Subject: Anti Virus Policy

<table>
<thead>
<tr>
<th>Effective Date</th>
<th>Supersedes</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>January 15, 2016</td>
<td>February 1, 2011</td>
<td>1 of 1</td>
</tr>
</tbody>
</table>

**Purpose:**
With the increased reliance on Internet connectivity, anti-virus software is necessary to protect a computer against viruses, worms and other types of malicious code.

**Scope:**
This policy applies to all computers connected to the University network for the transmission of electronic communications. This includes computers situated behind firewalls or NAT devices that are connected to the University network or are using a Virtual Private Network (VPN).

- All Users (defined above) must install and maintain up-to-date anti-virus software.
- The University standard anti-virus software is Symantec Anti Virus (part of the Symantec Client Security product suite); this software is provided without cost to all members of the Fordham community.
- To obtain a copy of anti-virus software, please call IT Customer Care at 718-817-3999 (internal extension 3999) or e-mail HelpIT@fordham.edu.
- While Symantec Anti Virus is provided to the University community at no cost, departments or individuals who choose to use other anti-virus solutions should refer to the documentation provided with the software they have chosen and are responsible for maintaining and updating the software they have installed. All users are required to configure the anti-virus software so that the software automatically updates virus definitions daily. Regardless of anti-virus product that you install, you may not: uninstall or disable the product for any reason.

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](http://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.