UNK Information Technology Services
IT Security Procedures – 8/20/2013

All employees are responsible for compliance with the *Guidelines for the Use of Information Technology Resources at the University of Nebraska at Kearney* and *Executive Memorandum No. 16, Responsible use of University Computers and Information Systems.* The Security Procedures in this document address specific security-related issues:

1. Access Control for IT Resources
2. Passwords
3. End User Devices
4. Multifunctional Devices on the Network
5. Remote Access
6. Server Administration
7. Network Services
8. Wireless
9. Domain Name Services
10. Internet Traffic Management
11. Information Security Procedures for Campus Departments
12. Information Security Incident Reporting and Response
13. ITS Procedures for Handling Compromised Devices
14. Application Development Policy

Access Control for IT Resources

Access control measures protect against unauthorized access and enable authorized access on a need-to-know basis to all information technology assets when utilizing networks, systems, and/or applications.

Access is granted based upon a formalized procedure initiated on receipt of information from Human Resources, Academic Affairs, or a manager/designee.

All applications must have an information custodian, who is responsible for approving access authorization. Access will be granted based upon role-based guidelines.

Compliance with this procedure is the responsibility of the information custodian, who ensures that formally documented processes for granting access control are developed, maintained, and followed. The processes should include adding users, changing user access, removing user access, and handling lost or forgotten passwords.

Documentation of granted access, changes to access, and removal of access should be maintained. Periodic auditing of user access may occur.

All user account and access information must be considered confidential.

Passwords

This provides guidance for the proper use of passwords and establishes a standard for creation of strong passwords, the protection of those passwords and the frequency of change.

This applies to all employees, contractors, consultants, temporaries, and students who are responsible for an account or any form of access that supports or requires a password or PIN on any system that resides at any UNK or NU facility, has access to the UNK network, or stores any non-public UNK information. All user-level and system-level passwords must conform to the guidelines described below.

General Password Rules:

- Do not share or reveal a password to anyone, regardless of the circumstances.
- Do not write down and store passwords near computers.
- Do not reveal a password in an email message or through other electronic communications.
- Do not reveal a password on a questionnaire or form.
- Default passwords of applications or systems must be changed immediately after installation.
- Initial passwords or reset passwords must be set to the highest level possible.
- Users are responsible for all activity performed with their user-IDs and passwords.
- User-IDs and passwords may not be utilized by anyone but the individuals to whom they have been issued.
- Users must not allow others to perform any activity with their user-IDs and passwords.
- Users must not perform any activity with user-IDs and passwords belonging to other users.
- Do not use the same password for UNK accounts as for other non-UNK access (e.g. personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various UNK access needs.
- Do not use the "Remember Password" feature of applications.
- If an account or password is suspected to have been compromised, report the incident to the Technology Helpdesk and change all passwords.

When technically feasible, this password criteria will be implemented in current systems and applications to secure IT resources. As new systems and applications are purchased, password capability should meet this password criteria.

- Each system requires that passwords be changed at least every 90 days.
- Each system requires that all passwords have at least ten (10) characters.
- Each system checks the length of passwords automatically at the time that users construct or select them.
- After five unsuccessful attempts to enter a password, each system will suspend the involved user-ID until reset by a system administrator.
- The password file maintained by the application should be encrypted.
- At a minimum, the previous ten passwords cannot be reused.

User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user.

Systems and application administrators will ensure that vendor supplied accounts are secure. Such account should be enabled only when necessary for vendor access. This applies to operating system and application software.

General Password Construction Guidelines

Poor, weak passwords have the following characteristics:

- The password contains less than ten characters.
- The password is a word found in a dictionary (English or foreign).
- The password is a common usage word such as:
    - Names of family, pets, friends, co-workers, fantasy characters, etc.
    - Computer terms and names, commands, sites, companies, hardware, software.
    - The words "UNK", "Kearney", or any derivation.
    - Birthdays and other personal information such as addresses and phone numbers.
    - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
    - Any of the above spelled backwards.
    - Any of the above preceded or followed by a digit (e.g. secret1, 1secret).

Strong passwords have the following characteristics:

- The password contains both upper and lower case characters (e.g. a-z, A-Z)
- The password has digits and punctuation characters as well as letters (e.g. 0-9, 1234567890_+\";:<>,./?)
- The password is at least ten alphanumeric characters long.
- The password is not a word in any language, slang, dialect, jargon, etc.
- The password is 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. For example, the phrase might be "This May Be One Way To Remember" and the password could be "TmB1w2R!" or "Tmb1w>r`" or some other variation.

Note: Do not use either of these examples as passwords!

