SUBJECT	INTERNET SECURITY POLICY

Internet Security Policy

Purpose

The purpose of this policy is to establish management direction, procedures, and requirements to ensure the appropriate protection of Northern College (NC) information and equipment by Internet connections.

Scope

This policy applies to all employees, contractors, consultants, temporaries, and other users at Northern College, including those users affiliated with third parties who access Northern College computer networks. Throughout this policy, the word "worker" will be used to collectively refer to all such individuals. The policy also applies to all computer and data communication systems owned by and/or administered by Northern College.

Specific policy

All information traveling over Northern College computer networks that has not been specifically identified as the property of other parties will be treated as though it is a Northern College corporate asset. It is the policy of Northern College to prohibit unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft of this information.

In addition, it is the policy of Northern College to protect information belonging to third parties that has been entrusted to Northern College in confidence as well as in accordance with applicable contracts and industry standards.

Introduction

The new resources, new services, and interconnectivity available via the Internet all introduce new opportunities and new risks. In response to the risks, this policy describes Northern College's official policy regarding Internet security. It applies to all users (employees, contractors, temporaries, etc.) who use the Internet with Northern College computing or networking resources, as well as those who represent themselves as being connected—in one way or another—with Northern College.

All Internet users are expected to be familiar with and comply with these policies. Questions should be directed to the Manager of Information Technology and Property. Violations of these policies can lead to revocation of system privileges and/or disciplinary action, including termination.

SUBJECT	INTERNET SECURITY POLICY

Information Movement

All software downloaded from non-Northern College sources via the Internet must be screened with virus detection software prior to being opened or run. Whenever the provider of the software is not trusted, downloaded software should be tested on a stand-alone (not connected to the network) nonproduction machine. If this software contains a virus, worm, or Trojan horse, then the damage will be restricted to the involved machine. Information Technology Services is to be contacted whenever it is required that software from the Internet is to be downloaded.

All information taken off the Internet should be considered suspect until confirmed by separate information from another source. There is no quality control process on the Internet, and a considerable amount of its information is outdated or inaccurate.

Unless tools like privacy enhanced mail (PEM) are used, it is also relatively easy to spoof another user on the Internet. Likewise, contacts made over the Internet should not be trusted with Northern College information unless a due diligence process has first been performed. This due diligence process applies to the release of any internal Northern College information (see the following section).

Users must not place Northern College material (software, internal memos, etc.) on any publicly accessible Internet computer that supports anonymous file transfer protocol (FTP) or similar services, unless the Director of Marketing has first approved the posting of these materials.

In more general terms, Northern College internal information should not be placed in any location, on machines connected to Northern College internal networks, or on the Internet, unless the persons who have access to that location have a legitimate need-to-know.

All publicly writable (common/public) directories on Northern College Internet-connected computers will be reviewed and cleared periodically. This process is necessary to prevent the anonymous exchange of information inconsistent with Northern College's business.

Examples include pirated software, purloined passwords, stolen credit card numbers, and inappropriate written or graphic material (i.e., erotica). Users are prohibited from being involved in any way with the exchange of the material described in the last sentence.

Information Protection

Wiretapping and message interception are straightforward and frequently encountered on the Internet. Accordingly, Northern College secret, proprietary, or private information must not be sent over the Internet unless it has first been encrypted by approved methods (contact the

SUBJECT	INTERNET SECURITY POLICY

Information Technology Services department for assistance).

Unless specifically known to be in the public domain, source code must always be encrypted before being sent over the Internet (contact Information Technology Services for assistance).

Credit card numbers, telephone calling card numbers, log in passwords, and other parameters that can be used to gain access to goods or services must not be sent over the Internet in readable form. The PGP (pretty good privacy) encryption algorithm, or another algorithm approved by the Northern College's Manage of Information Technology and Property, must be used to protect these parameters as they traverse the Internet.

