

SCSU Security Policy Document

DRAFT

Southern Connecticut State University

501 Crescent Street
New Haven, Connecticut 06515
(203) 392- SCSU

Southern Connecticut State University - For Internal Use Only

Southern Connecticut State University

SCSU Security Policy Document

INTRODUCTION	2
ACCEPTABLE USE POLICY.....	3
OVERVIEW	3
PURPOSE	3
SCOPE.....	3
POLICY	4
<i>System and Network Activities</i>	5
EMAIL AND COMMUNICATIONS ACTIVITIES.....	7
ANTI-VIRUS POLICY.....	8
IDENTITY POLICY.....	8
PASSWORD POLICY	10
ENCRYPTION POLICY.....	14
REMOTE ACCESS POLICY	15
VIRTUAL PRIVATE NETWORK (VPN) POLICY	18
EXTRANET POLICY	20

Introduction

More and more high profile information security events have garnered media attention in recent years. As a result, those responsible for protecting their organization's critical assets have increasingly realized the need for greater attention to the security imperatives faced in doing business in an information-based economy.

However, for too many people in such positions of responsibility, cognizance of prevailing threats and the will or means to act on them remains inconsistent with the increased risks involved in internet, intranet and extranet endeavors. And what money and energy is being allocated tends to be disproportionately focused on the external threat -- based to a tremendous degree on the media focus on hacking incidents -- rather than looking at an inside-out approach as the most effective route to a secure information infrastructure.

Information Security efforts take many forms and have become increasingly daunting to both IT managers and system administrators as both internal and external connectivity challenges become more complex.

Being more aware of and paying more attention to the following key elements of internal security will protect your information assets against the majority and most common security threats and will allow you to head off a significant portion of the consequential damage to your core business interests.

Acceptable Use Policy

Overview

The Acceptable Use Policy is not intended to impose restrictions that are contrary to Southern Connecticut State University policies, but rather to establish a culture of trust and integrity. Southern Connecticut State University is committed to protecting its Faculty, Staff, Students, and the university from illegal or damaging actions by individuals, whether committed 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, Web browsing, and FTP, are the property of Southern Connecticut State University. You are expected to use these systems for business purposes in the interests of the university, our clients, and our customers in the course of normal operations. Please review Human Resources policies for further details.

http://www.southernct.edu/faculty/hr/legal_tec.html

Effective security is a team effort involving the participation and support of every Southern Connecticut State University employee and affiliate who deals with information and/or information systems. It is your responsibility as a computer user to know these guidelines, and to act accordingly.

Purpose

This policy outlines the acceptable use of computer equipment at Southern Connecticut State University. These rules protect you and Southern Connecticut State University. Inappropriate use exposes Southern Connecticut State University to risks including virus attacks, compromise of network systems and services, and legal issues.

Scope

This policy applies to employees, contractors, consultants, temporaries, students, and other workers at Southern Connecticut State University, including all personnel affiliated with third parties. This policy applies to all

equipment that is owned or leased by Southern Connecticut State University.

Policy

General Use and Ownership

1. While Southern Connecticut State University's network administration desires to provide a reasonable level of privacy, you should be aware that the data you create on university systems remains the property of Southern Connecticut State University. Because of the need to protect Southern Connecticut State University's network, management does guarantee the confidentiality of information stored on any network device belonging to Southern Connecticut State University.
2. You 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, you should follow departmental policies on personal use, and, if there is any uncertainty, consult your supervisor or manager.
3. Southern Connecticut State University recommends encrypting any information that you consider sensitive or vulnerable. For guidelines on information classification, see [the Information Sensitivity Policy](#). For guidelines on encrypting email and documents, [see the Awareness Initiative](#).
4. For security and network maintenance purposes, authorized individuals within Southern Connecticut State University may monitor equipment, systems and network traffic at any time, per the [Audit Policy](#).
5. Southern Connecticut State University reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Security and Proprietary Information

1. The user interface for information contained on Internet/intranet/extranet-related systems should be classified as either confidential or non-confidential, as defined by [university confidentiality guidelines found in Human Resources policies](#). Examples of confidential information include, but are not limited to: [university private, system strategies, competitor sensitive, trade secrets, specifications, customer lists, and research data](#). You should take all necessary steps to prevent unauthorized access to this information.
2. Keep passwords secure and do not share accounts. As an authorized user, you are responsible for the security of your

