Northern Oklahoma College

Information and Instructional Technology Policy

TABLE OF CONTENTS

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. Managerial staff are also responsible for notifying the Information Technology Department 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 closets.
- 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

2 SECURITY INCIDENT POLICY

PURPOSE

The purpose of this policy is to establish a standard for escalating, reporting and resolving information security incidents. Northern Oklahoma College will escalate potentially sensitive information security incidents and issues to the Director of Information Technology directly or by email or telephone.

SCOPE

This policy applies to all Northern Oklahoma College "Users." The term "users" apply to any person Northern Oklahoma College, third party contractors, temporaries, guests, licensees or invitees, as well as those who represent themselves as being connected – in one way or another – to Northern Oklahoma College who uses, possesses or has access to communications systems and equipment.

POLICY

Potentially sensitive incidents include, but are not limited to:

- Security breaches of Northern Oklahoma College systems, whether or not resulting in the loss of Northern Oklahoma College confidential information, intellectual property, or other highly sensitive information;
- Violations of the Northern Oklahoma College Professional Conduct and Code of Ethics;
- Violations of the Northern Oklahoma College Confidential Information Protection Policy and Practice;
- Significant instances of misuse or misappropriations of computer assets and systems;
- Thefts of Northern Oklahoma College computing assets;
- Sensitive security issues relating to, or involving, Northern Oklahoma College executives;
- Situations requiring forensic analysis/investigation of Northern Oklahoma College computing assets, and
- Any situation which may pose a serious threat to Northern Oklahoma College's IT business processes and potentially impact Northern Oklahoma College's ability to continue operations or service its customers.

RESOLUTION

Department of Information Technology will confer on the referred matter as soon as possible to identify the potential risks/exposure and potential responses. Northern Oklahoma College will engage Legal, Internal Audit, Human Resources and other internal resources, as appropriate, in determining the appropriate course of action.

INCIDENT REPORTING

Immediately report unauthorized disclosures or uses of confidential information, as well as other potential information security issues, to your manager, the Director of Information Security or you may call the Northern Oklahoma College Help Desk. The caller may report allegations without fear of retaliation and elect to remain anonymous.

ENFORCEMENT

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

3 PASSWORDS

POLICY

This policy applies to all Northern Oklahoma College "Users." The term "users" apply to any person in Northern Oklahoma College, third party contractors, guests, temporaries, licensees, as well as those who represent themselves as being connected – in one way or another – to Northern Oklahoma College who uses, possesses or has access to Northern Oklahoma College communication systems.

GENERAL

- All user-level passwords (e.g., email, desktop computer, local/domain, etc.) must be changed at least every 90 days.
- All passwords must contain at least eight (8) characters.
- Passwords must not be inserted into email messages or other forms of electronic communication without using approved encryption software.
- All user-level and system-level passwords must conform to the guidelines described below.
- All local accounts (to the system) must conform to the guidelines described below.
- All application passwords must be generated randomly if not managed within the password management database. A standard, default password is not to be granted for all users or groups of users.

GUIDELINES

Some of the more common uses of passwords include the following: user level accounts, web accounts, email accounts, screen saver protection, and voicemail password. Due to cost constraints, very few systems have support for one-time tokens (i.e., dynamic passwords which are only used once) and everyone should be aware of how to select strong passwords.

Weak passwords have the following characteristics:

- The password contains less than six (8) characters
- The password is a word found in any language (English, non-English, slang, jargon, proper nouns, etc.)
- The password is a common usage word such as:
    - Names of family members, pets, friends, co-workers, fantasy characters, etc.
    - Computer terms and names, commands, sites, companies, hardware, software.
    - Birthdays and other personal information such as addresses and phone numbers.
    - Word or number patterns like aabbccdd, qwerty, zyxwvuts, 12344321, etc.
    - Any of the above spelled backwards.
    - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)
    - Any of the above with some letters substituted (like passw0rd)

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Contain numbers (0-9)
- Contain at least eight characters.
- Is not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.

Passwords should never be written down or stored on-line. Try to 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.

Passwords should never be shared with anyone for any reason. If an issue or situation arises that requires you to share your password, immediately change it at the first opportunity.

PASSWORD MANAGEMENT

Do not share Northern Oklahoma College passwords with anyone, including administrative assistants or secretaries. The Information Technology Support Staff will be the only exception. All passwords are to be treated as sensitive, confidential information.

Here is a list of "don'ts":

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an email message
- Don't reveal a password to your boss
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation
- In summation, don't talk about a password at all

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

Do not use the "Remember Password" feature of applications (e.g., Microsoft Internet Explorer, Microsoft Outlook, Mozilla Firefox, Netscape Messenger, etc.).

IT Security 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 will be required to change it. Password cracking and guessing are not to be performed by anyone outside of IT Security or an approved third party auditor.

ACCOUNT LOCKOUT

After three (3) consecutive failed login attempts within two (2) hours, the account is locked for good.

APPLICATION DEVELOPMENT STANDARDS

Application developers must ensure their programs contain the following security precautions.

Applications:

- Support authentication of individual users, not groups.
- Must be encrypted on the screen.
- Should not cache the password in a cookie or any other local media format on the client system.
- 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.
- Should provide security capabilities for all sensitive data

ENFORCEMENT

Any employee found to have violated this policy may be subject to disciplinary action which could include termination of employment.

4 USE OF THE INTERNET/ONLINE AND MAIL SERVICES

4.1 Example 1 of Internet Usage and Mail Services Policy

PURPOSE

To communicate Management objectives for the acceptable use of Northern Oklahoma College-provided electronic mail and Internet/Intranet services by all employees and agents ("Users") of Northern Oklahoma College and its subsidiaries.

POLICY

COLLEGE BUSINESS

Northern Oklahoma College-provided electronic mail and Internet/Intranet services are valuable business tools that enhance productivity and communication, but these tools cannot be abused. While incidental and occasional personal use of provided electronic mail and Internet/Intranet services are permitted, they are valuable corporate resources and must not be used for personal solicitation of non-college business, advancement of individual views, or illegal activity. All use and product of such use, including e-mails, are Northern Oklahoma College's not the individual's.