End User Devices

Administrative and academic business at UNK requires end-user devices, including, but not limited to, desktop devices, mobile devices, and shared devices, such as printers. Protection of these devices and the information handled by them is essential to conducting business at UNK. These procedures apply to all employees who utilize end-user devices and apply to all desktop machines, mobile devices, and shared devices, whether the devices are stand-alone or connected to the campus data network.

Configuration Control
Users are allowed to utilize any legally licensed software that helps accomplish business or academic goals. Software should not be installed or utilized unless the user explicitly trusts the source.

Vendor updates and patches must be installed for all software on end-user devices, unless an exemption is granted by UNK Information Technology Services.

Some classifications of software are expressly forbidden for security reasons. In general, users are not allowed to utilize software that intercepts data they are not intended to see, interrupts the flow of data, modifies data they do not have permission to modify, jeopardizes the integrity of information technology resources, or fabricates any information. Exemptions must be granted by Information Technology Services for the following:

- *Spyware* is software that is used to gather sensitive information or to test for weaknesses in systems. It includes packet sniffers, port scanners, password cracking tools, key loggers, and vulnerability testers. ITS-approved spyware detection/removal software should be installed on all university-owned devices, if such software is available for the device.
- *Malicious code* is software that performs an unintended, and often unseen task when executed by an unsuspecting user. It includes viruses, worms, Trojan horses, and backdoors. ITS-approved antivirus software must be installed on all university-owned devices, if such software is available for the device.
- *Peer-to-peer file sharing* software is used to share files with users over the network/Internet. It includes Kazaa, Gnutella, Aimster, and BitTorrent. These applications are commonly used to illegally distribute copyrighted material.
- *Security bypass* software is used to circumvent security mechanisms, like GoToMyPC and dsniff.
- *Remote control* software is used to remotely control or administer a system from another system and includes terminal services, PC Anywhere, and Back Orifice. (PCAnywhere is allowed when utilized through a VPN.)
- *Network management* software is used to gather information from and to control network equipment. Only Information Technology Services staff is allowed to use network management software.

Information Technology Services may periodically scan the network to look for signs of the above software and ensure the integrity of the network. If prohibited software is discovered, the user will be contacted to obtain compliance with this procedure. Questions regarding the use or classification of software can be directed to the Technology Helpdesk at 865-8363 or unkhelpdesk@unk.edu.

Access Control to End-user Devices

It is the responsibility of each employee to ensure that all technology devices are accessed only by authorized individuals. Employees should not utilize a device they are not authorized to use. Also, each employee must ensure that all technology devices for which he/she is responsible comply with all security guidelines and procedures.

Employees must log out of sessions and lock and password-protect access to devices when temporarily leaving an office or desk.

Employees must use strong passwords that conform to the Password Policy. Certain confidential information, including Social Security Numbers, cannot be stored electronically unless an exemption to the Social Security Number Policy is granted by Information Technology Services and campus-approved encryption software is utilized for storing the confidential data.

Physical security measures, such as safes, locking furniture drawers, and locking office doors, are recommended as supplemental measures to protect confidential information.

Viruses
ITS-approved antivirus software must be installed on all university-owned devices, if such software is available for the device. Antivirus software must run when the device is turned on. It must be installed to automatically update at least weekly.

If an employee suspects a device has been compromised or infected by a virus not removed by antivirus software, he/she should immediately stop using the device and call the Technology Helpdesk at 865-8363 or contact a designated support person.

All email attachments should be scanned prior to opening.

Software Licenses
Software license documentation must be retained to get technical support, qualify for upgrade discounts, and verify the legal validity of the licenses.

Employees must comply with software vendor license agreements and copyright holders' notices. Making unauthorized copies of licensed and copyrighted software, even for evaluation purposes, is strictly forbidden.

Backup
All data residing on university-owned devices should be periodically backed up. Employees are encouraged to store data on network file servers managed by Information Technology Services. Network file servers are backed up regularly. Employees who store data on a local device are responsible for ensuring that a backup copy exists.

Destruction
Employees are required to delete data from devices when the data is clearly no longer needed or is no longer useful. Before deleting data, employees must ensure that removal complies with record retention schedules and that the data is not part of a legal records hold process.

Media, including paper, CDs, DVDs, etc., containing confidential information must be shredded for disposal.

Confidential information must be properly removed from hardware devices prior to disposal of the device.

Communication
Remote users must connect to the UNK network through a VPN. Access is available by contacting the Technology Helpdesk at 865-8363.

Establishing local area networks or connections to existing internal networks requires consultation with Information Technology Services to ensure that unauthorized access is not allowed.

Only Information Technology Services may assign an IP address to a device.