- passwords and accounts. Change system level passwords quarterly; change user level passwords every six months.
3. Secure all PCs, laptops and workstations with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off (Ctrl-Alt-Delete for Windows XP users) when the host will be unattended.
 4. Use encryption of information in compliance with the Acceptable Encryption Use policy.
 5. Because information contained on portable computers is especially vulnerable, exercise special care. Protect laptops in accordance with "Laptop Security Tips."
 6. Newsgroup postings from a Southern Connecticut State University email address should contain a disclaimer stating that the opinions expressed are strictly your own and not necessarily those of Southern Connecticut State University, unless posting is in the course of business duties.
 7. All hosts used by you that are connected to the Southern Connecticut State University Internet/intranet/extranet, whether owned by you or by Southern Connecticut State University, must continually execute approved virus-scanning software with a current virus database (unless overridden by departmental or group policy).
 8. Use extreme caution when opening email attachments received from unknown senders. These attachments may contain viruses, email bombs, or Trojan horse code.

Unacceptable Use

The following activities are, in general, prohibited. In special cases, you may be exempted from these restrictions during the course of your legitimate job responsibilities (for example, systems administration staff may need to disable the network access of a host that is disrupting production services).

Under no circumstances is an employee of Southern Connecticut State University authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Southern Connecticut State University-owned resources.

The lists that follow are by no means exhaustive, but provide a framework for activities that 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 Southern Connecticut State University.
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 Southern Connecticut State University or the end user does not have an active license.
 3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws. Consult appropriate management prior to export of any material that is in question.
 4. Introducing malicious programs into the network or server (e.g., viruses, worms, Trojan horses, email 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 working at home.
 6. Using a Southern Connecticut State University computing asset to procure or transmit 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 Southern Connecticut State University account.
 8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
 9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which you are not an intended recipient or logging into a server or account that you are not expressly authorized to access, unless these duties are within the scope of regular duties. "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, **unless you previously notify Southern Connecticut State University.**
 11. Executing any form of network monitoring that will intercept data not intended for your host, unless this activity is a part of your normal duties.
 12. Circumventing user authentication or security of any host, network, or account.
 13. Interfering with, or denying service to, any user other than your host (for example, a 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, Southern Connecticut State University employees to parties outside Southern Connecticut State University.

Email and Communications Activities

Purpose

The policy defines standards for conducting communications within Southern Connecticut State University's network email system. These standards minimize the potential exposure to Southern Connecticut State University from unsolicited email messages and attachments. Damages include the loss of sensitive or university confidential data or intellectual property, damage to public image, damage to critical Southern Connecticut State University internal systems, and unintentional employee exposure to inappropriate content or material.

1. Sending unsolicited email messages, including sending "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. Soliciting email for any other email address, other than that of the poster's account, with the intent to harass or collect replies.
5. Creating or forwarding "chain letters" or "Ponzi" or other "pyramid" schemes of any type.
6. Using unsolicited email originating from within Southern Connecticut State University's networks or other Internet/intranet/extranet service providers on behalf of, or to advertise, any service hosted by Southern Connecticut State University or connected via Southern Connecticut State University's network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

Enforcement

Any employee violating this policy may be subject to disciplinary action, up to and including termination of employment.

Definitions

Term	Definition
Spam	Unauthorized and/or unsolicited electronic mass mailings

Anti-Virus Policy

Purpose

The policy defines standards for protecting Southern Connecticut State University's network from any threat related to Virus, Worm or Trojan Horse. These standards minimize the potential exposure to Southern Connecticut State University from damages that may result from an unprotected network. Damages may include the loss of sensitive or university confidential data or intellectual property, damage to public image, damage to critical Southern Connecticut State University internal systems, etc.

1. Always run the Southern Connecticut State University standard, supported anti-virus software available from the Southern Connecticut State University download site. Download and run the current version; download and install anti-virus software updates as they become available.
2. Never open any files or macros attached to an email from an unknown, suspicious, or un-trusted source. Delete these attachments immediately, then "double delete" them by emptying your trash.
3. Delete spam, chain, and other junk email without forwarding, per Southern Connecticut State University's Acceptable Use Policy.
4. Never download files from unknown or suspicious sources.
5. Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.
6. Always scan a floppy diskette from an unknown source for viruses before using it.
7. Back up critical data and system configurations regularly and store the data in a safe place.
8. If lab testing conflicts with anti-virus software, run the anti-virus utility to ensure a clean machine, disable the software, and then run the lab test. After the lab test, enable the anti-virus software. When the anti-virus software is disabled, do not run any applications that could transfer a virus, e.g., email or file sharing.
9. New viruses are discovered almost every day. Periodically check the university Anti-Virus Policy and this Recommended Processes list for updates.