CONFIDENTIALITY

Electronic information on Northern Oklahoma College-provided electronic mail and Internet/Intranet services is an asset of Northern Oklahoma College, not the individual User. The college has the right at all times to monitor all electronic activity and information on the provided electronic mail and Internet/Intranet services. This policy serves as notice to each user that the college may monitor activity on provided electronic mail and Internet/Intranet services without any advance notification to or consent by the user. Northern Oklahoma College reserves the right to disclose any information or communication transmitted or received using the provided electronic mail and Internet/Intranet services as may be appropriate, including disclosure to management, internal security, and law enforcement.

ELECTRONIC MASS MAILING

Mass mailings are messages sent to large email groups such as faculty, the staff, the student body, a division, or a group of organizations. While such messages may seem like a good way to spread information to a wide audience, many recipients perceive them as junk mail and find them offensive. Below is a set of guidelines developed for anyone interested in sending such messages.

Appropriateness:

Think about these points regarding the message you want to send, and the group to whom you want to send it.

- Is the subject of the message relevant to the audience?
- Would you feel comfortable presenting this message in person to each recipient?

- Would you go through the effort to do a mailing like this on paper?
- Has the message already been seen by your audience?
- If a group has a representative body (such as the Student Senate), you may wish to contact that body to confirm the appropriateness of a message, or to ask them to send it for you. The manager of your department or division can also assist in deciding if a message is appropriate.
- It is always inappropriate, and often illegal, to mass mail messages of a commercial, political, or fundraising nature.
- It is always inappropriate to forward chain letters or electronic "petitions."
- As a general principal, the larger a mailing list, the greater the burden to establish that the recipients will find a message useful.

Alternatives:

You should consider these as alternatives to a mass mailing in light of the nature and scope of your message.

- Campus publications
- Box Stuffers
- Posters/Flyers
- Verbal announcement at group meetings

Technical Issues/Netiquette:

If a mass mailing seems appropriate, follow these guidelines for actually posting the message.

- Contact the IT Department to learn about any current technical issues.
- If the message is part of a series to the same audience, make a statement at the top of the message identifying its purpose.
- Mail the message TO yourself and put the distribution list in the BCC field. This hides the very long list of names and addresses at the top of the message, making it easier for the recipient to read and print.
- Don't ask recipients to forward the message on to others.

If you receive inappropriate email, notify the Department of Information Technology. If the message originated within Northern Oklahoma College, IT can communicate with the sender about the distribution of their message.

CONTROLLED AND PROHIBITED ACTIVITIES

All information posted on the Internet representing Northern Oklahoma College must be approved by the appropriate corporate department and consistent with the college's policy for communicating information to the public. Only specifically authorized management or their designee may send broadcast messages to all e-mail Users within one or more of the Northern Oklahoma College campuses.

PROHIBITIONS:

- Creation of Web pages or information sites without appropriate written approval.
- Posting statements representing or purporting to represent Northern Oklahoma College on the Internet or Intranet.
- Using email for purposes of political lobbying or campaigning except as permitted by college rules and regulations.
- The generation or circulation of any form of "chain letter" or other nonprofessional communication.

- Use of Northern Oklahoma College-provided electronic mail and Internet/Intranet services to transmit information on behalf of any company or entity other than Northern Oklahoma College.
- Use of pseudonyms to disguise the identity of a sender.
- Postings to "message boards" about business or individuals within Northern Oklahoma College or any opinions about Northern Oklahoma College or individuals within Northern Oklahoma College.
- Communications on Northern Oklahoma College-provided electronic mail and Internet/Intranet services should be professional and should not contain any pictures, materials, comments, language, links or anything else that might be considered inappropriate or offensive.
- The access of inappropriate web sites and the posting of offensive materials on or using Northern Oklahoma College-provided electronic mail and Internet/Intranet services will not be tolerated and may subject offenders to immediate discharge. The college reserves the right to restrict access to certain sites.
- Use of proxies or services that by-pass the Network controls for Internet content and message filtering.

ILLEGAL ACTIVITIES

Illegal activities, such as harassing other users, accessing or distributing threatening or obscene material, and intentional spread of computer viruses or other destructive information, malicious service disruption, unauthorized attempts to break into any computer system or use resources or access or destroy data belonging to Northern Oklahoma College or any other organization or individual, or unauthorized use or retrieval or distribution of copyrighted material are strictly prohibited. Any illegal use of Northern Oklahoma College-provided electronic mail and Internet/Intranet services will subject the user to prosecution to the full extent of the law. Users can also be held personal liable for any and all damages caused by such activities and may be subject to immediate discharge.

SECURITY

Access to the Northern Oklahoma College-provided electronic mail and Internet/Intranet services must be approved. Only Northern Oklahoma College-approved software may be used when connecting to the Internet through Northern Oklahoma College's network. Before access to the provided electronic mail and Internet/Intranet services will be granted, the user is required to acknowledge receipt and understanding of this policy and sign a statement of acceptance. Account IDs and passwords for the Services are strictly for the use of the registered User and should not be shared or made accessible to others. Under circumstances in which passwords must be provided to others to gain access to the computer, such as system maintenance or repair, a new password should be created and used after the completion of that process. Computers capable of live access to the provided electronic mail and Internet/Intranet services should not be left unattended. Sensitive information must be protected while being transmitted over the Services.

MISADDRESSED MESSAGES

Recipients of messages or information inadvertently sent or misaddressed to them should not copy, retain or disclose the contents of such messages. It is the policy of Northern Oklahoma College that such messages should be deleted and the sender should be notified, if possible, that the message was misaddressed or misdirected.

ACCOUNTABILITY

Every employee at each level is strictly accountable for the enforcement of this policy. Users and their managers are strictly accountable for the accuracy and appropriateness of links and information available from the User's Internet sites.

APPROVAL REQUIREMENTS

N/A

POLICY OWNER/CONTACT

The policy owner is the Director, Information Technology. Questions regarding this policy should be directed to the policy owner.

