Security

1.1 Access to Information Resources

Northern Oklahoma College facilitates legitimate access to information and information technology resources to facilitate normal business activities for all users of Northern Oklahoma College systems while at the same time reducing exposure to unauthorized access to both employees and non-employees.

BASIS

Many of Northern Oklahoma College employees rely on information and information technology to perform their job functions. Access to information resources should be reasonably simple, have integrity and maintain confidentiality. While security measures can sometimes complicate legitimate access, the consequences of security problems that result from unauthorized access can be severe and include:

- Time, effort and monetary resources to correct security problems
- Damage, deletion and compromise of critical data and information
- Damage to Northern Oklahoma College's reputation

DATA AND APPLICATION IMPLICATIONS

- Managerial staff are responsible for determining when the user accounts of ex-employees can be removed from the system and destroyed. Managerial staff are also responsible for notifying the correct personnel to carry out such actions.
- Employees should exercise precautions when sending or receiving information over the Internet to prevent viruses, worms, Trojan horses and other potentially damaging software.
- All computer files, including e-mail, are Northern Oklahoma College's assets. Employees should be aware that computer files are not private and can be accessed or quarantined at any time by Northern Oklahoma College.
- Northern Oklahoma College respects and adheres to all copyrights and licensing agreements.
- Individual departments are responsible for enforcing the terms of software agreements and preventing illicit software copying.

INFRASTRUCTURE SECURITY IMPLICATIONS

- There must be offsite access guidelines for all employees so that a standard set of protocols is followed to reduce risk.
- Dial-in modems must not be left on auto-answer when connected to Northern Oklahoma College servers or desktop computers. Exceptions to this must be reviewed and approved by the Network and Server Administrator. Information Technology Services will prepare guidelines for potential exceptions and the circumstances that warrant them.
- Access from remote locations and systems must be monitored and passwords changed on a periodic basis.
- Connections between computers on the Northern Oklahoma College network and computers outside the Northern Oklahoma College network must adhere to Northern Oklahoma College's firewall design.
- Access to the network from outside the firewall should only be allowed to those who require access to meet our business needs.

- A specific individual should be ultimately responsible and accountable for systems that connect to outside networks.
- Ex-employees should not have access to Northern Oklahoma College's computers or network. Access should be removed immediately following their termination of work for the organization. Managers have discretion to determine access for employees who are on leave of absence.
- Systems that connect to outside networks must be architecturally-compatible and secured.

COMPUTER SECURITY IMPLICATIONS

- Password security must be implemented and enforced.
- Department managers are responsible for seeing that passwords for ex-employee accounts are changed promptly by submitting a work order to the Department of Information Technology.
- Account, file, and device access privileges, including file sharing on desktop computers, should not be turned on by default.
- Guidelines are necessary to determine who gets privileged access on computers, including how the decision is made, how privileged account usage is monitored, and a minimal standard of behavior is enforced.
- Varying levels of access privileges may be needed on some systems.

PHYSICAL SECURITY IMPLICATIONS

- Physical security for computer rooms and public computer areas must be properly maintained.
- Biometric, restricted key or electronic card key access must be enforced for all machine rooms and network access points.
- Northern Oklahoma College has the right to remove an employee's computer to ensure the integrity of the computer files.
- Sensitive and/or confidential record information must be secured. Printed copies, disks, and tapes should be kept in locked cabinets or rooms.
- When no longer needed, confidential and/or sensitive hard copy output must be shredded, not recycled.

BREAK-INS, VIRUSES, WORMS, AND TROJAN HORSE IMPLICATIONS

- Northern Oklahoma College's network and computers must be routinely monitored for potential break-ins and security breaches.
- Information Technology Services should maintain and review a central log of all security problems.
- IT staff must use good judgment in publicizing security problems. Information should often only be disseminated on a need-to-know basis.
- If a break-in is detected or a virus, worm, or Trojan horse infects Northern Oklahoma College's resources, IT staff must be adequately prepared to take appropriate actions.
- Information Technology Services will provide the IT groups with written procedures on what to do in the event of a security breach, including information on determining how the intrusion occurred, how to change passwords for suspected accounts, and how to check for Trojan horses and trap doors.
- Escalation procedures should be clearly documented and include information about who can be contacted for higher-level help and the departments that should be notified.
- All computers must run current anti-virus software.

1.2 Information Security Participation

All users of Northern Oklahoma College information technology systems must participate in information security.