Identity Policy

Purpose

The policy defines rules and practices for protecting Southern Connecticut State University's network from unauthorized access. These practices help reduce the potential for identity information getting into the wrong hands. Damages may include the loss of sensitive or university

confidential data or intellectual property, damage to public image, damage to critical Southern Connecticut State University internal systems, etc.

Train Your Employees

One of the most important and often overlooked elements of a successful information security program is having employees trained to a higher degree of security awareness. Employees should be trained to appreciate the importance of data that they handle daily and not be lulled into a sense of ambivalence based on the routine of working with such information. Formal information security awareness training should be provided that reinforces the need to keep all information on your university's information assets confidential -- even data that appears the most innocuous. Workers should be further trained to not reveal this information until the requesting party is identified and their need to know authenticated.

An important follow-up measure is to have written information security policy that explains the university's security philosophy and the business rationale behind it. This policy should be imparted to all new employees as a part of new-hire orientation.

How can having security savvy employees help protect your organization? Many hackers make ample use of "social engineering" skills in which they attempt to convince employees that they have a legitimate right to obtain and know information about your university. For example, a clever intruder may call your information services department claiming to be an outside vendor and simply ask for the name of your systems and what operating system they are running. He may follow up by asking for the names of key employees at your university. Armed with that basic information, this unwelcome visitor now knows how to identify your systems, what operating system holes they may be able to exploit and what potential user IDs they can try to use to access those systems.

Watch Your Visitors

Temporary workers, contractors and consultants represent a unique security threat in that they are generally not subject to the same scrutiny as a firm's full-time employees but may be granted the same high levels of system access. In addition, they will sometimes know the applications and operating systems running on your network better than your own employees will.

Watch these ad-hoc employees closely until you are familiar with their qualifications, the caliber of their work and, most importantly, the degree of trust that it is safe to allow.

Though usually honest and competent, these outside resources must be monitored closely to ensure that their work is sound and that they are truly

working in your university's interest. Vendors, for example, will sometimes leave behind trap doors into your systems with the purest intentions of using them only to protect you from yourself or to make future modifications or updates -- guard against this and make it expressly known that these mechanisms will not be tolerated.

Policy

1. Workstations must be logged off to a point that requires a new logon whenever employees leave their work area.
2. Any employee who does not access an administrative system in a six months time period will have his/her access removed and must be reauthorized for access.
3. Sharing of IDs is prohibited.
4. **Access managers** will (immediately) delete the access of employees who have terminated the institution and will modify the access of ones who transfer to (remove capabilities dependent on the previous position).
5. Computer installations running administrative applications will, where possible, provide a mechanism that records and logs off a user ID after a specified period of time of inactivity; they will also provide a mechanism that locks a user logon ID after multiple unsuccessful attempts to log on.

Password Policy

Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Southern Connecticut State University's entire system network. As such, all Southern Connecticut State University employees (including contractors and vendors with access to Southern Connecticut State University systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Purpose

The purpose of this policy is to establish a standard for creating strong passwords, protecting those passwords, and change frequency.

Scope

This policy applies to all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Southern Connecticut State University

facility, has access to the Southern Connecticut State University network, or stores any non-public Southern Connecticut State University information.

Policy

1. Change all system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) **at least quarterly.**
2. Make all production system-level passwords part of the Southern Connecticut State University **administered global password management database.**
3. Change all user-level passwords (e.g., email, Web, desktop computer, etc.) at least every six months. The recommended change **interval is every four months.**
4. User accounts that have system-level privileges granted through group memberships or programs such as “sudo” must have a unique password from all other accounts held by that user.
5. Do not insert passwords into email messages or other forms of electronic communication.
6. Where using SNMP, define community strings as something other than the standard defaults of “public,” “private,” and “system” and make them different from the passwords used to log in interactively. Use a keyed hash where available (e.g., SNMPv2).
7. All user-level and system-level passwords must conform to the guidelines below.