4.2 Example 2 of Internet Usage and Mail Services Policy

ACCEPTABLE INTERNET USE POLICY

- Ensure all software downloaded from non-Northern Oklahoma College sources via the Internet are screened with a virus detection software prior to being invoked.
- Do not place Northern Oklahoma College material (software, internal memos, etc.) in any location, on machines connected to Northern Oklahoma College internal networks or on the Internet, unless the persons who have access to that location have a legitimate need-to-know.
- Be aware that all publicly writable directories on Northern Oklahoma College Internet-connected computers can be reviewed and cleared each evening;
- Be aware that all internet traffic is recorded;
- Do not use the Internet for commercial purposes such as advertising, marketing, or business transactions without approval of Northern Oklahoma College management;
- Do not create, modify, execute, or distribute any computer program or instructions intended to obscure the true identity of the sender of electronic mail or electronic messages;
- Do not probe security measures at either Northern Oklahoma College or other Internet sites unless you have first obtained permission from Northern Oklahoma College;
- Do not send or disclose Northern Oklahoma College secret, proprietary, or confidential information over the Internet;
- Do not sell or transfer any of Northern Oklahoma College's software, documentation or any other internal information to any non-Northern Oklahoma College party for any purposes other than business purposes expressly authorized by management;
- Do not participate in pirated software, music exchanges, or other non-business related newsgroups, chat rooms (including but not limited to: USENET, web forums, blogs, etc.), and FTP sites; and
- Do not participate in peer-to-peer applications (including but not limited to: WinMX, Kazaa, Bearshare, Morpheus, eDonkey, etc.).

5 INSTANT MESSAGING POLICY

GUIDELINES FOR INSTANT MESSAGING USE

- Employees are permitted use of Instant Messaging (IM) for business related work only.
- Accessing, contributing and downloading of pirated software such as application, music, games, movies, etc. is prohibited.
- File transfers are not supported.
- Use of offensive language and/or derogatory comments to any individual or group is prohibited.
- Northern Oklahoma College will log IM traffic per the Records Management Policy. The retention period will be modeled after email. This information can be used to take disciplinary action against employees who have misused the facilities.

6 TELEPHONE USAGE

This policy is designed to help employees understand the importance of phone usage for Northern Oklahoma College land lines and cellular telephone use. Employees rely on the telephone system and cellular telephones to conduct daily business and to better serve the Northern Oklahoma College community. It is important that managers be proactive in educating employees in the appropriate usage of the telephone system.

LOCAL CALLS

All Northern Oklahoma College owned or operated telephone systems should be used only to conduct official business. Employees should limit personal telephone calls, in frequency and duration, to the greatest extent possible. This includes incoming as well as outgoing telephone calls. Personal calls should not interfere with an employee's duties or with the duties of others and should not impact an employee's productivity.

Certain personal phone calls may be allowed including:

- Calls to notify or contact family members and/or physician in the case of an emergency;
- Calls to notify family members of a scheduling change or travel delay that is a result of Northern Oklahoma College business including calls to make alternate child care or transportation arrangements;
- Brief calls to an employee's residence or family members, and
- Brief calls to local businesses (including government agencies, physicians, auto or home repair) that can only be reached during working hours.

These calls should always be kept to a minimum and only be made on Northern Oklahoma College owned telephones **if** they could not be reasonably made on a non-NOC owned telephone, for example, personal cell phones or pay telephones.

LONG DISTANCE CALLS

Long distance telephone calls using Northern Oklahoma College owned telephones should only be made for official college business and these calls should be approved by a manager prior to making the call. Students are not authorized to make long distance calls on Northern Oklahoma College owned or operated telephones. Collect calls to the college are not authorized unless the employee accepting the call has full knowledge of the intent of the call and that it is college business related.

Long distance calls should not be made for personal reasons unless they are made for an appropriate reason as discussed above, are approved by a supervisor, and the employee does one of the following:

- charges the call to a third number (such as the employee's home phone number); or
- makes the call collect; or
- charges the call to a personal prepaid calling card or to a personal credit or debit card; or
- places the call to a toll free (800,877,888) number.

Only under limited circumstances should long distance calls be allowed without employee pre-payment.

CELLULAR PHONE

Cellular phone use in the work place shall falls under the same policy standards as listed previously. Employees should limit personal cell phone calls, in frequency and duration, to the greatest extent possible. This includes incoming as well as outgoing cell phone calls. Personal calls should not interfere with an employee's duties or with the duties of others and should not impact an employee's productivity.

In addition, Northern Oklahoma College employees that use cellular phones to conduct business should be aware of the laws and regulations that pertain to the use of cellular devices while operating a motor vehicle. These laws and regulations differ among states. Employees should act in a manner that is in accordance with these laws and regulations while operating a motor vehicle. Confidential information should not be discussed on a cellular phone in a public place where the information could be overheard.

REIMBURSEMENT

Monthly invoices can be used to identify calls that should be reimbursed by the employee. Reimbursement for personal calls may be made through a payroll deduction or through a direct payment from the employee.

MANAGEMENT RESPONSIBILITIES

Managers should be responsible for making their employees aware of the telephone usage policies. Managers should also be responsible for:

- ensuring employee compliance with the policy;
- reviewing and evaluating requests for telephone services and equipment.

All employees are required to be familiar with the features and functions of the phone system. All staff will review the features as explained in the Avaya IP Phone Guide. Questions concerning the phone system and its features should be referred to the telephone system administrator or a technical support person.

All employees are expected to utilize the voice mail feature of the phone system. This is required to ensure all call messages are received. This will also help alleviate the need for handling messages through the main switchboard. All employees will ensure that the:

- voicemail message is current and appropriate to the image of the college;
- voicemail message is programmed appropriately during extended periods of absence such as during the summer months;
- all messages received via voice mail are responded to in a timely manner.

7 GENERAL COMPUTER USAGE

A computer is defined as any system, server or workstation, that runs an operating system, including imbedded, that is but not limited to Microsoft Windows, Linux, UNIX and Macintosh. Information on computers should be protected from disclosure to, modification of or theft by unauthorized persons, and controls should be in place to minimize loss or damage.

GUIDELINES

- Where appropriate, paper and computer media should be stored in suitable locked cabinets when not in use, especially outside working hours.
- Users should not store confidential information on the personal computers. File servers should be used to store confidential information since appropriate access restriction can be applied for such confidential data. Availability of information is also ensured by regular backup at the server level.
- Users should not download, install or store games on their computers.
- Sensitive or classified information, when printed, should be cleared from printers immediately.
- The following control measures should be undertaken by the users to secure their personal computers from unauthorized access:
    - Users should terminate or lock their logon session if they are leaving the desktops unattended.
    - Hard disk(s) of the personal computer should not be shared. In the event sharing is required, then the hard disk should be shared by an access control list with no open shares (everyone with either READ or higher access).
- The usage of personal computers or laptops in the office is not permitted.
- The use of Non-Wireless Access Points (WAP) or wireless network adaptors for the purpose of communicating with other computers or networked devices is prohibited and not supported.

