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

Network Services Policy

POLICY CONTENTS

Scope

The policy applies to all employees, contractors, consultants, temporary employees, students, and guests.

Policy Statement

Internet Service

Access to the Internet is a privilege granted to students, faculty, and staff, as well as contractors, consultants, and temporary employees. Since some services and resources can result in significant Internet and network traffic, this traffic is managed to control resource usage while meeting the educational needs of users, with priority for activities supporting the educational mission 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.

Security and Privacy

The network infrastructure on the UNK campus and within buildings, including the Museum of Nebraska Art, 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, or when the health or safety of people or property may be involved, or when required by legal obligations.

Network Administrators may 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.

Network Management

Only authorized Information Technology Services Staff may install, manage, or change the UNK network infrastructure and equipment. Unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse or theft of networking equipment is prohibited. In addition, UNK protects equipment belonging 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.

Only Information Technology Services Staff may install, configure, and/or use software that can evaluate, conduct host/port scans, compromise, or disrupt the production environment. Examples include tools that discover or “trap” passwords, identify security vulnerabilities, or intercept or copy information.

If a separate network is needed for research or a for a lab environment, the Director of Networking and IT Infrastructure will work with the department to design and install the network.

Installation of all data communications cabling and equipment must be approved by the Director of Networking and IT Infrastructure.

Private networks must be approved by the Assistant Vice Chancellor for Information Technology.

Installation of any IP-based applications, including audio and video, will be managed by Information Technology Services.

Remote Access

Remote access to UNK technology resources is granted by Information Technology Services via a VPN connection. Complete the Virtual Private Network Access Agreement and send to the UNK Security Team at childressa@unk.edu. See the link in the Related Information section.

Remote access requires two-factor authentication to minimize the potential exposure to UNK from damages that could result from unauthorized access to and/or use of UNK resources. Damages could include, but are not limited to, the loss of high risk or university confidential data, intellectual property, damage to public image, and damage to critical UNK internal systems.

All devices that connect to the UNK network via remote access must use the most up-to-date antivirus software. This includes personally-owned devices.

Personally-owned equipment that is used to connect to UNK's network must meet the requirements of UNK-owned equipment for remote access.

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.

Username and password cannot be shared with anyone. This includes family members.

General access to the Internet for recreational use by immediate household members through the UNK network is not allowed.

Direct access initiated from the Internet is not allowed to any device connected to the UNK network.

Anyone with remote access privileges must ensure that their device is not connected to any other network at the same time is it remotely connected to the UNK network, with the exception of personal networks that are under the control of the user.

Wireless Service

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

All wireless connectivity is managed by Information Technology Services.

All campus-installed wireless networks, including those not attached to the campus wired network infrastructure, must be reviewed and approved by the Director of Networking and IT Infrastructure.

Vendor contracts involving a vendor-supplied wireless solution must be reviewed by the Assistant Vice Chancellor for Information Technology prior to signing.

All vendor-supplied wireless solutions must be reviewed and approved by the Director of Networking and IT Infrastructure to ensure compatibility with other campus-installed wireless solutions.

Network equipment must be approved by the Director of Networking and IT Infrastructure for all authorized wireless networks. To facilitate support, ensure security, and prevent interference, the management of all authorized campus-installed wireless networks will be coordinated by Information Technology Services.

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

Information Technology Services may scan radio frequencies looking for unregistered wireless networks. If such a network is found, Information Technology Services will assist the owner 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 contacted to identify alternatives to eliminate the disruption.

All wireless networks must maintain compliance with all FCC regulations and guidelines

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

The University of Nebraska at Kearney provides networking services and facilities to support the educational mission of the campus. The data network and network infrastructure at the University of Nebraska at Kearney are critical to the operations of the campus and are essential to the daily activities of faculty, staff and students. This policy addresses network services, Internet traffic management, remote access, and wireless service.

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.

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.

The *internet* is all networks external to UNK.

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.

Networking equipment shall include all devices that allow computers or other devices 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.

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

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.

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

Two Factor Authentication is a process that requires a user to provide two methods of identification, typically something the user knows, such as a password or code, and something the user possesses, such as a card or a token.

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***
VPN	Andrea Childress		childressa@unk.edu
Networking	Brian Cox		Coxbl2@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)

Virtual Private Network Access Agreement

History

Initial Draft – November 3, 2016
Updated November, 2017 – Responsible University Administrator changed from Assistant Vice Chancellor-IT to Chief Information Officer