Guidelines

General Password Construction Guidelines

Southern Connecticut State University uses passwords for various purposes. Some of the more common uses include: user-level accounts, Web accounts, email accounts, screen saver protection, voicemail passwords, and local router logins. Since very few systems have support for one-time tokens (i.e., dynamic passwords that are only used once), everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

1. They contain less than eight characters.
2. They are a word found in a dictionary (English or foreign).
3. They are a common usage word such as
4. Names of family, pets, friends, co-workers, fantasy characters, etc.
5. Computer terms and names, commands, sites, companies, hardware, software.
6. The words “Southern Connecticut State University,” and geographical indicators such as “sanjose,” “sanfran” or any derivation.
7. Birthdays and other personal information such as addresses and phone numbers.

8. Word or number patterns such as aaabbb, qwerty, zyxwvuts, 123321, etc.
9. Any of the above spelled backwards.
10. Any of the above preceded or followed by a digit (e.g., secret1, 1secret).

Strong passwords:

1. Contain both upper and lower case characters (e.g., a-z, A-Z).
2. Include digits and punctuation characters as well as letters, e.g., 0-9, !@#\$%^&*() +|~-=\{}|:~<>?.,/).
3. Are at least eight alphanumeric characters long.
4. Are not a word in any language, slang, dialect, jargon, etc.
5. Are not based on personal information, names of family, etc.
6. Are never written down or stored on-line.

Create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some variation.

NOTE: Do not use either of the preceding examples as passwords!

Password Protection Standards

1. Do not use the same password for Southern Connecticut State University accounts as for other non-Southern Connecticut State University access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, do not use the same password for various Southern Connecticut State University access needs. For example, select one password for engineering systems and a separate password for IT systems. Also, select a separate password for an NT account and a UNIX account.
2. Do not share Southern Connecticut State University passwords with anyone, not even your secretary or departmental administrative assistant. All passwords are sensitive, confidential Southern Connecticut State University information.
3. Here is a list of "don'ts":
4. Don't reveal a password to anyone over the phone.
5. Don't reveal a password in an email message.
6. Don't reveal a password to the boss.
7. Don't talk about a password in front of others.
8. Don't hint at the format of a password (e.g., "my family name").
9. Don't reveal a password on questionnaires or security forms.
10. Don't share a password with family members.
11. Don't reveal a password to a co-worker when you go on vacation.
12. Don't write down a password and store it anywhere in your office.

13. Don't store passwords in a file on any computer, including a handheld computer, without encryption.
14. Don't use the "Remember Password" feature of an application such as Eudora, Outlook, or Netscape Messenger.

If someone demands a password, refer them to this document or have them call the **Information Security Department**.

If you suspect an account or password has been compromised, report the incident to Southern Connecticut State **University Information Systems department** and change all passwords.

Southern Connecticut State University or its delegates may perform password cracking or guessing on a periodic or random basis. If a password is guessed or cracked during one of these scans, the user is required to change it.

Application Development Standards

Application developers must ensure that their programs contain the following security precautions:

1. Applications should support authentication of individual users, not groups.
2. Applications should not store passwords in clear text or in any easily reversible form.
3. Applications should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.
4. Applications should support TACACS+ , RADIUS, and/or X.509 with LDAP security retrieval wherever possible.

Use of Passwords and Passphrases for Remote Access Users

Control remote access to Southern Connecticut State University networks using either a one-time password authentication or a public/private key system with a strong passphrase.

Passphrases

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, which is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access. A passphrase typically consists of multiple words, making it more secure against "dictionary attacks." A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. Here is an example of a good passphrase:

"The*?#>*@TrafficOnThe101Was*&#!#ThisMorning"

All of the guidelines for creating strong passwords also apply to passphrases.

Enforcement

Any employee found violating this policy may be subject to disciplinary action, up to and including termination of employment.

Definitions

Term	Definition
Application Administration Account	Any account that is for the administration of an application (e.g., Oracle database administrator, ISSU administrator)

Encryption Policy

Purpose

This policy provides guidance so that encryption efforts will use only those algorithms that have received substantial public review and have proven to work effectively. The policy also provides direction to ensure that federal regulations are followed regarding the dissemination and use of encryption technologies outside of the United States.

Scope

This policy applies to all Southern Connecticut State University employees and affiliates.