8 BYOD USAGE POLICY

PURPOSE

The purpose of this policy is to define standards, procedures, and restrictions for end users who have legitimate requirements to access college data from a mobile device connected to an unmanaged network outside of Northern Oklahoma College's direct control. This mobile device policy applies to, but is not limited to, all devices and accompanying media that fit the following device classifications:

- Laptop/notebook/tablet computers
- Ultra-mobile PCs (UMPC)
- Mobile/cellular phones
- Smartphones
- Personal Digital Assistant (PDA)
- Home or personal computers used to access institutional resources
- Any mobile device capable of storing corporate data and connecting to an unmanaged network

The policy applies to any hardware and related software that could be used to access institutional resources, even if said equipment is not college sanctioned, owned, or supplied.
The overriding goal of this policy is to protect the integrity of the private and confidential institutional data that resides within Northern's technology infrastructure. This policy intends to prevent this data from being

deliberately or inadvertently stored insecurely on a mobile device or carried over an insecure network where it can potentially be accessed by unsanctioned resources. A breach of this type could result in loss of student or employee information, damage to critical applications, and damage to the institution's public image. Therefore, all users employing a mobile device connected to an unmanaged network outside of Northern's direct control to backup, store, and otherwise access corporate data of any type must adhere to college-defined processes for doing so.

APPLICABILITY

This policy applies to all Northern Oklahoma College employees, including full and part-time staff, contractors, freelancers, and other agents who utilize either company-owned or personally-owned mobile devices to access, store, back up, relocate or access any department or student-specific data. Such access to this confidential data is a privilege, not a right, and forms the basis of the trust Northern has built with its students, employees and community. Consequently, employment at Northern does not automatically guarantee the initial and ongoing ability to use these devices to gain access to institutional networks and information.

It addresses a range of threats to – or related to the use of – institutional data:

Threat	Description
Loss	Devices used to transfer or transport work files could be lost or stolen.
Theft	Sensitive institutional data is deliberately stolen and sold.
Copyright	Software copied onto a mobile device could violate licensing.
Malware	Viruses, Trojans, Worms, Spyware and other threats could be introduced via a mobile device.
Compliance	Loss or theft of financial and/or personal and confidential data could expose the college to the risk of non-compliance with various identity theft and privacy laws.

Addition of new hardware, software, and/or related components to provide additional mobile device connectivity will be managed and issued at the sole discretion of the Department of Information Technology.

AFFECTED TECHNOLOGY

Connectivity of all mobile devices will be centrally managed by Northern's Information Technology Department and will utilize authentication and strong encryption measures. Although Northern is not able to directly manage external and mobile devices which may require connectivity to an external network, end users are expected to adhere to the same security protocols when connected to non-institutional networks. Failure to do so will result in immediate suspension of all network access privileges so as to protect the college's infrastructure.

POLICY AND APPROPRIATE USE

It is the responsibility of any employee of Northern who uses a mobile device to access institutional resources to ensure that all security protocols normally used in the management of data on conventional storage infrastructure are also applied here. It is imperative that any mobile device that is used to conduct college business be utilized appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that user's account. Based on this, the following rules must be observed:

ACCESS CONTROL

Northern reserves the right to refuse, by physical and non-physical means, the ability to connect mobile devices to institutional and institutional-connected systems. Northern will engage in such action if it feels such equipment is being used in such a way that puts the college's systems, data, employees, and students at risk.

Prior to initial use on Northern's network or related infrastructure, **all college owned mobile devices must be purchased through and registered with the Information Technology Department.**

All mobile devices attempting to connect to the corporate network through an unmanaged network (i.e. the Internet) will be inspected using technology centrally managed by Northern's Information Technology (IT) Department. Devices that have not been previously approved by IT, are not in compliance with IT's security policies, or represent any threat to the college network or data will not be allowed to connect. Laptop computers or personal computers may only access the college network and data using a Secure Socket Layer (SSL) Virtual Private Network (VPN) connection. The SSL VPN portal Web address will be provided to users as required. Smart mobile devices such as smartphones, PDAs, and UMPCs will access the corporate network and data using Mobile VPN software installed on the device by IT.

SECURITY

Employees using mobile devices and related software for network and data access **will**, without exception, **use secure data management procedures.** All mobile devices must be protected by a **strong password (See Section 3 of IT Policy)**. **Employees agree to never disclose their passwords to anyone**, particularly to family members if institutional work is conducted from home.

All users of mobile devices must employ reasonable physical security measures. End users are expected to secure all such devices used for this activity whether or not they are actually in use and/or being carried. This includes, but is not limited to, passwords, encryption, and physical control of such devices whenever they contain college data. Any non-college computers used to synchronize with these devices will have installed up to date anti-virus and anti-malware software deemed necessary by Northern's IT Department. Any mobile device that is being used to store Northern Oklahoma College data must adhere to the authentication requirements of Northern's IT Department.

IT will manage security policies, network, application, and data access centrally using whatever technology solutions it deems suitable. Any attempt to contravene or bypass said security implementation will be deemed an intrusion attempt and will be dealt with in accordance with Northern's Information Technology policy.

Employees, contractors, and temporary staff must erase all college related data permanently from **personally owned devices** once their use is no longer required. Divisions and departments must notify the IT Department when a **college owned device** needs a transfer in users, be replaced or is no longer needed.

In the event of a lost or stolen mobile college device it is incumbent on the employee to report this to IT immediately. IT will attempt to remotely wipe all data and lock the device to prevent access by anyone other than IT. If the device is recovered, it can be submitted to IT for re-provisioning.

Usage of location-based services and mobile check-in services, which leverage device GPS capabilities to share real-time user location with external parties, is prohibited within the workplace. This applies to corporate-owned mobile devices being used within the college premises.

HELP & SUPPORT

Northern's IT Department will support its sanctioned hardware and software, but is not accountable and will support such devices on a very limited basis and at the discretion of the Director of Information Technology for conflicts or problems caused by the use of unsanctioned media, hardware, or software. This applies even to devices already known to the IT Department.