Physical Security
If equipment has been vandalized, lost, stolen, or is otherwise unavailable for normal business activities, the head of the department, the Technology Helpdesk, and Public Safety should be promptly informed. Equipment must not be moved or relocated without approval of the designated support person.

Each employee is responsible for the physical security of all devices, include mobile devices, assigned to the employee. All devices assigned to an employee will be stored in Firefly Objects on Loan.

The display screens for all devices used to handle confidential data must be positioned or shielded so information cannot be readily viewed by others.

Confidential printed material must not be left on unattended printers.

Mobile digital storage media cannot be used to store confidential information unless the information is encrypted. When not in use by authorized employees, mobile digital storage media must be locked in secure enclosures, such as a locked file cabinet or a locked furniture drawer.

Devices with critical production applications should have emergency power.

Mission critical applications and any application utilizing confidential information must be hosted on servers in the Information Technology Services Data Center or an NU Data Center.

Management
Employees must promptly report all suspected unauthorized access or tampering with an end-user device to the Technology Helpdesk or a designated support person.

Multifunctional Devices on the Network

A Multifunctional Device (MFD) is an office machine that incorporates the functionality of multiple devices into one piece of equipment. It is typically a combination of printer, copier, fax and scanner.

The steps outlined below are intended to secure an MFD that may scan sensitive data and to reduce the risk of information leakage through logs, SNMP attacks, poorly configured network services, buffer overflows, and potential for data recovery from an internal hard drive.

The MFD should be secured before it is connected to the network.

- Disable all unneeded management protocols, services and applications, including FTP and Telnet services. Protocols necessary to upgrade firmware or configure the device can be open on request.
- Ensure the print/copy/fax/scan services are restricted to required protocols.
- Configure the MFD so print services run only on authorized ports (9100 and/or LPD). Any unused ports must be disabled.

- Assign the MFD a static private campus IP address.
- All default passwords must be changed and must comply with the UNK password standards or to an agreed upon naming convention.

- Restrict access to the MFD's management function to a specific set of IP addresses or trusted subnets.
- Only authorized MFD administrators can modify the global configuration.

- The MFD must maintain its configuration state after power-down or reboot.
- Maintain the MFD patches on a consistent basis. Firmware must never be more than two revisions old.
- All security measures must be restored following maintenance or repair.
- If auditing is available, it must be fully enabled.

- The MFD must be physically secure in an area with restricted access.
- If hard disk functionality is enabled, configure the MFD to remove spooled files, images, and other temporary data using secure overwrite between jobs.
- If the MFD has a removable hard drive, it must be locked into the device to prevent unauthorized access.
- Any storage devices or non-volatile memory must be erased before the MFD or the storage components leave the office.

- If scanning to a file share is enabled, access to the file share must be restricted.

Remote Access

This defines standards for connecting to UNK's network from any remote host, untrusted host, or remote network. These standards are designed to minimize the potential exposure to UNK from damages which may result from unauthorized use of UNK resources. Damages include, but are not limited to, the loss of sensitive or university confidential data, intellectual property, damage to public image, and damage to critical UNK internal systems.

This applies to all UNK employees, students, third-party contractors, vendors and agents with a UNK-owned or personally owned computer or workstation used to connect to the UNK network. This policy applies to any and all remote access connections to the UNK network.

Requests for remote access should be communicated to the Technology Helpdesk at 308-865-8363 or unkhelpdesk@unk.edu.

Anyone found to have violated this Policy may have their network access privileges temporarily or permanently revoked.

It is the responsibility of UNK employees, students, third party contractors, vendors and agents with remote access privileges to UNK's campus network to ensure that their remote access connection is given the same consideration as the user's on-site connection to UNK. They must abide by all UNK policies and procedures while remotely connected to the UNK campus network.

General access to the Internet for recreational use by immediate household members through the UNK network is not allowed. The UNK employee is responsible to ensure that family members do not violate this policy. The UNK employee bears responsibility for the consequences should the access be misused.

Requirements:

- Permission for remote access to a University-owned device may require the requester to scan the University-owned device and present documentation that the scan detects no Social Security Numbers.
- Secure remote access is enforced via password authentication.
- At no time should username or password be shared with anyone, not even family members.
- All devices that are connected to the UNK internal network via remote access technologies must use the most up-to-date anti-virus software. This includes personally owned computers.
- Direct access (initiated from the Internet) will not be allowed to any device connected to the UNK network.
- UNK employees and contractors with remote access privileges must ensure that their UNK-owned or personal computer or workstation, which is remotely connected to UNK's network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.
- Personal equipment that is used to connect to UNK's network must meet the requirements of UNK-owned equipment for remote access.