BASIS

- Everyone must handle all information and information technology resources in a manner that doesn't compromise Northern Oklahoma College's information security.
- Northern Oklahoma College owns all information produced by its employees in the course of doing business.
- All files stored on a Northern Oklahoma College computer belong to Northern Oklahoma College.

EMPLOYEE IMPLICATIONS

- All employees are responsible for exercising sound business sense to maintain, protect, and share information and data.
- Employees should not share Northern Oklahoma College's information and data with people outside the organization except when doing so helps achieve our business goals.
- Employees shall participate in open communication of information with other Northern Oklahoma College staff when necessary or beneficial.
- Department managers are responsible for their staff's appropriate use of Northern Oklahoma College's computers and related services.
- Failure to comply with Northern Oklahoma College's computer security and privacy policies is grounds for disciplinary action, including termination of employment.
- Employees will be permitted to use Northern Oklahoma College computers and services for personal use when such use does not interfere with legitimate business uses.
- Employees must consent to Northern Oklahoma College's requests for access to corporate information stored on personally-owned computers.
- Employees are responsible for protecting and destroying any Northern Oklahoma College data and information stored on personally-owned computers, telecommunication devices, copied to portable computers, stored on portable drives, printed on faxes, and printed on printers.

DATA AND SOFTWARE IMPLICATIONS

- Each department is responsible for insuring that data on desktop computers is backed up regularly.
- Northern Oklahoma College must develop and implement a comprehensive, tested backup procedure that includes making backups, storing backup material, and recovering data.
- Computer files, including e-mail, created on Northern Oklahoma College's computer systems are Northern Oklahoma College property. They should not be considered private and may be searched for litigation or other corporate purposes at any time as needed.
- Information published using Northern Oklahoma College computers is covered by the employee confidentiality agreement. Posting to public bulletin boards or sending e-mail to large distribution lists from Northern Oklahoma College computers may constitute publication.
- Northern Oklahoma College can require that all corporate information, data, and software on personally-owned computers be destroyed.

COMMUNICATION IMPLICATIONS

- Information security guidelines must be clear and brief.
- All Northern Oklahoma College employees must be trained to properly handle information, data, and appropriate security measures.
- All Northern Oklahoma College employees must be educated about the importance of security.
- Information Technology Services must provide guidelines for employees about Internet and other network access to sites outside the network.

1.3 Benefits, Risks and Costs

The cost of information security measures should be balanced against the risks and benefits involved.

BASIS

- Security measures will cost money, require personnel time, and inconvenience users and administrators of the services.
- Data and information should be protected when there is a clear business need to do so.
- Good judgment is necessary when balancing security concerns and business needs.

IMPLICATIONS

Costs may include:

- Extra routers with better filtering capabilities.
- Expansion of firewall security.
- Operational costs to set up and run the equipment.
- Costs in convenience, productivity, and staff morale.

Benefits may include protection of data critically important to Northern Oklahoma College from a competitive point of view.

1.4 Levels of Information Technology Security

Different levels of information technology security and types of legal agreements are required to support Northern Oklahoma College's many types of information and users.

BASIS

Northern Oklahoma College has many types of information:

- Information that is important to achieving corporate goals.
- Confidential information, such as personnel data and patent information.
- Information such as personal databases on desktop computers that may not require protection.

Northern Oklahoma College has many types of users:

- Faculty

- Adjuncts
- Staff
- Students
- Contractors
- Consultants
- Interns
- Collaborators

Information security and legal issues will be different for each type of information and user.

IMPLICATIONS

- What needs to be protected and define different levels of access.
- Definition of security classes (e.g., confidential, proprietary, public) and their levels of access must be defined.
- Access restrictions can apply to data, information, or services.
- Different types of users will require different degrees of supervision and different levels of access of data, information, and services.

1.5 Guidelines of Information Security

Northern Oklahoma College's information security must be:

- Coordinated amongst all groups.
- Controlled appropriately.
- Audited periodically.
- Improved regularly.

BASIS

- None of Northern Oklahoma College's resources are secure unless all of them are secure.
- We should never assume that Northern Oklahoma College's computing environment is totally secure.
- Regular audits will help identify any weak points.

IMPLICATIONS

- Management support of information security is a requirement.
- IT groups must cooperate on security issues.
- Specific information, security responsibilities, and authorities must be well defined at a corporate level to ensure prompt responses to security problems.
- There must be periodic audits of the security of Northern Oklahoma College's systems and network.

1.6 Consultants and Contractors

CONSULTANTS/CONTRACTOR (NON-EMPLOYEE NETWORK ACCESS PROCEDURE)

PURPOSE

This document defines approval considerations regarding network access for non-employees. Whenever possible, non-employees should use stand-alone computers for their work; however, network access may be provided to non-employees if they have a specific business need. Network access includes on-site and remote access, if needed. Non-employees may need access to specific databases and servers that are on the Northern Oklahoma College network.