Employees, contractors, and temporary staff will make no modifications of any kind to company-owned and installed hardware or software without the express approval of Northern's IT Department. This includes, but is not limited to, any reconfiguration of the mobile device.

IT reserves the right, through policy enforcement and any other means it deems necessary, to limit the ability of end users to transfer data to and from specific resources on the enterprise network.

ORGANIZATIONAL PROTOCOL

IT can and will establish audit trails and these will be accessed, published and used without notice. Such trails will be able to track the attachment of an external device to a device, and the resulting reports may be used for investigation of possible breaches and/or misuse. The end user accepts that his or her access and/or connection to Northern's networks may be monitored to record dates, times, duration of access, etc., in order to identify unusual usage patterns or other suspicious activity. This is done in order to identify accounts/devices that may have been compromised by external parties. In all cases, data protection remains Northern's highest priority.

Northern employees must **immediately report** to his/her manager and Northern's IT Department **any incident or suspected incidents of unauthorized data access**, data loss, and/or disclosure of company resources, databases, networks, etc.

Northern Oklahoma College will not reimburse employees if they choose to purchase their own mobile devices. Employees will not be allowed to expense mobile network usage costs.

9 ACCEPTABLE USE ACKNOWLEDGEMENT STATEMENT FORM

This acknowledgement is to certify that I have read and understand the guidelines set forth within the Northern Oklahoma College's Use of the Internet/Online and Mail Services Policy. As an employee or agent of Northern Oklahoma College or its subsidiaries, I will comply with this policy and guidelines. I understand that these guidelines may be modified by Northern Oklahoma College at any time and that I will be advised of such modifications as far in advance as reasonably possible.

I realize privacy is not guaranteed on Northern Oklahoma College's network, Internet/Intranet, and E-mail, and any transmission is subject to review. My use of college provided E-mail, Internet or Intranet services will constitute acceptance of the guideline, and consent to monitoring while using the services. I understand that I am personally liable for my misuse of E-mail, Internet or Intranet services provided by Northern Oklahoma College. I also understand failure to adhere to this policy may result in disciplinary action up to and including discharge.

Name: _____ _____ SSN: _____

Signature: _____ ____ Date: _____

Division/Department: _____

10 CONFIDENTIAL INFORMATION PROTECTION

The protection of confidential information is critical to any business in defining and maintaining success. These information assets include the following:

- The features of unreleased product, schedules, and launch strategies
- Pre-released financial data, not yet available to the public
- Future business ideas and concepts
- Network and systems access passwords
- Information relating to pending acquisitions and joint ventures
- Operational strategies
- Production, marketing, and sales forecasts
- Student's names and their product needs
- Employee records
- Student records
- Security procedures
- Any other information that has value, provides competitive advantage, and is not generally public

Confidential information can be presented or stored in many forms, including but not limited to the following: paper documents, information on electronic storage media, information passed by voice, charts and graphic presentations, audio and video tapes, and email. In any form, it must be protected.

SCOPE

This policy applies to all employees, contractors, temporary workers, and business partners of Northern Oklahoma College and its subsidiaries, worldwide. It applies to proprietary and confidential information in all forms and expressions, developed, owned, and maintained by and for Northern Oklahoma College.

DEFINITION

Confidential information is defined as any data, whether it be technical, financial, operational, or strategic, that if improperly used or disclosed to unauthorized parties, could adversely affect Northern Oklahoma College competitive advantage, or be otherwise damaging to Northern Oklahoma College.

RESPONSIBILITIES

Management personnel are responsible for implementing information protection policy and procedures and monitoring compliance within their respective organizations.

The Director of Information Technology is responsible for establishing and implementing organization-wide information systems and network security policies, standards, and procedures.

Employees, contractors, temporary workers, and business partners are responsible for protecting Northern Oklahoma College confidential information by following this policy and the related protection procedures and for protecting the confidential information of others that has been entrusted to Northern Oklahoma College.

The Originator of a document or other expression containing confidential information is responsible for classifying the information as "confidential" and labeling it properly with handling instructions as appropriate.

CLASSIFYING AND LABELING CONFIDENTIAL INFORMATION

It is the responsibility of the *originator* of confidential information to identify it as *confidential* and label it properly. Information that needs safeguarding – including emails and presentations – should be visibly labeled "**Northern Oklahoma College Confidential"** at the top or the bottom of each page.

The originator of confidential information may specify distribution and handling instructions by including them in the label. Typical handling instructions include the following:

Internal Use Only, which specifies that the information is only for Northern Oklahoma College (who have signed confidentiality agreements).

Do Not Copy or Distribute, which stipulates that the receiver of this information may not distribute it further, forward it, or otherwise disclose it to others, without the agreement of the originator. The label should read, **Northern Oklahoma College: Do Not Copy or Distribute.**

In certain situations, documents will contain headings and labels established by the Legal Department to maintain attorney-client privilege or as "registered and restricted" as determined by the executive staff and Board of Regents. Once the college releases confidential information to the public, or other circumstances undo the need for confidentiality, we should discontinue using these labels.

INFORMATION PROTECTION PROCEDURES

- Employees must be careful when discussing confidential information so those without authorization and a need-to-know do not overhear these conversations. This is especially important in public places and while traveling. Do not expose confidential information, presentations, etc., to those seated around you when traveling on airplanes. Be careful using a computer in conditions where others can view the screen.
- When traveling, do not put confidential information in your checked baggage. Keep it with you and protect it at all times. Use the hotel room safe or safe deposit box to store it if you need to leave it at the hotel. Keep electronic versions of confidential information separate from your computer. Use password protection and, whenever possible, encryption.
- Third parties, including contractors, vendors, and business partners who are privy to Northern Oklahoma College confidential information should sign confidentiality or non-disclosure agreements. Consult the Legal web site for information.
- Employees must lock their workstations (using a password screen saver, lock workstation, or other security feature) to prevent access when away from their desks.
- Employees must protect their workstations and college networks from computer viruses by using Northern Oklahoma College resident virus scanning applications. Do not disable or modify this software.
- Northern Oklahoma College facilities must be secure and access must be restricted to areas where confidential information is processed, used and stored.
- While visitor procedures may vary among Northern Oklahoma College locations, all guests are to identify themselves and register with security, the receptionist, or their host before entering Northern Oklahoma College facilities. Visitors to non-public work areas within Northern Oklahoma College must be escorted.
- When handing out a confidential document, make sure it is delivered directly to the recipient. Do not leave it on their desk or chair. Use a Northern Oklahoma College confidential envelope if you must send it through internal mail.