Server Administration

UNK strives to maintain an environment for education and research. In order to maintain this environment, we are required to protect electronic information resources and comply with applicable laws and regulations. This outlines security and control measures to protect servers and systems connected to the UNK network infrastructure and to protect the confidential data that may be stored on them.

This procedure ensures that appropriate steps are taken to secure servers and the applications and data stored on servers. This procedure applies to all UNK and business partner servers and systems that are connected to the UNK network infrastructure.

Location
Servers that support mission critical applications and/or store confidential data must be physically located in the ITS-managed data center. It is recommended that all servers be physically located in the ITS data center to assure physical security and backup power during electrical outages.

Administration of Servers
Information Technology Services System Administrators will serve as primary administrator for servers with mission critical applications or confidential information. Every server will be assigned a system administrator.

Hardening the Operating System and Applications
All servers must be "hardened". Hardening is the process of shutting off unnecessary protocols and services and applying necessary security patches to the operating system and applications on the system. Servers may be scanned and audited periodically for new vulnerabilities. If a vulnerability or security risk that threatens the network is found, Information Technology Services may temporarily disconnect a server from the network until it has been determined that the vulnerability has been patched or the security risks have been mitigated. System administrators should ensure that no "back doors" access the server.

Passwords
All servers must comply with UNK password requirements. (See the Password section above.) Steps must be taken to ensure that passwords are not sent over the network in "clear text". For servers that are located in the ITS-managed data center and not administered by Information Technology Services System Administrators, an account should be established for use by the Information Technology Services system administration staff to verify that the system is operational when resolving problems.

Content
The content on all systems connected to the UNK network must comply with UNK policies and procedures. Servers storing confidential information should utilize encryption of data at rest and should be located behind a firewall.

Communication
Communication to or from servers, except for web servers, may be limited to the internal network.

Protocols
The use of network communication protocols other than TCP/IP must be coordinated with Information Technology Services.

Disaster Recovery
A 24x7x365 contact will be provided to Information Technology Services System Administrators for any departmental system placed in the ITS-managed data center.

Authentication
All servers must have authentication.

Remote Administration
Remote administration must conform to standards established by Information Technology Services.

Banners
Where possible, all servers should display a login banner that says, "If you are not an authorized user of this system, disconnect immediately."

Auditing
Where possible, system administrators must enable logging and auditing functions on systems they administer. Operating system audit logs should be reviewed periodically. Any suspicious activity found in audit logs should be brought to the attention of the Technology Helpdesk as soon as possible (See Information Security Reporting and Response Procedure.)

Network Services

The data network at the University of Nebraska at Kearney is critical to the operations of the campus and is essential to the daily activities of faculty, staff and students.

The purpose of this procedure is to establish management direction, procedures, and requirements to ensure the appropriate protection of UNK resources supporting network infrastructure, including devices and all information flowing across the network.

The University of Nebraska at Kearney strives to maintain access for its faculty, staff, students, and administrators to electronic systems. To ensure that access is not compromised, interrupted or derogated, all users must abide by the rules defined below. Failure to comply may result in loss of access to the network.

Unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse or theft of networking equipment is prohibited. In addition, UNK protects equipment which belongs to third parties in the same manner that UNK equipment is protected. If networking equipment is found whose ownership is in question, Information Technology Services staff will identify the owner of the equipment and ensure that the equipment is in compliance with all policies and procedures.

Only authorized Information Technology Services staff may install, manage, or change the UNK network infrastructure.

Only networking equipment that has been authorized by Information Technology Services staff shall be connected to the production environment. If a separate network is needed for research or for a lab environment, the ITS Assistant Director-Networking will work with the department to design and install the network. All design configuration changes to the production environment network must be approved by the Assistant Vice Chancellor for Information Technology.

- Modems are prohibited, unless authorized by the Assistant Vice Chancellor for Information Technology.
- Installation of all data communications cabling and equipment must be approved by the Information Technology Services Assistant Director-Networking.
- Private networks must be approved by the Assistant Vice Chancellor for Information Technology.
- Only Information Technology Services staff, may install, configure, and/or use software that can evaluate, compromise, or disrupt the production environment. Use by others is expressly prohibited. Examples include tools that discover or "trap" passwords, identify security vulnerabilities, or intercept or copy information.
- All wireless connectivity is managed by Information Technology Services. All users and devices on the UNK wireless network are required to authenticate.
- Installation of any IP based applications, including audio and video, will be managed by Information Technology Services

Wireless

Wireless or wi-fi service requires specific planning to address security issues and interference problems and to offer highly available, reliable and secure connectivity.

Any campus-installed wireless networks including those not attached to the campus wired network infrastructure, must be reviewed and approved by the ITS Network Manager. Also, the ITS Network Manager must approve any vendor-supplied wireless solution to ensure compatibility with other campus-installed wireless solutions. Vendor contracts involving a vendor supplied wireless solution should not be signed prior to review and approval by the ITS Network Manager. This applies to all members of the workforce.