This policy does not apply when logging into the machine that provides Internet services. Currently Northern College does not use any type of encryption. In keeping with the confidentiality agreements signed by all staff, Northern College software, documentation, and all other types of internal information must not be sold or otherwise transferred to any non-Northern College party for any purposes other than business purposes expressly authorized by management.

Exchanges of software and/or data between Northern College and any third party must specify the terms of the exchange, as well as the ways in which the software and/or data is to be handled and protected.

Regular business practices, such as shipment of software in response to a customer purchase order, need not involve such a specific agreement since the terms are implied.

Northern College strongly supports strict adherence to software vendors' license agreements. When at work, or when Northern College computing or networking resources are employed, copying of software in a manner that is not consistent with the vendor's license is strictly forbidden.

Likewise, off-hours participation in pirate software bulletin boards and similar activities represent a conflict of interest with Northern College work, and are therefore prohibited. Similarly, reproduction of words posted or otherwise available over the Internet must be done only with the permission of the author/owner.

Expectation of Privacy

Staff using Northern College information systems and/or the Internet should realize that their communications are not automatically protected from viewing by third parties. Unless encryption is used, staff should not send information over the Internet if they consider it to be private.

At any time and without prior notice, Northern College management reserves the right to examine e-mail, personal file directories, and other information stored on Northern College

SUBJECT	INTERNET SECURITY POLICY

computers.

This examination assures compliance with internal policies, supports the performance of internal investigations, and assists with the management of Northern College information systems.

Resource Usage

Northern College management encourages staff to explore the Internet, but if this exploration is for personal purposes, it should be done on personal, not College, time. Likewise, games, news groups, and other non-business activities must be performed on personal, not College, time.

Use of Northern College computing resources for these personal purposes is permissible so long as the incremental cost of the usage is negligible, and so long as no business activity is preempted by the personal use. Extended use of these resources requires prior written approval by a director.

Public Representations

Staff may indicate their affiliation with Northern College in bulletin board discussions, chat sessions, and other offerings on the Internet. This may be done by explicitly adding certain words, or it may be implied, for instance via an e-mail address.

In either case, whenever staff provide an affiliation, they must also clearly indicate that the opinions expressed are their own, or not necessarily those of Northern College.

All external representations on behalf of the College must first be cleared with the Director of Marketing. Additionally, to avoid libel problems, whenever any affiliation with Northern College is included with an Internet message or posting, "flaming" or similar written attacks are strictly prohibited.

Staff must not publicly disclose internal Northern College information via the Internet that may adversely affect Northern College’s customer relations or public image unless the approval of the director of marketing or president has first been obtained. Such information includes business prospects, unit costing, RFP information, and the like. Responses to specific customer e-mail messages are exempted from this policy.

Care must be taken to properly structure comments and questions posted to mailing lists, public news groups, and related public postings on the Internet. If staff are not careful, they may let the competition know that certain internal projects are underway. If a user is working on an unannounced product, a research and development project, or related confidential Northern College matters, all related postings must be cleared with one's program director prior to being placed in a public spot on the Internet.

SUBJECT	INTERNET SECURITY POLICY

Access Control

All users wishing to establish a connection with Northern College computers via the Internet must authenticate themselves at a firewall before gaining access to Northern College's internal network. This authentication process must be done via a password system approved by Information Technology Services. This will prevent intruders from guessing passwords or from replaying a password captured via a "sniffer attack" (wiretap).

Unless the prior approval of the Manager of Information Technology and Property has been obtained, staff may not establish Internet or other external network connections that could allow non-Northern College users to gain access to Northern College systems and information. These connections include the establishment of multi-computer file systems (like Sun's NIS), Internet home pages, FTP servers, and the like.

Likewise, unless Northern College has approved the practice in advance, users are prohibited from using new or existing Internet connections to establish new business channels. These channels include electronic data interchange (EDI) arrangements, electronic malls with online shopping, online database services, etc.

Reporting Security Problems

If sensitive Northern College information is lost, disclosed to unauthorized parties, or suspected of being lost or disclosed to unauthorized parties, the Manager of Information Technology and Property must be notified immediately.