- When using the post office or other carriers to send confidential information, put the document in a sealed Northern Oklahoma College confidential envelope, and then place that envelope inside the sealed mailing envelope. Do not label the outside envelope "Confidential" – it attracts attention.
- Documents and media containing confidential information must be stored out of view, inside the access controlled areas of our buildings, whenever possible. Confidential information should be stored in locked fine cabinets or secure file rooms.
- Information stored on networks, hard drives, and other electronic storage media, must be protected by properly constructed passwords. Employees must not divulge, or let others use, their passwords. Passwords must be changed every 90 days.
- Employees, contractors and partners must not make unauthorized copies of Northern Oklahoma College or others' licensed software or products.
- When no longer needed, documents and media containing confidential information should be shredded or otherwise destroyed, in accordance with the Northern Oklahoma College Records Management Policy.
- Faxing Confidential Information. If you must fax a confidential document, take these precautions:
    - Telephone the recipient and have them wait at their fax machine.
    - Carefully dial the number, double check it, send the fax, and wait for it to complete.
    - Telephone the recipient a few moments later and make certain they received all pages.
    - Confidential faxes should contain a paragraph instructing the recipient that the fax is confidential, and, if they receive it inadvertently, they are to notify Northern Oklahoma College and not divulge the information. Our standard heading for this purpose is:

This fax contains confidential information intended only for the addressee. Do not read, copy or disseminate it unless you are the addressee. If you have received this fax in error, please call us collect immediately at (insert phone number). Thank you.

- When photocopying confidential information, be careful to remove the original from the machine and take all the copies when you finish.

REPORTING

Immediately report unauthorized disclosures or uses of confidential information, as well as other potential information security issues, to your manager. The caller may report allegations without fear of retaliation and elect to remain anonymous.

PROTECTING MOBILE DEVICES

When a mobile device is stolen two kinds of loss are suffered: the device, and, perhaps far more serious, information stored in the device. Take these precautions:

- Do not leave your device unsecured in a Northern Oklahoma College office. Lock it in its docking station, secure it with a cable lock, or lock it up in a cabinet or your desk when it is not being used.
- Do not leave your device unattended in open view in your hotel room. Utilize the room safe if possible.
- Do not leave your device unattended and in open view in your automobile. If you must leave it in your car, lock it in the trunk.
- Never place your device in checked baggage and keep it securely with you in hotel lobbies, airports, restaurants, and other public places.
- Remember, the carrying case offers no protection from theft; what is inside is easily recognizable.

- Be careful using your device on airplanes and in public areas. Make certain those around you cannot read your screen if you are working with confidential presentations or other material.
- Use password protection and encryption, when possible.

DISCLOSING CONFIDENTIAL INFORMATION PROPERLY

Often Northern Oklahoma College business requires us to share confidential information with people outside our college. Northern Oklahoma College's Legal Department has produced special nondisclosure and confidentiality agreements to use with vendors, customers, consultants, partners, and contractors. Employees are responsible for ensuring these agreements are signed and properly executed before divulging confidential information to these outside parties. Refer to the Legal Department web site for forms and instructions. Confidential information can only be disclosed to people outside Northern Oklahoma College when these agreements are in place.

REVIEWING YOUR RESPONSIBILITIES

Northern Oklahoma College's employees have signed employment agreements with Northern Oklahoma College specifying that they will protect college confidential information and the confidential information of others with whom we work. Following these policies and procedures is required by these agreements.

11 CLASSIFYING TYPES OF INFORMATION

CONFIDENTIAL INFORMATION

Employee information

- Personnel data (privacy data)
- Payroll and financial data
- Human Resources actions
- Performance review data
- Benefits and health plan data and actions
- Manager-employee personnel correspondence and actions

Sensitive and Proprietary Business Information

- Trade Secrets
- Pre-patent information
- Acquisition, merger, and divestiture information
- Corporate business strategies and plans
- Business pricing and costing algorithms
- Competitive and market analyses, forecasts and plans
- Student accounts
- Privileged Legal Information
- Security or Operational Vulnerability Assessments
- Critical Infrastructure
- Safeguards and Security Controls
- Student lists and student information
- Customer account data and agreements

- Business and service proposals
- Vendor and supplier negotiations and agreements
- Legal actions and information
- Security Investigations related information
- Compliance and audit data
- Detailed facilities information
- Passwords, security control codes, access codes, security mechanisms for systems, networks and applications
- Physical and Logical protection processes and procedures
- Financial information which has not been officially certified and submitted for public release
- Asset inventory and value information
- Asset configurations and deployment plans
- Operational plans, status, processes and procedures
- Risk Assessment and Management information
- Real Estate Market Area Analysis Mapping
- Real Estate Owned & Leased Property Data & Reporting
- Tax Returns and Reports

12 Digital Media Management Policy

PURPOSE

The purpose of the Digital Media Management Policy is:

- To ensure compliance with existing state and federal legal requirements that applies to confidentiality, security and retention of Northern Oklahoma College's Information and Digital Media.
- To comply with Digital Media requirements related to litigation, government investigation or audit, and to ensure the availability of records to those who have legitimate needs for the requisite period of time.
- To communicate management objectives for the proper treatment and handling of sensitive information and the efficient and economical management of Digital Media.

This policy applies to all United States subsidiaries and affiliated companies. Offices operating outside the United States must comply with this policy except that they may be modified to comply with applicable local legal requirements regarding Digital Media and information protections.

POLICY

The Digital Media Management Program controls the creation, maintenance dissemination, and disposition of Northern Oklahoma College's digital media, no matter what the media. The Digital Media Management Program is designed to maintain the following principles:

- Comply with prevailing state, federal, and international legal requirements including legal requirements related to litigation, government investigation and audit.
- Apply appropriate safeguards to the access of college digital media to ensure compliance with all laws and to protect and preserve the confidentiality of confidential information.
- Maintain Digital Media in appropriate storage equipment, at appropriate locations.

- Maintain contracts with offsite storage companies.
- Identify and protect vital and historical Digital Media.
- Utilize Digital Media management technologies for appropriate applications.

Northern Oklahoma College digital media is the property of the college and not the author or custodian of those records. No employee has any personal or property right to the digital media of the college including media that the employee helped develop or compile.