This does not cover peer-to-peer infrared communication between portable devices.

UNK ITS will periodically scan radio frequencies looking for unregistered wireless networks. If an unregistered wireless network is found, UNK ITS will meet with the owner of the wireless network to develop a plan to meet information and connectivity needs and bring the wireless network into compliance with UNK network standards. If an unregistered wireless network is disrupting the business or academic mission of UNK, the wireless network will be disabled and the owner will be contacted. The ITS Network Manager will identify alternatives to eliminate the disruption.

Only network equipment approved by the ITS Network Manager may be used in a campus-installed authorized wireless network. To facilitate support, to insure security, and to prevent interference, the management of all authorized campus-installed wireless networks will be coordinated by UNK ITS.

All wireless networks with access to university resources will require authentication.

All wireless networks will encrypt data transmitted from the user device to the access point.

All wireless networks within the UNK environment must maintain compliance with all FCC regulations and guidelines.

Domain Name Services

Domain Name Services (DNS) is used by the Internet community to associate organizations with their electronic sites by assigning names and associated IP addresses to specific computers on the Internet.

Information Technology Services is responsible for Domain Name Services for all domains assigned to UNK. UNK faculty, staff and students may not acquire a company or special interest domain name unrelated to the UNK academic mission and have that name resolve to a workstation in a campus location that serves Web pages.

The primary name used by the University of Nebraska at Kearney is “unk.edu”. All uses of “unk.edu” will be in support of the academic mission of the university and will be restricted to use by campus units, faculty, staff, students, and organizations. Information Technology Services will assign third level domain names, such as “dept” in “dept.unk.edu”.

Other Domain Names

UNK will host domain names if a faculty or staff member makes the request in writing for a specific academic purpose. The request must include a brief statement of purpose, the name and email address of the requestor and the requestor’s department.

Domain names with “.com” or names that imply commercial activity require approval from the Assistant Vice Chancellor for Information Technology.

UNK has reserved the names “lopers.com” and “lopers.net”. The use of these names requires permission from the Assistant Vice Chancellor for Information Technology.

General Guidelines

All domain name requests are subject to availability, review for appropriateness, and the requirement that all full names must be unique and correspond to Internet conventions for included characters.

All names in the UNK Domain Name Servers must resolve to a UNK IP address unless a specific exception is allowed. Also, any UNK IP address will resolve to a UNK registered domain name entry.

The Domain Name Service allows alias names as well as primary names. A primary name is the direct name while an alias is a name that resolves to a primary name. A request for an alias must explain why the alias is needed.

If a formal domain name is established by a faculty or staff member that refers to a UNK IP address, permission must be obtained from the Assistant Vice Chancellor for Information Technology.

Domain names cannot be registered that imply association with UNK no matter who is providing domain name service, unless permission is obtained from the Chancellor.

Sites associated with UNK may not include commercial advertisements of any sort without the approval of the Chancellor. No one may use campus networks or servers for commercial activity. Use of vendor logos or identifiers or links to vendor web pages may be appropriate when used as information items or to acknowledge sponsorship. Questions should be referred to the Assistant Vice Chancellor for Information Technology.

Hosting of a Web site for a professional organization with which a department or other entity at UNK is associated , a formally recognized student organization, or a student group sponsored by a faculty or staff member is appropriate as long as it supports the educational, research and/or outreach missions of the campus.

Any Web site that is regarded as a UNK site must use the UNK Domain Name Services.

Internet Traffic Management

The University of Nebraska at Kearney provides computing and networking facilities and services, including Internet access, to support the educational mission of the campus. Access to the Internet is a privilege granted to students, faculty and staff.

Some Internet services and resources result in significant amounts of Internet traffic. Because UNK pays for Internet access based on the amount of traffic to and from the campus, this traffic is managed to control costs while addressing the educational needs of the users, with priority for activities supporting the educational mission of the campus.

The network infrastructure that supports access to the Internet is the property of the University of Nebraska at Kearney, along with the communications that traverse it. Network communications are treated in a confidential manner and contents are examined or disclosed only

- When authorized by the owner; or
- When required to evaluate the effective operation of the network; or
- When directed by the Assistant Vice Chancellor for Information Technology and the Chancellor or a Vice Chancellor if there is evidence of inappropriate use of technology resources, when the health or safety of people or property may be involved, or when required by legal obligations.

Network administrators reserve the right to ensure that systems connected to the UNK network meet minimum standards of security through the use of, but not limited to, active system scans across the network to preserve the integrity of the network and the safety of its users.

