UNIVERSITY OF NEBRASKA AT OMAHA

# Wireless Access

## Scope

This policy applies to all users who connect to the university's wireless network.

## Policy Statement

### Supported Technology
The University of Nebraska Omaha (UNO) has standardized on the 802.11g/n/ac protocols for its wireless networks, transmitting on the 2.4 GHz and 5 GHz radio frequency spectrums with the intention of delivering Internet connectivity to wireless devices.

### Policy and Appropriate Use
All wireless access points connected to the UNO network must be approved and centrally managed by Information Technology Services (ITS). The addition of new wireless access points within campus facilities will be collaboratively planned among campus departments and managed by ITS. Non-sanctioned installation of wireless equipment or use of unauthorized equipment on campus premises is prohibited.

In the course of maintaining and securing the UNO network, ITS may conduct the following procedures at its own discretion:

- Restrict, queue, or prioritize traffic on the wireless network discretion to ensure the overall health of the service and security of technology, data, and information resources.
- Occasionally conduct scans of the wireless network to ensure there are no rogue access points present.
- Disable, without notice, any access point connected to the network that is suspected or proven to put the university's systems, data, and users at risk.

Any device or equipment found to be interfering with access point signals may be subject to relocation or removal, including cordless phones, microwave ovens, cameras, light ballasts, rogue access points, and similar devices. Wireless users agree to immediately report to Information Services any incident or suspected incidents of rogue access point installation.

## Reason for Policy

This policy is intended to protect the UNO's technology-based resources from unauthorized use and/or malicious attack that could result in loss of information, damage to critical applications, or damage to the university's public image, and to comply with the Payment Card Industry (PCI) standard for protecting cardholder data. All users connecting to university technology resources must adhere to university-defined processes for doing so and by using university-approved access points. Unauthorized access to the wireless network is not allowed.

## Procedures

Any questions relating to this policy or requests for exceptions should be directed to Information Services' Help Desk at [unohelpdesk@unomaha.edu](mailto:unohelpdesk@unomaha.edu). Some examples of approved exceptions include registered wireless devices for research, academic coursework, and student housing.

If any rogue access points are identified, Information Technology Services will request the owner remove the device from the network within three (3) business days. If the device is not removed, Information Technology Services will disable all network access to the rogue access point.

# Policy Enforcement

This policy is enforced by Information Technology Services in coordination with Human Resources and/or Academic Affairs. Failure to comply with this policy may result in suspension of wireless access privileges and possible disciplinary action.

## Definitions

**Wireless Network**: A type of network that uses wireless data connections, typically radio frequency, to connect clients. Wireless networks are defined by Service Set Identifiers (SSIDs) which are the unique human-readable name. UNO broadcasts three standard SSIDs: UNOGuest, UNOSecure, and eduroam.

**Wireless Access Point**: A wireless access point (WAP) or access point (AP) is a device allows wireless devices to connect to a wired network using 802.11 wireless protocols.

**Rogue Access Point**: A wireless access point not installed or approved by Information Technology Services on the UNO network. Rogue access points are prohibited.

## Related Information

[NU Executive Memorandum 16](#)
[NU Executive Memorandum 26](#)
[UNO Privacy Policy](#)

## History

This policy is an update to the Wireless Access Policy that was previously updated in 2015.

---