Queens College Information Technology Standard	No: PR.MA.2.2 Remote Access
IT Standard: **Remote Access**	**Updated: 10/18/2022**
	Issued By: Queens College, Chief Information Security Officer **Owner: Queens College Information Technology Services**

1.0 Purpose and Benefits

The purpose of this standard is to establish authorized methods for remotely accessing resources and services securely.

Major security concerns with remote access include the lack of physical security controls, the use of unsecured networks, the connection of infected devices to internal networks, the availability of internal resources to external hosts, potential damage to resources, and unauthorized access to information.

2.0 Authority

- **Responsible Office(s):** Queens College Information Technology Services & Queens College General Counsel
- **Responsible Executive(s)**: General Counsel
- **Responsible Officer(s)**: Chief Information Security Officer

3.0 Scope

This is a college-wide policy and includes requirements that must be followed if Queens College is to protect the information that is collected in the standard process of business. This policy is to be an additional layer of security on top of existing CUNY security policies and is not intended or able to supersede CUNY policies.

This policy encompasses all systems, automated and manual, for which Queens College has administrative responsibility, including systems managed or hosted by third parties on behalf of Queens College. It addresses all information, regardless of the form or format, which is created or used in support of business activities.

4.0 Information Statement

Remote access is allowed when there is a clear, documented business need. Access may be allowed from entity-issued or personally-owned devices, at the discretion of the entity and in accordance with the standards below. Such access must be limited to only those systems necessary for needed functions.

4.1   Approved Methods of Remote Access

Approved methods of remote access to systems are listed in order of preference.

a. **Portals** - a server that offers access to one or more applications through a single centralized interface that provides authentication (e.g., web-based portal, virtual desktop interface (VDI)).

b. **Direct Application Access** – accessing an application directly with the application providing its own security (e.g., webmail, https).

c. **Remote System Control** – controlling a system remotely from a location other than the entity's internal network.

d. **Tunneling** - a secure communication channel through which information can be transmitted between networks (e.g., Virtual Private Network (VPN)).

4.2   Required Controls

a. Any method of remote access must use a centrally managed authentication system for administration and user access.

b. Devices and software used for remote access must be approved after review by the Information Security Officer/designated security representative. Blanket approvals may be provided based on this review.

c. The authentication token used for remote access must conform to the requirements of the appropriate assurance level.

d. Remote access sessions must require re-authentication after 30 minutes of inactivity.

e. Remote access sessions must not last any longer than 24 hours.

f. The entity must monitor for unauthorized remote connections and other anomalous activity and take appropriate incident response action as per the Cyber Incident Response Standard.

g. Tunneling specific controls:

   (a) Network controls regulating access to the remote access endpoint and between remote devices and networks are required.

   (b) When a remote access device will have access to other networked devices on the internal network, the remote device must be authenticated such that configuration of the device is compliant with applicable policies.

5.0 Compliance

This standard shall take effect upon publication. Compliance is expected with all enterprise policies and standards. Policies and standards may be amended at any time.

If compliance with this standard is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, entities shall request an exception through the Chief Information Security Officer's exception process.

6.0 Definitions of Key Terms

Term	Definition

7.0 Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at:
Aaron Wheeler
Aaron.Wheeler@qc.cuny.edu

8.0 Revision History

This standard shall be subject to periodic review to ensure relevancy.

Date	Description of Change	Reviewer
10/18/2022	Initial changes to apply to Queens College	DVogel
03/20/25	Added number convention and control title	AWheeler
	Policy Implemented	

9.0 Related Documents

[National Institute of Standards and Technology (NIST) Special Publication 800-46, Guide to Enterprise Telework and Remote Access Security](#)

[NIST Special Publication 800-113, Guide to SSL VPNs](#)

[NIST Special Publication 800-114, User's Guide to Securing External Devices for Telework and Remote Access](#)