Policy

Use proven, standard algorithms such as DES, Blowfish, RSA, RC5, AES, and IDEA as the basis for encryption technologies. These algorithms represent the actual cipher used for an approved application. For example, Network Associate's Pretty Good Privacy (PGP) uses a combination of IDEA and RSA or Diffie-Hillman, while Secure Socket Layer (SSL) uses RSA encryption. Symmetric cryptosystem key lengths must be at least 56 bits. Asymmetric cryptosystem keys must be of a length that yields equivalent strength. Southern Connecticut State University's key length requirements will be reviewed annually and upgraded as technology allows.

Using proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by Southern Connecticut State University. Be aware that the export of encryption technologies is restricted by the U.S. Government. Residents of countries other than the United States should learn the encryption technology laws of their countries.

Enforcement

Any employee violating this policy may be subject to disciplinary action, up to and including termination of employment.

Definitions

Term	Definition
Proprietary Encryption	An algorithm that has not been made public and/or has not withstood public scrutiny. The developer of the algorithm could be a vendor, an individual, or the government
Symmetric Cryptosystem	A method of encryption in which the same key is used for both encryption and decryption of the data
Asymmetric Cryptosystem	A method of encryption that uses two different keys: one for encrypting and one for decrypting the data (e.g., public-key encryption)

Remote Access Policy

Purpose

The policy defines standards for connecting to Southern Connecticut State University's network from any host. These standards minimize the potential exposure to Southern Connecticut State University from damages that may result from unauthorized use of its resources. Damages include the loss of sensitive or university confidential data or intellectual property, damage to public image, damage to critical Southern Connecticut State University internal systems, etc.

Scope

This policy applies to all Southern Connecticut State University employees, contractors, vendors, students and agents with a Southern Connecticut State University owned or personally owned computer or workstation connecting to the Southern Connecticut State University network. This policy applies to remote access connections to Southern Connecticut State University, including reading or sending email and viewing intranet resources.

This policy covers remote access implementations that include, but are not limited to, dialup modems, Frame Relay, ISDN, DSL, VPN, SSH, Wireless Access Points and cable modems, etc.

Rogue Modems and Wireless Access Points

The best firewall on the market won't protect you if you maintain scores of unprotected modems and wireless access points open to the outside world within the confines of your office. With what they believe to be the best of intentions, workers will sometimes hook up unauthorized modems to their workstations to avoid your officially sanctioned dial-in mechanism and make it easier for them to access their desktop data. IT employees who should be familiar with the dangers of such configurations will often plant a modem (with a publicly accessible incoming phone line attached) on a server to allow for access by an outside vendor. Whatever the cause of these unauthorized access mechanisms, it is imperative that organizations carefully control the extent to which modems are used to allow for remote access to your systems. All external access to networks, systems and data should be done through a centrally administered, tested and sanctioned remote access solution. Policy should exist that prohibits

the establishment of any unauthorized inroads to your systems and any discovered mechanisms of this sort should be removed immediately.

Policy

1. It is the responsibility of Southern Connecticut State University employees, contractors, vendors, students and agents with remote access privileges to Southern Connecticut State University's system network to ensure that their remote access connection is given the same consideration as their on-site connection to Southern Connecticut State University.
2. General access to the Internet for recreational use by immediate household members through the Southern Connecticut State University network on personal computers **is permitted for employees who have flat-rate services**. You are responsible to ensure that family members do not violate any Southern Connecticut State University policies, perform illegal activities, or use the access for outside business interests. You bears responsibility for the consequences should the access be misused.
3. Please review the following policies for details of protecting information when accessing the system network remotely, and acceptable use of Southern Connecticut State University's network:
 - a. Encryption Policy
 - b. Virtual Private Network (VPN) Policy
 - c. Wireless Communications Policy
 - d. Acceptable Use Policy
4. For additional information regarding Southern Connecticut State University's remote access connection options, including how to order or disconnect service, cost comparisons, troubleshooting, etc., refer to the Network Telecom Services Website.
<http://nts.southernct.edu/>

Requirements

1. Southern Connecticut State University strictly controls secure remote access to Southern Connecticut State University networks. Southern Connecticut State University enforces control via **one-time password authentication or public/private keys with strong passphrases**. For information on creating a strong passphrase see the Password Policy.
2. Never provide a login or email password to anyone, not even family members.
3. You must ensure that your Southern Connecticut State University-owned or personal computer or workstation, which is remotely connected to Southern Connecticut State University's system network, is not connected to any other network at the same time,

with the exception of personal networks that are under your complete control.

