



# Acceptable Use Policy

---

## CS Department Acceptable Use Policy

### 1.0 Overview

The Computer Science department's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to SUNY Stony Brook CS department established culture of openness, trust and integrity. The Director of Labs is committed to protecting SUNY Stony Brook CS department's faculty, students and staff from illegal or damaging actions by individuals, either knowingly or unknowingly. Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of SUNY Stony Brook CS department. These systems are to be used for the research and educational purposes of the department, and of our students in the course of normal operations. Effective security is a team effort involving the participation and support of every SUNY Stony Brook CS department employee and student who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

### 2.0 Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at SUNY Stony Brook CS department. These rules are in place to protect the users and SUNY Stony Brook CS department. Inappropriate use exposes SUNY Stony Brook CS department to risks including virus attacks, compromise of network systems and services, and legal issues.

### 3.0 Scope

This policy applies to employees, contractors, consultants, students, and other workers at SUNY Stony Brook CS department, including all personnel affiliated with third parties. This policy applies to all equipment that is owned by, leased to, on loan to SUNY Stony Brook CS department or connected to any network controlled by or the responsibility of SUNY Stony Brook CS department and any accounts issued by the CS department or any lab therein.

### 4.0 Policy

#### 4.1 General Use and Ownership

1. While SUNY Stony Brook CS department's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the department systems remains the property of SUNY Stony Brook CS department. Because of the need to protect SUNY Stony Brook CS department's network, management cannot guarantee the confidentiality of information stored on any network device belonging to SUNY Stony Brook CS department.

2. Users are responsible for exercising good judgment regarding the reasonableness of personal use.

3. Research labs are responsible for creating guidelines concerning personal use of their Internet/Intranet/Extranet systems. In the absence of such policies, users should be guided by departmental policies on personal use, and if there is any uncertainty, users should consult their advisor, professor or CS department Systems Staff.

4. DOL recommends that any information that users consider sensitive or vulnerable be encrypted. For guidelines on information classification, see the CS department's Information Sensitivity Policy. For guidelines on encrypting email and documents, go to the CS department's Awareness Initiative.

5. For security and network maintenance purposes, authorized individuals within SUNY Stony Brook CS department may monitor equipment, systems and network traffic at any time, per DOL's Audit Policy.
6. SUNY Stony Brook CS department reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

#### **4.2 Security and Proprietary Information**

1. Means should be made to classify data as either confidential or not confidential, as defined by confidentiality guidelines of the local controlling authority of the data. Examples of confidential information include but are not limited to: faculty/staff/student private data, research strategies, competitor sensitive, trade secrets, specifications, customer lists, and research data. Users should take all necessary steps to prevent unauthorized access to this information.
2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. Users are responsible for the activities of their account whether they are personally executing the activity or not. System level passwords should be changed every six months, user level passwords should be changed every nine months. Users must also conform to the CS department *Password Policy*.
3. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off (control-alt-delete for Win2K users) when the host will be unattended.
4. Use encryption of information in compliance with the CS department's Acceptable Encryption Use policy.
5. Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with the "Laptop Security Tips".
6. Postings by users from a SUNY Stony Brook CS department email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of SUNY Stony Brook CS department, unless posting is in the course of CS departmental business duties.
7. All hosts used by a user that are connected to the SUNY Stony Brook CS department Internet/Intranet/Extranet, whether owned by the user or SUNY Stony Brook CS department, shall be continually executing approved virus-scanning software with a current virus database. Unless overridden by departmental or the research lab policy in which the system is operating.
8. Users must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.
9. Users are responsible to report loss or compromise of their accounts to the local administrators immediately upon suspicion of the account being compromised. Users must fully cooperate in investigation efforts.

#### **4.3. Unacceptable Use**

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services). Under no circumstances is an employee or user of SUNY Stony Brook CS department authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing SUNY Stony Brook CS department-owned resources or CS department accounts. The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

## **System and Network Activities**

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by SUNY Stony Brook CS department.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which SUNY Stony Brook CS department or the end user does not have an active license is strictly prohibited.
3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.), unless this activity is a part of the user's normal job/duty and occurs within a research lab as part of an authorized procedure within that lab.
5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
6. Using a SUNY Stony Brook CS department computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
7. Making fraudulent offers of products, items, or services originating from any SUNY Stony Brook CS department account.
8. Providing unauthorized access to research data, executable code, source code, research results or partial results.
9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes. The sole exceptions to this rule are when the activity is limited to within a research lab AND authorized by the lab controlling authority or when the DOL has given prior approval for the activity outside of a given research lab.
10. Port scanning or security scanning outside a given research lab is expressly prohibited unless prior notification to DOL is made and approval received from DOL.
11. Executing any form of network monitoring which will intercept data not intended for the user's host, unless this activity is a part of the user's normal job/duty or occurs within a research lab as part of an authorized procedure within that lab.
12. Circumventing user authentication or security of any host, network or account, unless this activity is a part of the user's normal job/duty or occurs within a research lab as part of an authorized procedure within that lab.
13. Interfering with or denying service to any user other than the user's host (for example, denial of service attack), unless this activity is a part of the user's normal job/duty or occurs within a research lab as part of an authorized procedure within that lab.

14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
15. Providing information about, or lists of, SUNY Stony Brook CS department employees or users to parties outside SUNY Stony Brook.

### **Email and Communications Activities**

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within SUNY Stony Brook CS department's networks or other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by SUNY Stony Brook CS department or connected via SUNY Stony Brook CS department's network.
7. Posting the same or similar non-CS department business-related messages to large numbers of Usenet newsgroups (Newsgroup spam), mail lists or mail aliases (spam).

### **5.0 Enforcement**

Any user found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or expelling students from the university. DOL reserves the right to disconnect any host or network to prevent unauthorized activity.

### **6.0 Definitions**

#### **Term Definition**

*Business*

*Business-related* The "business" of the Computer Science department is education of Computer Science and Information Systems students and research in Computer Science or Information systems.

*DOL* Director of Labs

*Spam* Unauthorized and/or unsolicited electronic mass mailings.

*User(s)* Any person authorized to use department facilities (faculty, staff, students, guests, researchers)