TO WHOM DOES THIS APPLY?

This procedure applies to consulting companies, independent consultants, "fee for service" contractors, collaborators and vendors. All connections and network resources access between third parties that require access to non-public NOC resources fall under this policy, regardless of what technology is used for the connection. Connectivity to third parties such as the Internet Service Providers (ISPs) that provide Internet access for NOC or to the Public Switched Telephone Network does NOT fall under this policy.

HOW TO DECIDE IF A CONSULTANT QUALIFIES FOR NETWORK ACCESS

A consultant will generally qualify for network access if there is a need to access a server on the network, but may not need to use Northern Oklahoma College email. For example, a consultant is hired to develop a new software program on a development server. A consultant might be hired to maintain software on an existing system. All third party connections will go through a security review with the Department of Information Technology. The reviews are to ensure that all access matches the business requirements in the best possible way, and that the principle of least access is followed.

WHAT ABOUT ELECTRONIC MAIL FOR CONSULTANTS?

If there are no other business reasons for a consultant to have network access, electronic mail should not be provided to consultants, especially if they are working from a remote location. Most consultants already have electronic mail accounts elsewhere. They should use their own internet accounts to exchange e-mail unless business needs dictate they have a Northern Oklahoma College e-mail account.

WHAT AGREEMENTS ARE REQUIRED FOR CONSULTANT NETWORK ACCESS?

All new connection requests between third parties and NOC require that the third party and NOC representatives agree to and sign the Third Party Access & Confidentiality Agreement. This agreement must be signed by NOC's Director of Information Technology as well as a representative from the third party who is legally empowered to sign on behalf of the third party. By signing this agreement the third party agrees to abide by all referenced policies. The signed document is to be kept on file with the Department of Information Technology and a copy with the third party. All non-publicly accessible information is the sole property of NOC.

- POINT OF CONTACT: The third party authority must designate a person to be the Point of Contact for the third party connection. The Point of Contact acts on behalf of the third party, and is responsible for those portions of this policy and the "Third Party Access & Confidentiality Agreement" that pertain to it. In the event that the Point of Contact changes, the relevant third party person or organization, must be informed promptly.

- ESTABLISHING CONNECTIVITY: All third parties that wish to establish connectivity or network resource access to NOC are to file a "Third Party Access & Confidentiality Agreement" signed by the third party person, organization, or rightful designee. NOC will then engage the third party to address security issues inherent in the project. The sponsoring contract authority must provide full and complete information as to the nature of the proposed access to NOC's Department of Information Technology, as requested.

  All connectivity established must be based on the least-access principle, in accordance with the approved business requirements and the security review. In no case will NOC rely upon the third party to protect NOC's network or resources. The Department of Information Technology will grant access to all approved resources and reserves the right to refuse access on the basis of legitimate security concern as decided by the Director of Information Technology or designee.

- MODIFYING OR CHANGING CONNECTIVITY AND ACCESS: All changes in access must be accompanied by a valid business justification, and are subject to security review. The third party is responsible for notifying the Department of Information Technology when there is a material change in their originally provided information so that security and connectivity evolve accordingly. Extensions will be granted on a case by case basis and must be requested in writing by the third party. The Department of Information Technology reserves the right to establish an expiration date for any all remote access accounts.

CONSULTING AGREEMENT DURATION

When access is no longer required, the NOC Department or contracted third party must notify the Department of Information Technology, which will then terminate the access. This may mean a modification of existing permissions up to terminating the circuit, as appropriate. Connections that are found to be deprecated, and/or are no longer being used to conduct NOC business or other approved business transactions will be terminated immediately. Should a security incident or a finding that a circuit has been deprecated and is no longer being used to conduct NOC business necessitates a modification of existing permissions or termination of connectivity. The Department of Information Technology will notify the Point of Contact of the third party and the NOC Department the service was approved for of the change prior to taking any action.

ENFORCEMENT

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

Northern Oklahoma College
Department of Information Technology
Third Party Access & Confidentiality Agreement

Instructions: The Supervisor of the third party employee(s) must complete both pages of this document. Also, the Supervisor must have the employee read and sign the Confidentiality Security Agreement listed below. Submit the completed document to the IT Help Desk, Wilkin Hall, 1220 East Grand Ave, Tonkawa, OK 74653. Forms can be faxed to 580-628-6256.

