



Effective: April 1, 2016
Last Revised: November 27, 2017

Responsible University Office:
Information Technology Services

Responsible University Administrator:
Chief Information Officer

Policy Contact:
Deb Schroeder
schroederd@unk.edu

Guest Wireless Policy

POLICY CONTENTS

Scope
Policy Statement
Reason for Policy
Definitions
Additional Contacts
Related Information
History

Scope

This policy applies to the use of information, electronic and computing devices, and network resources on the entire computing network at UNK. All students, employees, guests, contractors, consultants, temporary, and other workers at UNK are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with UNK policies and standards, and local, state and federal laws and regulations.

This policy applies to students, guests, contractors, consultants, temporary employees, and other workers at UNK, including all personnel affiliated with third parties.

Policy Statement

General Use and Ownership

Any individual connected to the Guest Wireless Network in order to use it directly or to connect to any other network(s), must comply with this policy, the stated purposes and

acceptable use policies of any other network(s) or host(s) used, and all applicable laws, rules, and regulations.

THE UNIVERSITY OF NEBRASKA AT KEARNEY MAKES NO REPRESENTATIONS OR WARRANTIES CONCERNING THE AVAILABILITY OR SECURITY OF THE GUEST WIRELESS NETWORK, AND ALL USE IS PROVIDED ON AN AS-IS BASIS. BY USING THE GUEST WIRELESS NETWORK YOU AGREE TO DEFEND, INDEMNIFY, AND HOLD HARMLESS the University of Nebraska at Kearney FOR ANY LOSSES OR DAMAGES THAT MAY RESULT FROM YOUR USE OF THE GUEST WIRELESS NETWORK.

The University of Nebraska at Kearney takes no responsibility and assumes no liability for any content uploaded, shared, transmitted, or downloaded by you or any third party, or for anything you may encounter or any data that may be lost or compromised while connected to the Guest Wireless Network.

The University of Nebraska Kearney reserves the right to disconnect any user at any time and for any reason. The Guest Wireless Network is provided as a courtesy to allow our guests access to the internet. Users will not be given access to the University of Nebraska at Kearney intranet or permission to install any software on our computers.

The UNK network is a shared resource. Thus, network use or applications which inhibit or interfere with the use of the network by others are not permitted.

Forgery or other misrepresentation of one's identity via electronic or any other form of communication is prohibited.

Guests are responsible for any use of their wireless connectivity of personally-owned or personally-assigned devices.

UNK reserves the right to manage the use of the wireless spectrum within campus boundaries. Wireless devices that interfere with the operation of centrally-managed University systems must be disconnected when requested.

For security and network maintenance purposes, authorized individuals within UNK may monitor equipment, systems and network traffic at any time.

UNK reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

Unacceptable Use

Inappropriate use of the Guest Wireless Network is not permitted. This policy does not enumerate all possible inappropriate uses but rather presents some guidelines (listed below) that the University of Nebraska at Kearney may at any time use to make a determination that a particular use is inappropriate.

System and Network Activities

The following activities are strictly prohibited:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by UNK.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which UNK or the end user does not have an active license is strictly prohibited.
3. Accessing data, a server or an account for any purpose other than conducting UNK business, even if you have authorized access, is prohibited.
4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The Assistant Vice Chancellor for Information Technology or designee should be consulted prior to export of any material that is in question.
5. Introduction of malicious programs into the network or servers (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
6. Using a computing device to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
7. Making fraudulent offers of products, items, or services originating from any UNK account.
8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
9. Effecting security breaches or disruptions of network communication. "Disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
10. Port scanning or security scanning is expressly prohibited unless prior notification has been made and permission has been granted by the Director of Networking & IT Infrastructure or designee.
11. Executing any form of network monitoring which will intercept data not intended for the Guest's host.
12. Circumventing user authentication or security of any host, network or account.
13. Introducing honeypots, honeynets, or similar technology on the UNK network.
14. Interfering with or denying service to any user other than the guest's host (for example, denial of service attack).
15. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
16. Providing information about, or lists of, UNK students, employees or staff members to parties outside UNK.
17. Commercial or personal profit-making purposes or for personal benefit where such use incurs a cost to the University and is not academic or work related.

Email and Communication Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
4. Use of unsolicited email originating from within UNK's network of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by UNK or connected via UNK's network.

This policy is enforced by the Information Technology Services Security Team in coordination with the Director of Networking and IT Infrastructure and the Assistant Vice Chancellor for IT.

Reason for Policy

The purpose of this policy is to outline the acceptable use of the University of Nebraska at Kearney Guest Wireless network facilities and services. These rules are in place to protect the employee, student, staff member, guest and UNK. Inappropriate use exposes UNK to risks, including virus attacks, compromise of network systems and services, and legal issues.

Definitions

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.

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.

Additional Contacts

Subject	Contact	Phone	Email
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 \(Executive Memorandum No. 16\)](#)

History

Initial Draft - February, 2016

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