### Desktop Remote Access Policy

<table>
<thead>
<tr>
<th>Effective Date</th>
<th>Supersedes</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>January 15, 2016</td>
<td>April 22, 2013</td>
<td>1 of 1</td>
</tr>
</tbody>
</table>

**Purpose:**
To properly control remote access to a University computer desktop from a remote location.

**Scope:**
All employees and faculty members with a University owned system that resides on a University controlled network.

- All persons needing remote access to their University desktop (e.g. to work from home, access from a conference, etc.) must use only University approved software that is installed by Fordham IT to remotely gain access to these systems.
- The current University standard remote desktop access software is LogMeIn, Pro or Free versions that is managed by Fordham IT.
- Any employee requesting remote access must have a Vice President, direct report to Vice President, or Dean’s approval to obtain and use this software.
- Requests for the use of this software cannot be self-approved. In the event that you are requesting this software installed on your computer and you are at the level in which you can approve installation of the software, that request will be approved by the IT Security Office.
- All employees are prohibited from installing remote access software on their desktops, unless specifically directed by Fordham IT. Examples of remote access software include, but are not limited to unauthorized copies of LogMeIn (both Free and Pro versions), GoToMyPC, any VNC application, and PCAnywhere.
- Fordham IT will remove any unauthorized remote desktop software installed on a University-owned system on a University controlled network.
- IT support functions, including but not limited to IT Customer Care, IT User Support, Law School IT and others are authorized to used remote access software in the course of performing their job functions without the authorization required by this policy, provided that the IT support department uses a tool that has been vetted and approved by the Office of IT Security and that tool is updated and maintained as required to ensure its security and integrity. The Office of IT Security reserves the right to require the removal of the software in the event that it is deemed to pose an unacceptable risk to the University.

*Fordham IT*

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/tpolicy. 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.