Service areas include the residence halls, campus buildings, UNMC Nursing, and MONA.

To manage Internet traffic, a maximum level of Internet traffic for the campus is established. Traffic is prioritized by service area and a maximum level may be imposed on traffic types within a service area.

The maximum levels are adjusted to fit the prevailing traffic patterns while accommodating campus priorities.

The content and formats of Internet services and resources continue to evolve, along with the needs of the campus. Internet traffic management will adapt to the needs and priorities of the campus to provide the most effective use of the Internet.

Information Security Procedures for Campus Departments

This procedure applies to all employees in all UNK departments relative to the conduct of their responsibilities at the University of Nebraska at Kearney at any time and in any location.

By virtue of the execution of the objectives of the department, employees within any department may be required to generate, have access to, communicate, receive and otherwise handle information which is considered to be sensitive and protected by various federal and/or state statutes or regulations. Every student and employee has the freedom from unauthorized and unreasonable intrusion into their personal information whether it be verbal, written, or in digital form.

It is the practice of all employees of the University of Nebraska at Kearney to carry out their duties in such a manner as to assure information security of employee and/or student information and to safeguard it from unauthorized access and disclosure.

Departmental employees are to comply with appropriate access controls and protocols while handling confidential or proprietary information. Care is to be taken to assure that the access, use and security of information complies with all applicable federal, state, and local regulations and University Policies and Procedures governing confidentiality, privacy and information security.

Employees will demonstrate their commitment to information security when using or performing the following:

1. *Enterprise Software* – This software includes division, department, campus or system-wide applications which are utilized to manage information, including, but not limited to SAP and SIS.

2. *Electronic Storage Devices* – These devices include any local or remote networked drives, and storage devices such as CDs, DVDs, tapes, digital cameras, personal digital assistants (PDAs), laptop computers, etc. Encryption must be used for storing confidential information.

3. *Application Software* – This software includes, but is not limited to, Excel spreadsheets, Access Databases, and Word and PowerPoint documents. When utilizing such software and creating files which contain proprietary information, employees will apply the appropriate password protection and encryption.

4. *Computer Monitors/Workstation Displays* – Monitors/displays will be positioned so as to prevent unauthorized or unintentional viewing by employees, vendors, students or others. Privacy screens are to be used where appropriate to assist in protecting proprietary information.

5. *Facsimile Machines* – Facsimile machines must be located to provide maximum information security in compliance with policies. Attention must be given to high traffic areas or otherwise unsecured locations. When receiving a facsimile classified as proprietary, documents must be removed immediately upon receipt. When transmitting proprietary information, documents must be removed immediately upon completion of transmission, or after digital storage for future transmission. All employees transmitting information will verify new or unknown fax numbers before transmitting. Proprietary information must have a fax cover sheet with a confidentiality statement at the bottom stating that the transmitted information is confidential and if improperly received the recipient must notify sender, return or destroy, and not read the transmitted document.

6. *Photocopy Machines* – Recognizing that photocopy machine placement is for convenience, employees must be particularly attentive to photocopying of proprietary information. Such information is not to be left unattended at the machine. When such information is being photocopied, a departmental employee must be present and assure that the original as well as copies are not left on or in the machine when completed. See the section for Multifunctional Devices on the Network, also.

7. *Paper Document Handling and Storage* – When handling proprietary information, care must be given to the location and traffic of unauthorized individuals in proximity of such information. Employees will demonstrate due diligence to eliminate the viewing of or access to such document(s), including such actions as, turning over documents, conducting conversations away from said documents, and securing the office location when unattended. Paper filing systems of such documentation will be properly secured at all times.

8. *Verbal Communications (Telephone or Face-to-Face)* – Employees must demonstrate awareness and care when discussing proprietary information in person or on the telephone. Employees will be cognizant of others (unauthorized) who may be within hearing distance of such conversation(s). If the employee determines that a risk is present, the employee must

find a secure location to conduct a conversation – a closed door office, conference room, or other unpopulated area.

9. *Disposing of proprietary information* – All departmental employees are to determine what information is private and/or confidential and ensure that it is disposed of appropriately.

10. *Social Security Numbers* – The use of social security numbers is prohibited, except for those uses required by law, such as payroll, benefits and financial aid. Any person or office that uses social security number must be granted an exemption from the Social Security Number Policy by the Assistant Vice Chancellor for Information Technology.

Information Security Incident Reporting and Response

Information system security is a growing problem. Effective response and collective action are required to counteract security violations and activities that lead to security breaches. UNK administrators must know the extent of security problems to make proper decisions pertaining to policies, programs and allocation of resources. Responding to security alerts will help to prevent incidents from reoccurring. Quick reporting of incidents, such as new viruses or malware, is essential to stopping them from spreading and impacting other systems.

