rights, loss of access to sensitive data.

3.2 More Sensitive: Business, financial, technical, and most personnel information

Marking guidelines for information in hardcopy or electronic form.

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential". As the sensitivity level of the information increases, you may, in addition or instead of marking the information "SUNY Stony Brook CS department Confidential" or "SUNY Stony Brook CS department Proprietary", wish to label the information "SUNY Stony Brook CS department Internal Use Only" or other similar labels at the discretion of your individual business unit or department to denote a more sensitive level of information. However, marking is discretionary at all times.

Access: SUNY Stony Brook CS department employees and non-employees with signed non-disclosure agreements who have a business need to know.

Distribution within SUNY Stony Brook CS department: Standard interoffice mail, approved electronic mail and electronic file transmission methods.

Distribution outside of SUNY Stony Brook CS department internal mail: Sent via U.S. mail or approved private carriers.

Electronic distribution: No restrictions to approved recipients within SUNY Stony Brook CS department, but should be encrypted or sent via a private link to approved recipients outside of SUNY Stony Brook CS department premises.

Storage: Individual access controls are highly recommended for electronic information.

Disposal/Destruction: Physically destroy hard copy and dispose of in trash bin on SUNY Stony Brook CS department premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.

Penalty for deliberate or inadvertent disclosure: Not limited to loss of committee or group access and possible personal lawsuit depending upon the data disclosed.

3.3 **Most Sensitive:** Trade secrets, operational, personnel, financial, source code, student grades, disciplinary information, student social security numbers & technical information integral to the security of our department

Marking guidelines for information in hardcopy or electronic form.

Note: any of these markings may be used with the additional annotation of "3rd Party Confidential". To indicate that SUNY Stony Brook CS department Confidential information is very sensitive, you may should label the information "SUNY Stony Brook CS department Internal: Registered and Restricted", "SUNY Stony Brook CS department Eyes Only", "SUNY Stony Brook CS department Confidential" or similar labels at the discretion of your individual business unit or department. Once again, this type of SUNY Stony Brook CS department Confidential information need not be marked, but users should be aware that this information is very sensitive and be protected as such.

Access: Only those individuals (SUNY Stony Brook CS department employees and non-employees) designated with approved access and/or signed non-disclosure agreements.

Distribution within SUNY Stony Brook CS department: Delivered direct - signature required, envelopes stamped confidential, or approved electronic file transmission methods.

Distribution outside of SUNY Stony Brook CS department internal mail: Delivered direct; signature required; approved private carriers.

Electronic distribution: No restrictions to approved recipients within SUNY Stony Brook CS department, but it is highly recommended that all information be strongly encrypted.

Storage: Individual access controls are very highly recommended for electronic information. Physical security is generally used, and information should be stored in a physically secured computer.

Disposal/Destruction: Strongly Encouraged: Physical destruction of hard copy and disposal in trash bin on SUNY Stony Brook CS department premises; electronic data should be expunged/cleared. Reliably erase or physically destroy media.

Penalty for deliberate or inadvertent disclosure: Up to and including termination, possible civil and/or criminal prosecution to the full extent of the law.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action.

5.0 Definitions

Terms and Definitions

Appropriate measures

To minimize risk to SUNY Stony Brook CS department from an outside business or other connection. SUNY Stony Brook CS department computer use by competitors and unauthorized personnel must be restricted so that, in the event of an attempt to access SUNY Stony Brook CS department information, the amount of information at risk is minimized.

Configuration of SUNY Stony Brook CS department-to-others connections

Connections shall be set up to allow other entities to see only what they need to see. This involves setting up both applications and network configurations to allow access to only what is necessary.

Delivered Direct; Signature Required

Do not leave in interoffice mail slot, call the mail room for special pick-up of mail.

Approved Electronic File Transmission Methods

Includes supported FTP clients and Web browsers.

Envelopes Stamped Confidential

You are not required to use a special envelope. Put your document(s) into an interoffice envelope, seal it, address it, and mark it confidential.

Approved Electronic Mail

Includes all mail systems supported by the IT Support Team. These include, but are not necessarily limited to, pine, mailtool, dtmail, mailx, emacs, netscape mail client.

Approved Encrypted email and files

Techniques include the use of DES and PGP. DES encryption is available via many different public domain packages on all platforms. See department faq on PGP use or systems staff.

Department Information System Resources

Department Information System Resources include, but are not limited to, all computers, their data and programs, as well as all paper information and any information at the Internal Use Only level and above.

Expunge

To reliably erase or expunge data on a PC or Mac you must use a separate program to overwrite data, supplied as a part of Norton Utilities. Otherwise, the PC or Mac's normal erasure routine keeps the data intact until overwritten. The same thing happens on UNIX machines, but data is much more difficult to retrieve on UNIX systems.

Individual Access Controls

Individual Access Controls are methods of electronically protecting files from being accessed by people other than those specifically designated by the owner. On UNIX machines, this is accomplished by careful use of the chmod command (use *man chmod* to find out more about it). On Mac's and PC's, this includes using passwords on screensavers, such as Disklock.

Insecure Internet Links

Insecure Internet Links are all network links that originate from a locale or travel over lines that are not totally under the control of SUNY Stony Brook CS department.

Encryption

Secure SUNY Stony Brook CS department Sensitive information in accordance with the *Acceptable Encryption Policy*. International issues regarding encryption are complex. Follow department guidelines on export controls on cryptography, and consult your manager, group leader, lab manager, committee chairperson or department chairperson and/or university legal services for further guidance.

Secure Password Authentication

Secure Password Authentication on Internet connections is accomplished by using ssh or sftp to connect to SUNY Stony Brook CS department's internal network over the Internet. Information and downloadable executables are available on the CS department web site.

Physical Security

Physical security means either having actual possession of a computer at all times, or locking the computer in an unusable state to an object that is immovable. Methods of accomplishing this include having a special key to unlock the computer so it can be used, thereby ensuring that the computer cannot be simply rebooted to get around the protection. If it is a laptop or other portable computer, never leave it alone in a conference

room, hotel room or on an airplane seat, etc. Make arrangements to lock the device in a hotel safe, or take it with you. In the office, use a lockdown cable. When leaving the office for the day, secure the laptop and any other sensitive material in a locked drawer or cabinet.

Private Link

A Private Link is an electronic communications path that SUNY Stony Brook CS department has control over its entire distance. For example, all SUNY Stony Brook CS department subnetworks are connected via private link. A computer with modem connected via a standard land line (not cell phone) to another computer have established a private link. ISDN lines to employee's homes is a private link. DSL, Satellite, wireless or cable modems are not private links.

6.0 Revision History