4. Do not use non-Southern Connecticut State University email accounts (e.g., Hotmail, Yahoo, AOL), or other external resources to conduct Southern Connecticut State University business. This will help ensure that official business is never confused with personal business.
5. Routers for dedicated ISDN lines configured for access to the Southern Connecticut State University network must meet minimum authentication requirements of CHAP.
6. Reconfiguring your home equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
7. Frame Relay links must meet minimum authentication requirements of DLCI standards.
8. Non-standard hardware configurations must be approved by Remote Access Services, and Southern Connecticut State University must approve security configurations for access to hardware.
9. All hosts remotely connected to Southern Connecticut State University internal networks, including PCs, must use the most up-to-date anti-virus software (place URL to system software site here). Third-party connections must comply with requirements stated in the Third Party Agreement.
10. Any personal equipment that you use to connect to Southern Connecticut State University's networks must meet the requirements of Southern Connecticut State University-owned remote access equipment.
11. Organizations or individuals who wish to implement non-standard remote access solutions to the Southern Connecticut State University production network must obtain prior approval from Network Telecom Services and Southern Connecticut State University.

Enforcement

Any employee violating this policy may be subject to disciplinary action, up to and including termination of employment.

Definitions

Term	Definition
Cable Modem	Cable companies provide Internet access in their service areas over cable TV coaxial cable. A cable modem accepts this coaxial cable and can receive data from the Internet at over 1.5 Mbps.
CHAP	Challenge Handshake Authentication Protocol is an authentication method that uses a one-way hashing function.
DLCI	Data Link Connection Identifier is a unique number assigned to a Permanent Virtual Circuit (PVC) endpoint in a Frame Relay network.
Dialup Modem	A peripheral device that connects computers to each other for sending communications via the telephone lines. The modem modulates digital data into

	analog signals for transmission, and then demodulates the signals back into digital format to be read by the receiving computer.
Dual Homing	Having concurrent connectivity to more than one network from a computer or network device. Examples include: Being logged into the system network via a local Ethernet connection, and dialing into AOL or another Internet service provider (ISP). Being on a Southern Connecticut State University-provided remote access home network, and connecting to another network, such as a spouse's remote access. Configuring an ISDN router to dial into Southern Connecticut State University and an ISP, depending on packet destination.
Frame Relay	A method of communication offered by telephone companies that features a flat-rate billing structure and a variety of transmission speeds.
ISDN	Integrated Services Digital Network service comes in two types. Basic Rate Interface (BRI) is used for home office/remote access. Primary Rate Interface (PRI) is more often used for system Internet connectivity.
Remote Access	Any access to a private network through a non-private network, device, or medium.
Split-tunneling	Simultaneous direct access to another network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while remotely connected to a system network via a VPN tunnel.
VPN	Virtual private networking enables secure private network via a public network such as the Internet using "tunneling" technology.
DSL	Digital Subscriber Line is a broadband Internet access technology that works over standard phone lines.

Virtual Private Network (VPN) Policy

Purpose

The purpose of this policy is to provide guidelines for Remote Access IPsec or L2TP Virtual Private Network (VPN) connections to the Southern Connecticut State University system network.

Scope

This policy applies to all Southern Connecticut State University employees, contractors, consultants, temporaries, students and other workers including all personnel affiliated with third parties utilizing VPNs to access the Southern Connecticut State University network. This policy applies to implementations of VPN that are directed through an IPsec Concentrator.

Policy

Approved Southern Connecticut State University employees and authorized third parties (customers, vendors, etc.) may utilize the benefits of VPNs, which are a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees. Further details may be found in the Remote Access Policy.

Additionally,

1. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to Southern Connecticut State University internal networks.
2. VPN use is to be controlled using either a one-time password authentication such as a token device or a public/private key system with a strong passphrase.
3. When actively connected to the system network, VPNs will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped.
4. Dual (split) tunneling is NOT permitted; only one network connection is allowed.
5. VPN gateways will be set up and managed by Southern Connecticut State University's Network Services Group.
6. All computers connected to Southern Connecticut State University internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the system standard (provide URL to this software); this includes personal computers.
7. VPN users will be automatically disconnected from Southern Connecticut State University's network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.
8. The VPN concentrator is limited to an absolute connection time of 24 hours.
9. Users of computers that are not Southern Connecticut State University-owned equipment must configure the equipment to comply with Southern Connecticut State University's VPN and Network policies.
10. Only InfoSec-approved VPN clients may be used.
11. By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of Southern Connecticut State University's network, and as such are subject to the same rules and regulations that apply to Southern Connecticut State University-owned equipment, i.e., their machines must be configured to comply with Network security administrator/team Security Policies.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Definitions

Term	Definition
IPSec Concentrator	A device in which VPN connections are terminated.