Attacks on University information technology resources are serious infractions of the *Guidelines for the Use of Information Technology Resources at the University of Nebraska at Kearney*, as is misuse or vandalism of University resources.

The steps for the resolution and follow-up of information security incidents apply to all UNK information technology resources, provide guidance in determining the proper response to misuse of information technology resources from within or outside the University, and document the process UNK will follow to resolve the situation. The ultimate goal of security incident response and centralized reporting is to protect data and prevent damage to UNK operations.

Attacks on University resources will not be tolerated. Employees must report information security incidents that have a real impact on the UNK organization (such as when damage is done, access is achieved by an intruder, loss occurs, web pages are defaced, malicious code is implanted) or when you detect something noteworthy or unusual (new traffic pattern, new type of malicious code, specific IP as source of persistent attacks). Do not report routine probes, port scans, or other common events such as detection and removal of a virus from an email.

An information security incident includes, but is not limited to, the following events, regardless of platform or computer environment:

1. Evidence of tampering with data;
2. System is overloaded to the point it is not responsive (denial of service attack on the network);
3. Web site defacement;
4. Unauthorized access or repeated attempts at unauthorized access (from either internal or external sources);
5. Social engineering incidents;
6. Virus attacks which cause workstations or servers to be inoperable;

7. Email which includes threats or material that could be considered harassment;
8. Discovery of unauthorized or missing hardware or software in your area; and
9. Other incidents that could undermine or raise concern about the stability or reliability of UNK information technology systems.

Information Technology Services staff will work with campus offices/departments to resolve any incident. When evidence exists to suggest that a security incident may have occurred, the following steps will be followed:

1. The attack must be reported to the Assistant Vice Chancellor for Information Technology, who will notify the appropriate Information Technology Services staff members.
2. The users involved must fully cooperate with Information Technology Services staff in resolution of the issue. The Assistant Vice Chancellor for Information Technology, Dean or Vice Chancellor, system administrator, Director of Human Resources, University of Nebraska Information Security Officer, and the Office of the Vice President and General Counsel will determine if evidence should be preserved or if the system can be repaired as soon as possible.
3. If possible, actions will be taken to block or prevent escalation of the attack. ITS may temporarily block access to or from certain devices until the problem is resolved.
4. Steps will be taken to repair the resulting damage and fix the root cause.
5. Service will be restored to its former level, if possible.
6. Evidence will be preserved, as appropriate.

The Assistant Vice Chancellor for Information Technology or designee will:

1. If applicable, coordinate notification of the Internet service provider.
2. Notify and keep informed the Chancellor, the Vice Chancellors, and the appropriate Dean.
3. Notify and keep informed the Director of Human Resources and the Office of the Vice President and General Counsel as appropriate. Decision to involve law enforcement will be made by the Chancellor, the Assistant Vice Chancellor for Information Technology, and the Office of the Vice President and General Counsel;
4. Assemble the Computer Incident Response Team (CIRT) as required; and
5. Ensure the incident is reviewed retrospectively to determine methods of improving security.

Computer Incident Response Team (CIRT) is composed of the Assistant Vice Chancellor for Information Technology; the ITS Assistant Director-Systems; the ITS Assistant Director-Networking; other ITS staff members as appropriate and necessary; and representatives from the department or departments where the incident occurred. Representatives from Human Resources, Student Life, Legal, Public Relations, and Public Safety will be added as the need arises.

ITS Procedures for Handling Compromised Devices

Compromised or vulnerable devices will be blocked from accessing the UNK network as soon as they are identified. It is not always feasible to give prior notice to the individual using the affected device, but every effort will be made to notify the user.

A network block message will be sent to the responsible Technology Coordinator, the Helpdesk, and the ITS Security Team. The block notification will include the following:

- Subject heading of "Network Block Notification - <*building name*>"
- Reason(s) for blocking the device
- As much information as possible to aid in identifying the blocked device: IP address, MAC address, Hostname, End user

It is the responsibility of everyone contacted to identify and shut down the infected or vulnerable device. Under no circumstances should anyone reformat, copy, access, or otherwise alter the contents of the device until cleared to do so by the ITS Security Team.

Analysis will be performed to identify security vulnerabilities and personally identifiable information (PII). If the device must be preserved for evidence, it may not be returned to the user.

When the device is deemed safe, the Technology Coordinator or Helpdesk will reply to the notification email requesting removal of the network block. The unblock request message must include justification for removing the block.

ITS Networking will remove the network block and reply to the notification email confirming the block has been removed.

Application Development

This applies to application development and enhancement in the administrative and student services areas, including hardware, software, and contract personnel. It covers packages purchased from vendors and systems created by in-house developers.