Section 1: Third Party Information – This section is to be completed by the vendor/consultant.

Name: _____ E-mail: _____

Phone #: _____ Company Name: _____

Confidentiality Security Agreement

I understand that I will have access to a Northern resource(s). I will treat all information as sensitive and/or confidential unless notified in writing otherwise. I will ensure that the information is properly secured in electronic, written, and/or printed format while in my custody. I will not perform an illegal or unauthorized activity(s) that would cause harm directly or indirectly to the college network and/or computer technology. I am knowledgeable of state and federal regulations (i.e. Family Education Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPPA), Payment Card Industry (PCI) Compliance, etc.) and college technology policies (http://www.noc.edu/planning-policies) pertaining to confidentiality and disclosure and I agree not to violate them. I will only disclose information in verbal, electronic, printed, or written format with authorized college personnel. When I am no longer employed with the company specified above and/or when consultation/service is no longer necessary, I agree not to access college resources. Also, I will not keep nor disclose Northern information in any format.

_____ _____
Vendor/Consultant Signature Date

Section 2: College Staff Information – The primary NOC staff person completes this section.

Name: _____ Department: _____

Job Title: _____ NOC E-mail: _____

Phone #: _____ Fax #: _____

Vendor/Consultant Purpose:
_____

Duration of third party access: Begin Date: _____ End Date: _____

I understand that I'm responsible for the supervision of the vendor/consultant while he/she is at Northern.

Staff Signature: _____ Date: _____

Northern Oklahoma College
Department of Information Technology
Third Party Resource Guide

Use this guide to identify the resource(s) that a third party will need to access. Check the box next to the resource or circle the resource that is needed. This page must be submitted along with the Third Party Access & Confidentiality Agreement.

Network Access Request

☐ * Virtual Private Network (VPN) account necessary? Y N
* A vendor/consultant usually has a VPN client installed on a computer. Does the vendor already have a VPN client? Y N If yes, specify client _____

☐ Wireless connectivity or non-wireless/LAN connectivity? Y N

SIS, Document Imaging, and Telecom Request

Circle all requests that apply: SIS Document Imaging Telecom Software

Check which environment(s) access is requested to: ___TEST ___DEV ___PROD ___TRN

___Other, specify _____

Indicate, in general, what services are being performed:

_____

_____

_____

1.7 Identity Theft

IDENTITY THEFT ON THE INTERNET

Identity theft is on the rise. As defined by the Federal Trade Commission, identity theft occurs "when someone uses your personal information such as your name, Social Security number, credit card number or other identifying information, without your permission to commit fraud or other crimes."

Victims of identity theft can spend a great deal of time and money cleaning up the mess made by thieves.

Identity thieves can obtain your personal information in lots of ways, including; from the trash, by hacking into computer systems where this data is stored, or from people with legitimate access.

Frequently now, identity theft occurs on the internet via e-mail or the web. A newer strategy employed by identity thieves, and seen frequently by Northern Oklahoma College employees, is called phishing (pronounced fishing). Phishing , as defined by anit-phishing.org, is:

Phishing attacks involve the mass distribution of 'spoofed' e-mail messages with return addresses, links, and branding which appear to come from banks, insurance agencies, retailers or credit card companies. *These fraudulent messages are designed to fool the recipients into divulging personal authentication data* such as account usernames and passwords, credit card numbers, social security numbers, etc. Because these emails look "official", up to 20% of recipients may respond to them, resulting in financial losses, identity theft, and other fraudulent activity.

You should always be wary of e-mails requesting personal information. Here are some steps you can take to help protect yourself from identity theft:

- Don't give out personal information on the phone, through the mail or over the internet unless you've initiated the contact or are sure you know who you're dealing with. Identity thieves may pose as representatives of banks, Internet service providers (ISPs) and even government agencies to get you to reveal your SSN, mother's maiden name, account numbers, and other identifying information.
- Before you share any personal information, confirm that you are dealing with a legitimate organization. You can check the organization's Web site as many companies post scam alerts when their name is used improperly. Also, contact the company through an address or telephone number you know to be genuine – use the customer support number listed on your account statement or in the telephone book.
- If you receive an unexpected e-mail saying your account will be shut down unless you confirm your billing information, do not reply or click any links in the e-mail body.
- Before submitting financial information through a Web site, look for the "lock" icon on the browser's status bar. It means your information is secure during transmission.

For additional information on ID theft you can have a look at the Federal Trade Commission's web site:

http://www.consumer.gov/idtheft/

The anti-phishing site has information on the latest scams:

http://wwww.antiphishing.org