	Policy Title	Guest Wireless Network
Weill Cornell Medicine	**Policy Number**	500.04
	Department	ITS Security
	Effective Date	October 1, 2007
	Last Reviewed	July 23, 2024
	Approved By	Tom Horton
	Approval Date	July 23, 2024

Policy

Weill Cornell Medicine supports the need for visitors to have access to the internet and relevant Weill Cornell Medicine resources.

Purpose

Guest wireless networks further Weill Cornell Medicine's missions of research, education, and patient care by providing a method for visitors to gain easy access to pertinent and topical information technology resources. This policy ensures guest networks are provisioned only by the Information Technologies & Services Department (ITS). This policy also establishes rules for proper management, security, and use of Weill Cornell Medicine's guest network.

Scope

Applies to all members of the Weill Cornell Medicine community who utilize Weill Cornell Medicine information technology resources. This includes Weill Cornell Medicine-Qatar and those responsible for managing and safeguarding Weill Cornell Medicine data.

Procedure

The following principles must be followed to ensure Weill Cornell Medicine's guest networks are made reasonably secure and prohibit unauthorized access to Weill Cornell Medicine resources.

1.01 Guest Wireless Network Design Principles

Guest wireless networks may be provisioned only by ITS. In provisioning guest wireless networks, ITS must ensure users of these networks are unable to create or bridge network connections from guest wireless networks to internal Weill Cornell Medicine IT resources on non-guest wireless networks.

Weill Cornell Medicine recognizes that users of guest networks expect a reasonable level of performance (e.g., responsive access to the internet). Managers and administrators of guest networks are required to provide a level of service consistent with these expectations but are not required to guarantee a particular quality of service.

Weill Cornell Medicine guest networks must be reasonably secure and restrictive while also providing necessary services. Reasonable restrictions may include, but are not limited to, minimizing access to specific networks, ports, applications, systems, or other public and/or ITS resources.

Guest wireless networks may be monitored and reviewed for unauthorized, suspicious, or malicious activity.

ITS is not expected to ensure security or privacy for devices and/or data on guest wireless networks. ITS is responsible for informing users of guest wireless networks that they should not expect a completely secure or private environment, and that use of the network is at their own risk.
When first connecting to Weill Cornell Medicine guest networks, users must be informed in writing (electronic or otherwise) of at least the following conditions:

- Communications may be monitored,
- Users should not have any reasonable expectation of security or privacy, and
- Users may be disconnected from the network if unauthorized, suspicious, or malicious activity is detected.

1.02 Unacceptable Use

Users of Weill Cornell Medicine guest networks may be disconnected for any reason. Disconnections may be ordered by any one or more of the following Weill Cornell Medicine officials or their designees:

- Associate Vice President, Deputy General Counsel and Secretary
- Chief Compliance and Privacy Officer
- Chief Information Security Officer
- Research Integrity Officer
- Senior Director, Human Resources Services
- Senior Associate Dean, Education
- Dean, Weill Cornell Graduate School of Medical Sciences

2. Individual Responsibilities

Informational text regarding the acceptable use of the Weill Cornell Medicine guest wireless networks must be posted and accepted by all users at the start of network usage. The text shall read as follows:

Thank you for choosing the Weill Cornell Medicine Guest Wireless Internet Access. This service was created to give visitors an easy way to browse the web. Before you connect, there are a few things you should know:

Clicking on the "I Agree" link below indicates you agree with the following Weill Cornell Medicine Guest Wireless Internet Access Terms and Conditions:

- This service provides limited wireless internet access for visitors to Weill Cornell Medicine.
- This wireless network is monitored. Computers suspected of distributing malicious software (spyware, malware, viruses, etc.), exhibiting malicious or suspicious behavior, or attempting to transmit data or other material that is considered offensive, illegal, in violation of copyright, or in violation of local, state, or federal law will be disconnected.

- Please do not attempt to use this service for high volume data transfers. Users found to be engaging in consistent, high volume data transfers will be disconnected.
- This wireless internet access is provided on an "as is" and "as available" basis. This service is not guaranteed to be uninterrupted, error-free, or free of viruses or other malware. Browse at your own risk.
- Internal Weill Cornell Medicine information technology resources are not available from this wireless network. If you are a Weill Cornell Medicine student, faculty member, staff member, or long-term affiliate in need of wireless access to internal Weill Cornell Medicine resources, please contact the Information Technologies and Services department by visiting https://its.weill.cornell.edu/get-help or calling +1 (212) 746-4878.
- Weill Cornell Medicine policy governs network use, including monitoring for the maintenance of operations, and obliges users to adhere to all applicable policies and laws, including fraud and abuse of network systems and copyright infringement.

If you agree with these terms and conditions, please click the box below. Thank you again for using the Weill Cornell Medicine Guest Wireless Internet Access.

Compliance with this Policy

All WCM Workforce Members are responsible for adhering to this policy. Failure to comply will be evaluated on a case-by-case basis and could lead to corrective action, up to and including termination, consistent with other relevant WCM and University Policies. Instances of non-compliance that potentially involve a lapse of professionalism may lead to engagement of the Office of Professionalism for evaluation and intervention.

Contact Information

Direct any questions about this policy, 500.04 – [Guest Wireless Network], to the Chief Information Security Officer, using one of the methods below:

• Office:	(646) 962-3609
• Email:	ciso@med.cornell.edu

Policy Approval

Version History

Date	**Author**	**Revisions**
October 1, 2007		Policy implemented
March 14, 2023	Brian J. Tschinkel	Updated policy template and language
July 2, 2024	Tom Horton	Updated language and contact information
July 11, 2024	Christine Klucznik	Updated policy template and language