Subject: Mobile Device Management Policy for Fordham University-Owned Devices

<table>
<thead>
<tr>
<th>Effective Date</th>
<th>Supersedes</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>January 15, 2016</td>
<td>June 18, 2013</td>
<td>1 of 3</td>
</tr>
</tbody>
</table>

**Purpose:**
To ensure secure, reliable and accountable issuance and use of University-owned mobile devices that access Fordham University data and to comply with federal and state laws and regulations governing privacy and security of information in the event of the loss or theft those devices.

**Scope:**
This policy applies to all University-owned “mobile devices”, which includes removable electronic storage devices (e.g., floppy disks, USB flash drives, and external hard drives) and portable communications and computing devices (e.g., laptops, tablets, PDAs, and cellphones) used by the Fordham University constituency in the performance of their duties and to all “Fordham University Data” when accessed through, or stored on, University owned mobile devices. Fordham University Data includes Fordham Protected Data and Fordham Sensitive Data, but not Fordham Public Data, as defined in the Data Classification Policy. This policy is necessary to preserve the confidentiality, integrity and availability of University data.

All University-owned mobile devices that access any University Data must comply with the policies described herein as well as those set forth in the Fordham IT Acceptable Use Policy and the Fordham Third Party Data Transfer Policy.

**Issuance of Fordham University-owned mobile electronic and storage**
- Mobile devices may be issued to employees of the University for demonstrated business purposes.
- All requests for mobile devices must be made in writing using the Mobile Device Agreement Form and approved by the budget administrator (Dean, Executive Director level or above) of the employee’s department or unit of the University according to procedures outlined.
- University-owned mobile devices must be returned upon request by the approving University department or unit budget administrator, upon leaving the department or unit, or when the device is no longer needed to conduct Fordham University business.
- Incidental use of University owned devices by employees is permitted for personal use provided that this use is otherwise in keeping with this Mobile Device Policy. However,
Subject: Mobile Device Management Policy for Fordham University-Owned Devices

<table>
<thead>
<tr>
<th>Effective Date</th>
<th>Supersedes</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>January 15, 2016</td>
<td>June 18, 2013</td>
<td>2 of 3</td>
</tr>
</tbody>
</table>

employees will be required to reimburse Fordham University for any personal or unauthorized usage that results in additional charges.

- All devices remain the property of Fordham University.

Terms and Conditions for accessing Fordham University data
Use of Fordham University-owned mobile devices that access University Data must comply with the following security measures. For assistance implementing these security requirements, users should contact IT Customer Care at 718-817-3999 or HelpIT@fordham.edu.

- All devices, where possible, must be secured using a PIN (4 digit minimum) or other password protection.
- All devices, where possible, must enable automatic lockout for idle devices for (5) five or fewer minutes.
- All devices, where possible, must have remote wipe capability installed and enabled.
- Any lost, stolen or compromised device must be reported to the IT Customer Care Center immediately at 718-817-3999.

Consistent with the purpose of protecting the integrity and security of Fordham University data, all users of mobile devices that access University Data will be subject to remote locking or data-wiping of lost, stolen, or otherwise compromised devices.

User Code of Conduct
All users of mobile devices that access University data are expected to take reasonable measures to protect the security and integrity of that data, including:

- taking adequate precautions to protect the physical security of the device.
- maintaining the software configuration of the device – both the operating system and applications installed.
- installing up-to-date and secure operating system and application software updates/patches.
- preventing the storage of Fordham University Data in unapproved applications on the device.
- ensuring the device’s security controls are not subverted via hacks, jailbreaks, security software changes and/or security setting changes.

This is a “Related Policy” as defined in section B of the “IT Policy Statement” section of the “Fordham IT Acceptable Use Policy”, which is at www.fordham.edu/itpolicy. In the event that IT Security and IT Risk Management protocols or procedures are published, any deviation may only be done in concert with the University Information Security Office with sufficient time to allow for appropriate risk analysis, documentation and possible presentation to authorized University representatives. Willful failure to adhere to published policy or protocol may be met with University sanctions.
Subject: Mobile Device Management Policy for Fordham University-Owned Devices

<table>
<thead>
<tr>
<th>Effective Date</th>
<th>Supersedes</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>January 15, 2016</td>
<td>June 18, 2013</td>
<td>3 of 3</td>
</tr>
</tbody>
</table>

- installation of current versions of virus and spyware detection/protection software along with personal firewall protection (where applicable.)
- backing up all data, settings, media and applications.
- installing mobile tracking and remote wipe software such as Lookout for Android, Find My iPhone for iOS devices or LoJack for Laptops.
- working with the University Information Security Office and the IT Customer Care Center to test and validate any configuration, application or settings.