Through the implementation of the Digital Media Management Program, the college expects to improve appropriate access to and security of valuable information, facilitate appropriate and authorized sharing and transfer of information, reduce overall costs related to Digital Media management.

Northern Oklahoma College's information must be protected according to its level of sensitivity. Unless otherwise indicated, all college media should be considered and protected as internal-use-only information. That is, college information should be disclosed or distributed to external parties only after obtaining the proper authorizations, appropriate business agreements, and appropriate non-disclosure agreements.

A list of examples for confidential and sensitive information categories, along with references to applicable laws and directives, can be found in the Confidential and Sensitive Information Exhibit.

13 Printer Device Policy

PURPOSE

Northern Oklahoma College strives to provide quality and cost effective print, copy, fax and scan services to meet the needs of students, faculty, and staff while directly impacting the sustainability goals of the institution. As a result, this policy which formalizes current practice aims to:

- Reduce climate impact by minimizing the number of printing devices at the College.
- Reduce expense of consumables by using the most cost effective print/copy/scan/fax devices.
- Reduce the maintenance and upkeep expense of all print/copy/scan/fax devices.

The goal of this printer policy is to control costs, ensure that equipment is properly maintained and in working order, and ensure compliance of responsible use of computing equipment (i.e. for college business). The information contained in this document addresses the management and operation of Northern Oklahoma College's document production assets. These assets include the Print Shop, printers, copiers, faxes and some scanning devices; and this effort is part of the effective management of these college resources. While this document will address how documents can be cost effectively produced across the entire college system, it falls on the individuals to assess the need for document production and the overall effectiveness of printed material.

SCOPE

This policy applies to all employees of Northern Oklahoma College:

- Whenever possible, printing should be discouraged in favor of working from displayed images.
- If bulk printing is required, Printing Services is to be utilized.
- Personal printers and supplies will not be purchased.

EXCLUSIONS

Northern Printing Services

Faculty and staff are encouraged to send all jobs over 100 sheets to the Northern Printing Services Office. Individual programs or brochures must be approved by the Vice President for Development before being prepared for distribution. Additional information can be located in the Graphic Standards Guide at www.noc.edu/graphicstandards.

Northern Oklahoma College's IT Department and Printing Services will be ultimately responsible for the fair and consistent application of these policies in addition to ensuring that the college continuously improves the management and operations of college document production resources.

13.1 DEVICES

MULTIFUNCTION PRINTERS (MFP)

As part of Northern Oklahoma College's continuing sustainability objectives, to save cost on printing and copying, and to provide more widespread access to print/copy/scan/fax devices, a managed print environment has been implemented. This will allow networked multifunctional devices to be utilized for printing, copying, scanning, and faxing. The MFP's provide the college with several benefits:

- Greater user flexibility – a user can release a print job from any desired device on campus.
- Better managed services – a network managed environment assures the right devices in the right location to meet user needs and can provide detailed usage reports. Software used for monitoring devices can provide usage reports for each department or division.
- Sustainability – the MFP's are energy efficient devices that reduce the college's carbon footprint. Additionally, jobs can be set to only print when the user releases them, so if a mistake or change occurs, paper is not wasted.
- Economical – the MFP's are more cost efficient and both supplies and maintenance services are included as part of the program. Maximizing use of these devices allows leveraging this arrangement to achieve volume pricing that can further reduce campus printing costs. Scanning to email can provide a more efficient means of communicating and utilization of faxing through software.
- Privacy – the MFP's print jobs only when the user releases them, so confidential documents are not forgotten and left sitting on open printers.

Multifunction Printer

An MFP is considered to be any network capable document production device that performs at least two of these following operations: print, copy, fax, and scan. These devices capitalize on the existing network infrastructure and provide economies of scale by being able to handle large volumes of jobs. In addition to being able to track document production, MFP's are capable of accepting commands from print control software. Scan-enabled print/copy MFP's are part of the college's overall strategy to provide effective document production services to the college community.

NON MFP (DESKTOP PRINTERS/LASER PRINTERS/INKJET PRINTERS)

Desktop printers constitute one of the most expensive document output processes that the college currently has. It is part of the overall strategic direction of Northern to reduce the total number of desktop printers in operation. While it is impossible for any organization to completely rule out the use of such devices, Northern will make the continued operations and acquisition of such devices the exception. In the rare occasion, a department or division may present a set of extenuating circumstances that would require the college to consider using a less cost effective alternative such as desktop printing.

MODIFICATIONS

The purchase or lease of copiers, printers, faxes and scanners will be handled by request through the Department of Information Technology. No individual, department or division is authorized to purchase or lease these devices. Requests for additional or replacement equipment should also be made through the Department of Information Technology.

Personal printers purchased by individuals with their own personal money are not allowed on Northern Oklahoma College's campuses. If an employee is found to have violated this policy the device identification information will be recorded and the violation will be reported to their immediate supervisor. If further action is needed the device will be disconnected and the appropriate Executive will be contacted for further action.

Any department or division requesting a new device should contact the Department of Information Technology with a summary of the request. The Department of Information Technology will confer with the requesting department or division, Department of Financial Affairs, contracted print services and other campus operations in order to arrive at a recommendation. The Department of Information Technology will provide the requesting department or division the final recommendation. It is within the discretion of the Department of Information Technology to include as part of the final recommendation the relocation or disposal of output devices (printer, copier, fax, scanner).

REQUEST PROCEDURE

The Department of Information Technology should be contacted and provided with an initial definition of the need. IT will schedule an interview with the requestor and will personally conduct an assessment. The assessment will include the following:

- Location of current power, network, and analog service
- Number of users in the immediate area
- Applications, print job types
- Special Needs
- Sensitive Information
- Disability
- Current monthly usage (total output volume from printing, copying and fax)

If a device is approved, the Department of Information Technology will coordinate with the Department of Financial Affairs concerning any budgetary reporting arrangements. The Department of Information Technology will coordinate the install of any network, power or analog services, if needed. When the device arrives, the Department of Information Technology will contact the requesting department or division to schedule installation. After installation, the Department of Information Technology or the contracted print services vendor will conduct an onsite training session to ensure that the device works correctly in the intended environment as well as to educate users on the features and capabilities of the device.

