

Queens College Technology Standard	No: QC-ITS-Cyber-020
Mobile Device Security Standard	Updated: 08/25/2023
	Issued By: Queens College, Office of Chief Information Security Officer
	Owner: Queens College Information Technology Services

1.0 Purpose and Benefits

Mobile devices often need additional protection because their nature generally places them at higher exposure to threats than other client devices that are only used within an entity’s facilities and on the entity’s networks. This standard outlines the additional protections required for the use of mobile devices.

2.0 Authority

- **Responsible Office(s):** Queens College Information Technology Services
- **Responsible Executive(s):** Chief Information Officer (CIO)
- **Responsible Officer(s):** Chief Information Security Officer (CISO)

3.0 Scope: College Wide

This is a college-wide standard 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 standard 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 standard 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

1. Mobile devices are computing devices in a small form factor that have at least one network connection interface, non-removable and/or removable storage, and is portable (i.e., non-stationary). These devices come in the forms such as:

smartphones, PDAs, smart watches, tablets, laptops, and wearable devices. Mobile devices must follow all requirements of the Information Security Policy.

2. As per the Encryption Standard, all mobile devices that access or contain any entity information must be encrypted.
3. For Queens College-issued mobile devices with direct access to managed networks, only those applications which are approved may be installed and or run on the mobile devices. Applications must be restricted through the use of whitelisting (preferable) or blacklisting. Applications must be digitally signed to ensure that only applications from trusted entities are installed on the device and that code has not been modified.
4. Queens College information must be removed or rendered inaccessible from mobile devices after no more than 10 incorrect authentication attempts.
5. Mobile devices must automatically lock after being idle for a period not to exceed 10 minutes.
6. Mobile devices which directly connect to managed private networks, virtually connect to managed private networks in a manner consistent with a directly connected device, or which contain or could contain information, including e-mail data, must be managed by a Mobile Device Management (MDM) or other centralized management solution.
7. Use of synchronization services, such as backups, for mobile devices (e.g., local device synchronization, remote synchronization services, and websites) must be controlled through an MDM or other centralized management solution.
8. Mobile devices may not access private networks unless their operating environment integrity is verified (including whether the device has been rooted/jailbroken).
9. Queens College must manage all mobile devices by:
 - a. Implementing device policies and configurations as appropriate to the use of the device.
 - b. Developing and implementing processes which check for upgrades and patches to the software components, and for appropriately acquiring, testing, and deploying the updates to entity issued devices.
 - c. Reconfiguring access control features as needed based on factors such as policy changes, technology changes, audit findings, and new security needs.
 - d. Detecting and documenting anomalies which may indicate malicious activity or deviations from policy and procedures. Anomalies should be reported to other systems' administrators as appropriate.
 - e. Providing training and awareness activities for mobile device users on threats and recommended security practices which can be incorporated into the entity's security and awareness training.

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; compliance with amended policies and standards is expected.

If compliance with this standard is not feasible or technically possible, or if deviation from this standard 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 standard owner at:

Chief Information Security Officer
Damon Vogel
CISO@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
08/25/2023	Conversion to Standard, Add #10, Alignment to Gartner Recommendations	DVogel

9.0 Related Documents

10.0 External Documents

[NIST Special Publication 800-124, Guidelines for Managing and Securing Mobile Devices in the Enterprise](#)

NIST Special Publication 800-164, Guidelines on Hardware-Rooted Security in Mobile Devices