The UNK Student Information System Steering Committee approves the development of all new applications that collect, store, manipulate, display or extract student information. The Committee considers how information is be used, the functionality of the applications, and the constituencies being served. Each request for approval must include a plan that specifies a proposed implementation date as well as the description and dates associated with critical development tasks or events. The Committee can advise the sponsors of applications, and as needed may require the exclusion or inclusion of information or functionality in the final design.

Major changes desired by the sponsor to a previously approved application must be re-submitted to the Committee for review and approval. The application sponsors are allowed to determine when changes are classified as major and warrant review by the Committee. Major changes include changing the student information output to include or exclude data, changing the functionality of the application, or changing the constituencies being served.

Project ownership of a major application system resides with the department or departments that will use the system and "own" the data. These departments are responsible for informing other departments affected by the system implementation of time estimates and business process modifications.

The sponsors and the programming staff are required to support the applications and to review any major modifications with the Committee. Input from user departments regarding applications and modifications is encouraged.

The Committee authorizes when applications are moved into production and available for use by university users.

Definitions

Confidential information means proprietary information, which is information regarding business and academic practices, including, but not limited to, financial statements, contracts, business plans, research data, employee records, and student records. Employee records refers to all information, records, and documents pertaining to any person who is an applicant or nominee for any University personnel position, regardless of whether any such person is ever actually employed by the University, and all information, records, and documents pertaining to any person employed by the University. Student records refers to all information and documents of academic, demographic, or financial data pertaining to one student or to many students in a single record, on lists, or in aggregated data format.

Denial of service is an event in which a user or organization is deprived of resource services that they would normally expect to have.

Employee refers to faculty, staff, students, independent contractors and other persons whose conduct in the performance of work at UNK is under the direct control of UNK, whether or not they are paid by UNK.

Employee records refers to all information, records and documents pertaining to any person who is an applicant or nominee for any University personnel position described in the Board of Regents Bylaws 3.1, regardless of whether any such person is ever actually employed by the University, and all information, records and documents pertaining to any person employed by the University.

End-user Device is a device used by a member of the workforce to accomplish access to information technology resources, including PCs, laptops, printers, and cell phones.

Information is data presented in readily comprehensible form. (Whether a specific message is informative or not depends in part on the subjective perceptions of the person who receives it.) Information may be stored or transmitted via electronic media, on paper or other tangible media, or be known by individuals or groups.

Information custodians are people responsible for specifying the security properties associated with the information systems their organization possesses. This includes the categories of information that users are allowed to read and update. The information custodian is also responsible classifying data and participating in ensuring the technical and procedural mechanisms implemented are sufficient to secure the data based upon a risk analysis that considers the probability of compromise and its potential business impact.

Information security is defined as the ability to control access and protect information from accidental or intentional disclosure to unauthorized persons and from alteration, destruction, or loss.

Information technology resources include, but are not limited to, voice, video, data and network facilities and services.

The *internet* is all networks external to UNK.

Local Area Networks (LANs) include the use of routers, switches and mini-hubs in the production environment and consist of a computer communications system limited to no more than a few miles using high-speed connections.

Mission Critical System is any system that is necessary to conduct the day-to-day business operations of UNK.

The Network is defined to be all UNK owned or managed internal data communication networks without incoming direct public access.

Network Infrastructure includes fiber, copper, circuits, trunks, routers, switches, hubs, wireless access devices, and any other components required to deliver network services to data, voice or video equipment.

Networking equipment shall include all devices that allow computers to communicate with other computers and/or devices (except the internal or external NIC card in a computer/server). This includes, but is not limited to, routers, switches, bridges, wireless access points, and hubs.

Privacy is defined as the right of individuals to keep information about them from being disclosed.

Private Network is a network owned and managed by an organization that is not associated with UNK.

Production environment is all interconnected equipment whose maintenance has been delegated to ITS. Production environment includes equipment necessary to support the day-to-day operating business of UNK.

Proprietary information refers to information regarding business and academic practices, including, but not limited to, financial statements, contracts, business plans, research data, employee records and student records.

Remote access is any access to UNK's network through a non-UNK controlled network, device, or medium.

Server refers to any system that provides or shares resources (files, drives, printing, applications, etc.) with any other system.

Social engineering describes a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedures.

Virtual Private Network (VPN) refers to an encrypted communication link between the campus network and the public Internet. Since all data passing through the communication link is encrypted, it is referred to as being virtually private.

Wide Area Network (WAN) is a physical or logical network that provides capabilities for a number of independent devices to communicate with each other over a common transmission-interconnected topology in geographic areas larger than those served by local area networks.