The Department of Information Technology will review any medical-related issue that may warrant the use of a more local printer for the individual employee. These efforts will be conducted in association with Human Resources and will be handled on a case-by-case basis.

13.2 Supplies & Support

Supplies

The Managed Print Services Agreement of the approved MFP/Copiers and laser based print devices includes all supplies in the cost of a print/copy in the managed print environment (paper is not included), as well as equipment servicing.

Sustainable Print Practices

- Double-sided printing (Duplexing)
- Alternatives to printing: Faculty members are encouraged to consider substituting digital formats (Blackboard, etc.) for standard paper course packets as feasible. Faculty are encouraged to consider electronic vs. paper submission for class assignments as feasible.
- Printing Multiple Copies: Avoid printing multiple copies or sets of the same document on a desktop printer. A desktop printer is not a copier and in most cases desktop printers have a much higher operating cost than workgroup printers and MFP/copiers.

The following supplies for the normal operation of MFP/copiers and desktop devices will be ordered and deployed by the Department of Information Technology.

These supplies include:

- All toner and ink cartridges
- Staples used in finishers
- Maintenance Kits

The following supplies and devices are NOT ordered and deployed by the Department of Information Technology but can be ordered through the campus bookstore.

These supplies include:

- Inkjet Printers (toner can be purchased through the campus Bookstore)
- Paper

Support

All printers located within the department or division will be supported and maintained by the contracted print service staff unless the device is labeled otherwise. If the device is not supported by the contracted vendor it will be the responsibility of Northern Oklahoma College's Department of Information Technology. Although the devices supported by the contracted vendor are monitored for toner replacement, it will be the department's or division's responsibility to contact Northern Oklahoma College's IT Help Desk when toner needs to be replaced.

When requesting support or service for a device in your department or division please follow these steps:

- Call the IT Help Desk or submit the request online through the Printer Services Request form located on the IT web site
- Indicate the campus, building and room number
- Indicate whether the device is supported by the contracted vendor or not. If the device is supported by the vendor please report the service ID number located on the device
- Provide a brief description of the problem
- Provide your contact information

Before an actual service ticket is assigned to the contracted print service or IT's Track-IT system, Northern Oklahoma College's IT Technician will make every effort to resolve the issue immediately. If the issue is not resolved immediately the IT Technician will initiate additional steps with the contracted vendor or other means to provide a solution. The Department of Information Technology has a small inventory of backup devices that can be utilized as a temporary device while the assigned device is serviced. The contracted vendor has been authorized to work directly with faculty and staff remotely after a service ticket has been issued by the Department of Information Technology in an effort to resolve certain issues in the most efficient and effective manner.

13.3 INCURRED COSTS

CHARGES

Departments and divisions are billed an allocated Universal Cost Per Print (CPP) rate for mono and color according to volume. These costs include toner, service, supplies, as well as delivery charges for printing service jobs.

- **Cost per Print (CPP)**
  This is the pricing methodology that the college has adopted for the entire document production system. A print refers to ink/toner/pigments applied to a side of paper.

The Department of Financial Affairs will compile usage reports for network printing and copying output for each department and division and will charge each department and division accordingly. Charges will be reported on the expenditure report issued to each department and division. Networked printing charges will rely on the IP address, service ID number and physical location for reporting and tracking usage. Software has also been installed on most of Northern Oklahoma College's computers to enable tracking of usage to those devices that are not networked or supported by the contracted vendor. MFP devices that are not locked by an access code will be charged 100% of the usage to the department or division where the device is physically located.

- **Obtaining Copy/Print Codes (Access Code)**
  - Departments and divisions are fully responsible for the charges incurred under their specific copy/print code.
  - Placing copy/print codes in public access is strictly prohibited.
  - Many MFP/copiers will require a copy/print code for use. An access code has been created for every campus organization. If a new code is needed, the department head, division chair or designee should contact the Department of Financial Affairs.

In general, access codes are distributed to all MFP's on campus, so once a new access code is created, it is made available for use on most of the MFP's on campus.

PROHIBITED ACTIONS

- All printing and copying activity done through college MFP's and desktop devices should be for college business only. Non-work related printing, copying, scanning or faxing is prohibited.
- Printing or copying related to the employee's enrolled course work/assignments is not considered as part of their department's or division's work.
- Interfering with the intended use of college MFP's and desktop devices such as destroying, altering, dismantling, disfiguring, preventing rightful access to or otherwise interfering with the integrity of the device.
- Modifying or removing MFP's or desktop devices or print drivers without proper authorization.
- Using College MFP's and desktop device resources for commercial purposes or non-college-related activities without written authorization from the college. In these cases, the college will require restitution payment of appropriate fees.
- Using college MFP's and desktop devices in any manner which violates Federal, state, or local laws, or college policies.
- Using MFP's and desktop device resources to engage in political campaigning or commercial advertisement.

14 Revoking Privileges after Termination

OBJECTIVE

The objective of this policy is to ensure availability, integrity and confidentiality of systems and information of Northern Oklahoma College by revoking the user accounts/accesses of those who are no longer employed by Northern Oklahoma College.

SCOPE

The Policy describes guidelines and procedures to revoke access for any Northern Oklahoma College "user" who is no longer employed by Northern Oklahoma College. The term "user" applies to any person who is a Northern Oklahoma College employee, staff, faculty, adjunct, student worker, third party contractors, temporaries, guests, licensees of Northern Oklahoma College, as well as those who represent themselves as being connected – in one way or another – to Northern Oklahoma College who uses, possesses or has access to Northern Oklahoma College communications systems and equipment.

POLICY

- User Access Administration teams are primarily responsible for revoking employee's access to Northern Oklahoma College information system in the event of employee's transfer or termination.
- It is inadvisable to maintain employee's accounts and accesses on the systems once the employee leaves the organization. It may lead to security threats in future. Certain accounts such as remote access or extranet VPN accounts may allow access to critical systems.
- It is the responsibility of the employee's manager and the Human Resources department to notify User Access Administration about an employee's termination and begin the process to revoke access.
- Upon receiving such notification to revoke access either via email or helpdesk ticket, access management teams will initiate the process of revoking employee's access to information systems.

- Access to systems will be revoked automatically once the employee ID of the terminated employee is revoked. This includes an employee's access to all of the domains, Email System, and Extranet. This will prevent further access to any systems.

ENFORCEMENT

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