Subject: Third Party Data Transfer Policy

<table>
<thead>
<tr>
<th>Effective Date</th>
<th>Supersedes</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>January 15, 2016</td>
<td>September 1, 2009</td>
<td>1 of 2</td>
</tr>
</tbody>
</table>

Purpose:
To secure Fordham University data that is transferred or transmitted between Fordham University controlled systems and non-Fordham University controlled systems.

Scope:
Any user or department that transfers or transmits University data to or from a system outside the administrative control of Fordham University is bound by this policy.

"Fordham University data" or "University data" means and includes all information, documents and things containing Fordham University's proprietary or confidential information or designated by Fordham University as proprietary and confidential.

- All transfers or transmission of data, to or from Fordham University to an external third party, vendor or system must be reviewed by the office of IT Risk and Integrity and approved prior to the transfer or transmission.
- To receive approval, the requestor must provide the following information via e-mail to datatransfer@fordham.edu:
  - The corporate name of the outside party and all individuals at the third party corporation that may have access to Fordham University data, or if to an individual, the individual's name, title and contact information.
  - The specific data elements that will be transferred between Fordham University and the third party (including but not limited to: Social Security numbers, credit card numbers, family information, financial information, health records, other personally identifiable information, etc.)
  - The method of transfer (including but not limited to: SFTP, VPN, HTTPS, etc.) and all security measures taken or to be implemented to ensure a secure transfer or transmission.
- The purpose of the transfer or transmission.
- Any external vendor that stores University data must have a signed contract with Fordham University. This contract must be approved by Fordham University's Legal

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: Third Party Data Transfer Policy

<table>
<thead>
<tr>
<th>Effective Date</th>
<th>Supersedes</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>January 15, 2016</td>
<td>September 1, 2009</td>
<td>2 of 2</td>
</tr>
</tbody>
</table>

Department prior to any transfer or transmission of University data. The Fordham University Legal Department must confirm that the proper legal protections and requirements for confidentiality are in place prior to execution of any such contract.

- Any protocol that transmits credentials in “clear text” (including but not limited to: FTP, TELNET or HTTP) is strictly prohibited.
- Any protocol that transmits data in “clear text” may be used, based upon the sensitivity of the data that is transmitted as defined by the Data Owner responsible for the data in question. The office of IT Risk and Integrity will have final approval process of these protocols for specific applications on a case-by-case basis.

---

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.