



Administrative Policy

2014-08 Information Security – Wireless Network

Title	Information Security – Wireless Network
Policy Owner and Contact Information	Chief Information Officer and EVP IT Security Website: https://health.uconn.edu/information-technology/
Applies to	UConn Health Employees, Business Associates, Students, Residents
Campus Applicability	UConn Health
Effective Date	6/2/2021

PURPOSE:

To ensure wireless network security and integrity, to protect the integrity of connected computing systems, and to minimize interference between wireless networks and other electronic resources deployed throughout UConn Health.

APPLIES TO:

This policy applies to all UConn Health Workforce, Business Associates, Non-Workforce, and all other individuals granted access to UConn Health electronic resources. The policy applies to all computing and networking equipment owned, leased, operated, or contracted by UConn Health.

POLICY STATEMENT:

1. UConn Health reserves the right to restrict the use of any and all wireless devices in UConn Health buildings and all outdoor spaces on UConn Health property, whether leased or owned.
2. UConn Health Information Technology (IT) must be consulted for coordination of engineering, installation, maintenance, and operation of wireless networks serving, or on any property owned or leased by, UConn Health.
3. Any independently installed wireless communications equipment, which has not been approved by UConn Health IT, is prohibited, subject to removal from service without notice, and may be confiscated.
4. All wireless network devices, including wireless access points/routers, building monitoring systems, classroom presentation/response systems, security systems, retail systems, and wireless research endeavors must be secured, in accordance with the *Wireless Network Device Secure Configuration Standards*.
5. All wireless access points that connect clients to the internal network shall require users to provide unique authentication.
6. Wireless access point device owners are responsible for updating software, hardware and firmware of devices to address security vulnerabilities.

7. The use of wireless networks at UConn Health shall be subject to all other policies and guidelines, as may be applicable

DEFINITIONS:

None

PROCEDURES/FORMS:

Wireless Network Device Secure Configuration Standards – (Restricted Access – Contact Information Security Office).

REFERENCES:

None

RELATED POLICIES:

None

ENFORCEMENT:

Violations of this policy or associated procedures may result in appropriate disciplinary measures in accordance with University By-Laws, General Rules of Conduct for All University Employees, applicable collective bargaining agreements, the University of Connecticut Student Code, other applicable University Policies, or as outlined in any procedures document related to this policy.

APPROVAL:

Andrew Agwunobi (Signed)
UConn Health Chief Executive Officer

6/2/2021

Kiki Nissen (Signed)
Administrative Policy Committee Vice-Chair

6/2/2021

Janel Simpson (Signed)
Administrative Policy Committee Chair

6/2/2021

POLICY HISTORY:

New Policy Approved: 11/18/14

Revised: 7/9/18

Reviewed without changes: 6/2/2021