UNIVERSITY OF NEBRASKA
UNK
KEARNEY

Effective: *February 1, 2017*
Last Revised: *November 27, 2017*

Responsible University Office:
Information Technology Services

Responsible University Administrator:
Chief Information Officer

Policy Contact:
Deb Schroeder
schroederd@unk.edu

End User Device Policy

POLICY CONTENTS

Scope

The policy applies to all employees, temporary employees, students, contractors, and consultants, and applies to all desktop devices, mobile devices, and shared devices, whether the devices are stand-alone or connected to the campus data network.

Policy Statement

Software on Devices

All devices must have a legally licensed and currently supported operating system. Exceptions must be approved by the Assistant Vice Chancellor for Information Technology.

Users can utilize any legally licensed software or app that helps accomplish business or academic goals. Software or apps cannot be installed or utilized unless the user explicitly trusts the source and knows a legal license exists.

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.

Vendor updates and patches for operating systems, software and apps must be installed on end-user devices, unless an exemption is granted by the Assistant Vice Chancellor for Information Technology.

Some classifications of software are expressly forbidden for security reasons. In general, users cannot 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 the Assistant Vice Chancellor for Information Technology for the following:

- Spyware is software that is used to gather sensitive information or to test for weaknesses in systems. It includes, but is not limited to, packet sniffers, port scanners, password cracking tools, key loggers, and vulnerability testers. ITS-approved spyware detection/removal software must be installed on all university-owned devices, if such software is available for the device.
- Malicious code, including viruses, worms, Trojan horses, and backdoors, is software that performs an unintended, and often unseen task when executed by an unsuspecting user. 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.
- Peer-to-peer file sharing software is used to share files with users over the network/Internet. Examples include 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.
- Ping sweeps are used to find devices that are active and being used. Port scans search for open ports that can be used to breach a network. This includes, but is not limited to, generic sweep, strobe, stealth, FTP bounce, Fragmented packet, SIN, FIN, TCP and UDP scans.

Information Technology Services staff 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 and asked to comply with this policy.

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

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. Each employee must ensure that all technology devices for which he/she is responsible comply with all security policies, guidelines, and procedures.

All end-user devices must be password protected where technically feasible.

Employees must use strong passwords that conform to the Password Policy. Certain high risk data, including Social Security Numbers, cannot be stored electronically unless an exemption to the Social Security Number Elimination/Usage Policy is granted by Information Technology Services and campus-approved encryption software is utilized for storing the high risk data. See the links in the Related Information section for the referenced policies.

Domain Membership

All Windows devices must be a member of the UNK Active Directory domain unless not technically feasible. Exceptions must be annually approved by the Assistant Vice Chancellor for IT.

Patching/Updating

All networked devices must have a device management program where technically feasible that handles patching and upgrading of software

Backups

If data is stored on a local device rather than a networked file server, the user must utilize a backup solution for the local device approved by Information Technology Services.

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. Record retention schedules are provided by the Division of Business & Finance.

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

High risk data must be properly removed from hardware devices prior to disposal of the device.

Remote Access/Network Connectivity

Remote users must comply with the UNK Network Services Policy. See the link in the Related Information section.

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.

Multifunctional Devices

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. An MFD must not be used to print, copy, fax, or scan high risk data unless the device is configured securely. See the Guidelines for Multifunctional Devices on the Network in the Related Information section for configuration requirements.

Physical Security

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

Mobile digital storage media cannot be used to store high risk data 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.

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

Enforcement

This policy is enforced by the Information Technology Services Security Team in coordination with Human Resources (staff) and/or Academic Affairs (Faculty). Failure to comply with this policy may result in disciplinary actions.

Reason for Policy

Administrative and academic business at UNK require end-user devices, including, but not limited to, desktop devices, mobile devices, and shared devices, such as printers and multifunction devices. Protection of these devices and the information handled by them is essential to conducting business at UNK.

Definitions

High Risk Data is data that must be protected by law or regulation. Data is classified as High Risk if UNK is required to self-report to the government and/or provide notice to the individual if the data is accessed inappropriately. The loss of confidentiality, integrity, or availability of High Risk Data could have a significant adverse impact on the mission, safety, finances, or reputation of the University of Nebraska at Kearney.

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.

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.

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.

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.

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.

Network is defined to be all UNK owned or managed internal infrastructure for converged services, including but not limited to, data, video and voice, to facilitate resource sharing and communication.

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

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.

Additional Contacts

Subject	***Contact***	***Phone***	***Email***
Questions	UNK Helpdesk	308-865-8363	unkhelpdesk@unk.edu

Related Information

Guidelines for the Use of Information Technology Resources at the University of Nebraska at Kearney

Responsible Use of University Computers and Information Systems (Executive Memorandum No. 16)

Guidelines for Multifunctional Devices (MFDs) on the Network

Guidelines for End User Devices on the Network

Network Services Policy (see http://www.unk.edu/policies)

Password Policy (see http://www.unk.edu/policies)

History

Reviewed and reformatted – November, 2016
Updated November, 2017 – Responsible University Administrator changed from Assistant Vice Chancellor-IT to Chief Information Officer