Extranet Policy

Purpose

This document describes the policy under which third-party organizations connect to Southern Connecticut State University networks for the purpose of transacting business related to Southern Connecticut State University.

Scope

Connections between third parties that require access to non-public Southern Connecticut State University resources are governed by this policy, regardless of whether a telco circuit (such as Frame Relay or ISDN) or VPN technology is used for the connection. Connectivity to third parties such as the Internet service Providers (ISPs) that provide Internet access for Southern Connecticut State University or to the Public Switched Telephone Network does NOT fall under this policy.

Policy

Prerequisites, Security Review

All new extranet connectivity must undergo a security review with the Southern Connecticut State University **Information Security department**. This review ensures that all third-party network access serves a legitimate business need.

Third-Party Connection Agreement

All new connection requests between third parties and Southern Connecticut State University require the signature of a Third-Party Agreement **by the vice president of the sponsoring organization** and a representative who is legally empowered to sign on behalf of the third party. The signed document will be kept on file with **[name of team responsible for extranet agreements]**. Documents pertaining to connections into Southern Connecticut State University labs are to be kept on file with the **[name of team responsible for lab security]**.

Business Case

All production extranet connections must be accompanied by a valid written business justification, which is approved by a project manager in the extranet group. Lab connections must be approved by the **[name of team responsible for lab security]**. This business case is typically included as part of the Third-Party Agreement.

Point Of Contact

The sponsoring organization must designate a person to be the Point of Contact (POC) for the extranet connection. In the event that the POC changes, promptly inform the relevant extranet organization.

Establishing Connectivity

Sponsoring organizations within Southern Connecticut State University that wish to establish connectivity to a third party must submit a new site request, including complete information about the proposed access, to the extranet group. The extranet group will address potential security issues raised by the project. If the proposed connection is to terminate within a lab, the sponsoring organization must also engage the [name of team responsible for lab security].

All extranet connectivity must be based on the least-access principle, in accordance with the approved business requirements and the security review. In no case will Southern Connecticut State University rely upon the third party to protect Southern Connecticut State University's network or resources.

Modifying or Changing Connectivity and Access

All changes in access must be accompanied by a valid business justification, and are subject to security review. Implement changes via the Southern Connecticut State University change management process. The sponsoring organization is responsible for notifying the extranet management group and/or Southern Connecticut State University when there is a material change in their original access request so that security and connectivity evolve accordingly.

Terminating Access

When access is no longer required, the sponsoring organization must notify the extranet team responsible for that connectivity, which will then terminate the access. This may mean modifying existing permissions up to terminating the circuit, as appropriate. The extranet and lab security teams must audit their respective connections on an annual basis to ensure that all existing connections are still needed, and that the access provided meets the needs of the connection. Connections that are no longer used to conduct Southern Connecticut State University business, will be terminated immediately. Should a security incident or review determine that a circuit has been compromised or is no longer used to conduct Southern Connecticut State University business, Southern Connecticut State University and/or the extranet team will attempt to notify the POC or the sponsoring organization prior to modifying permissions or terminating the connection.

Enforcement

Any employee violating this policy may be subject to disciplinary action, up to and including termination of employment.

Definitions

Term	Definition
Circuit	For the purposes of this policy, circuit refers to the method of network access,

	and may include ISDN, Frame Relay, etc., or VPN/encryption technologies.
Sponsoring Organization	The Southern Connecticut State University organization that requested third-party access to Southern Connecticut State University networks.
Third Party	A business that is not a formal or subsidiary part of Southern Connecticut State University.

Additional Resources and References:

<http://www.rx2000.org/KnowledgeCenter/hipaa/hipfaq.htm>

http://www.hospitalconnect.com/aha/key_issues/hipaa/whatsnew/whatsnew.html

<http://www.smed.com/hipaa/overview/fastfacts.php>

<http://aspe.hhs.gov/admsimp/>

<http://www.hipaadvisory.com/>

<http://www.sans.org/>