Departmental IA security policy
SCIS (ARNe) Acceptable Use Policy (adapted from SAN.org)

1.0 Overview
ARNeSec's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to SCIS’s established culture of openness, trust and integrity. ARNeSec is committed to protecting SCIS’s students, partners and the University 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 SCIS. These systems are to be used for University purposes in serving the interests of the University, and of our students in the course of normal operations. Please review Regis/SPS student policies manual for further details.

Effective security is a team effort involving the participation and support of every SCIS student and affiliate 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 SCIS. These rules are in place to protect the student and SCIS. Inappropriate use exposes SCIS to risks including virus attacks, compromise of network systems and services, and legal issues.

3.0 Scope
This policy applies to students, contractors, consultants, temporaries, and other workers at SCIS, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by SCIS.

4.0 Policy
4.1 General Use and Ownership
1. While SCIS's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the University systems remains the property of SCIS. Because of the need to protect SCIS's network, management cannot guarantee the confidentiality of information stored on any network device belonging to SCIS.

2. Students are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, students should be guided by departmental policies on personal use, and if there is any uncertainty, students should consult their faculty member.

3. ARNeSec recommends that any information that users consider sensitive or vulnerable be encrypted. For guidelines on information classification, see
ARNeSec's Information Sensitivity Policy. For guidelines on encrypting email and documents, go to Acceptable Encryption Use policy.

4. For security and network maintenance purposes, authorized individuals within SCIS may monitor equipment, systems and network traffic at any time, per ARNeSec’s Audit Policy.

5. SCIS 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. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential, as defined by corporate confidentiality guidelines, details of which can be found in student policies manual. Examples of confidential information include but are not limited to: University private, marketing strategies, competitor sensitive information, trade secrets, specifications, customer lists, and research data. Students should take all necessary steps to prevent unauthorized access to this information and respect the confidentiality of University Intellectual Property.

2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed during each practicum, user level passwords should be changed every six months (A and B terms).

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 ARNeSec'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. All hosts used by the student that are connected to the SCIS Internet/Intranet/Extranet, whether owned by the student or SCIS, shall be continually executing approved virus-scanning software with a current virus database. Unless overridden by departmental or group policy.

7. Students must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

4.3. Unacceptable Use

The following activities are, in general, prohibited. Students 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 a student of SCIS authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing SCIS-owned resources.
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 University 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 SCIS.
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 SCIS 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.).
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 SCIS 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 SCIS account.
8. Making statements about warranty, expressly or implied, unless it is a part of normal student practicum duties.
9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the student is not an intended recipient or logging into a server or account that the student 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.
10. Port scanning or security scanning is expressly prohibited unless prior notification to ARNeSec is made.
11. Executing any form of network monitoring which will intercept data not intended for the student's host, unless this activity is a part of the student's normal job/duty.
12. Circumventing user authentication or security of any host, network or account.
13. Interfering with or denying service to any user other than the student's host.
(for example, denial of service attack).
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, SCIS students to parties outside SCIS.

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 SCIS's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by SCIS or connected via SCIS's network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

5.0 Enforcement
Any student found to have violated this policy may be subject to disciplinary action, up to and including the terms set forth in the student policy manual.

6.0 Definitions
Term Definition
Spam Unauthorized and/or unsolicited electronic mass mailings.

7.0 Revision History
version 1.0 9/2/2005
version 2.0 11/30/2005

8.0 Reference
http://www.sans.org/resources/policies/#template