If any unauthorized use of Northern College's information systems has taken place, or is suspected of taking place, Information Technology Services must likewise be notified immediately. Similarly, whenever passwords or other system access control mechanisms are lost, stolen, or disclosed, or are suspected of being lost, stolen, or disclosed, Information Technology Services must be notified immediately (contact your nearest Technical Support person)

Because it may indicate a computer virus infection or similar security problem, all unusual systems behavior, such as missing files, frequent system crashes, misrouted messages, and the like must also be immediately reported. The specifics of security problems should not be discussed widely but should instead be shared on a need-to-know basis.

Users must not "test the doors" (probe) security mechanisms at either Northern College or

other Internet sites unless they have first obtained permission from the Manager of Information Technology and Property. If users probe security mechanisms, alarms will be triggered and resources will needlessly be spent tracking the activity.

SUBJECT	INTERNET SECURITY POLICY

Responsibilities

As defined below, Northern College groups and staff members responsible for Internet security have been designated in order to establish a clear line of authority and responsibility.

a) Information Technology Services (ITS) must establish Internet security policies and standards and provide technical guidance on PC security to all Northern College staff. The ITS department must also organize a computer emergency response team to respond to virus infestations, hacker intrusions, and similar events.

b) ITS staff must monitor compliance with Internet security requirements, including hardware, software, and data safeguards. Program directors must ensure that their staffs are in compliance with the Internet security policy established in this document. ITS staff must also provide administrative support and technical guidance to management on matters related to Internet security.

c) ITS staff must periodically conduct a risk assessment of each production information system they are responsible for to determine both risks and vulnerabilities.

d) ITS staff must check that appropriate security measures are implemented on these systems in a manner consistent with the level of information sensitivity.

e) ITS staff must check that user access controls are defined on these systems in a manner consistent with the need-to-know.

f) Northern College information owners must see to it that the sensitivity of data is defined and designated on these systems in a manner consistent with in-house sensitivity classifications.

g) Northern College Managers must ensure that:

1. Employees under their supervision implement security measures as defined in this document.
2. Employees under their supervision delete sensitive (confidential) data from their disk files when the data is no longer needed or useful.
3. Employees under their supervision who are authorized to use personal computers are aware of and comply with the policies and procedures outlined in all Northern College documents that address information security.
4. Employees and contractor personnel under their supervision complete the pre-exit clearance process upon their official termination of employment or contractual agreement.

SUBJECT	INTERNET SECURITY POLICY

5. Employees and contractor personnel under their supervision make back-up copies of sensitive, critical, and valuable data files as often as is deemed reasonable.

h) Users of Northern College Internet connections must:

1) Know and apply the appropriate Northern College policies and practices pertaining to Internet security.
2) Not permit any unauthorized individual to obtain access to Northern College Internet connections.
3) Not use or permit the use of any unauthorized device in connection with Northern College personal computers.
4) Not use Northern College Internet resources (software/hardware or data) for other than authorized College purposes.
5) Maintain exclusive control over and use of his/her password, and protect it from inadvertent disclosure to others.
6) Select a password that bears no obvious relation to the user, the user's organizational group, or the user's work project, and that is not easy to guess.
7) Ensure that data under his/her control and/or direction is properly safeguarded according to its level of sensitivity.
8) Report to the Information Technology Services staff any incident that appears to compromise the security of Northern College information resources. These include missing data, virus infestations, and unexplained transactions.
9) Access only the data and automated functions for which he/she is authorized in the course of normal business activity.
10) Obtain supervisor authorization for any uploading or downloading of information to or from Northern College multi-user information systems if this activity is outside the scope of normal business activities.
11) Make backups of all sensitive, critical, and valuable data files as often as is deemed reasonable by their supervisor.

Disciplinary Process

Violation of these policies may subject employees or contractors to disciplinary procedures up to and including termination.