



## **Contract Language for the Secure Handling of NU Data V1.0**

### **Secure Protection and Handling of Data**

1. Network Security. Vendor agrees at all times to maintain network security that – at a minimum – includes: network firewall provisioning, intrusion detection, and regular third party penetration testing. Likewise Vendor agrees to maintain network security that conforms to one of the following:
  - a. Those standards that Northwestern applies to its own network, as found at <http://www.it.northwestern.edu/policies/network/index.html> and elsewhere;
  - b. Current standards set forth and maintained by the National Institute of Standards and Technology, including those at:  
<http://checklists.nist.gov/repository/1023.html> and  
<http://checklists.nist.gov/repository/>; or
  - c. Any generally recognized comparable standard that Vendor then applies to its own network.
2. Data Security. Likewise, Vendor agrees to protect and maintain the security of data with protection that is at least good as or better than that maintained by Northwestern. These security measures include maintaining secure environments that are patched and up to date with all appropriate security updates as designated, for example, by Microsoft notification.
3. Data Transmission. Vendor agrees that any and all transmission or exchange of system application data with Northwestern and/or any other parties expressly designated by Northwestern – solely in accordance with Section 6 below -- shall take place via secure means, e.g. HTTPS or FTPS.
4. Data Storage. Vendor also agrees that any and all Northwestern data will be stored, processed, and maintained solely on designated target servers and that no Northwestern data at any time will be processed on or transferred to any portable or laptop computing device or any portable storage medium, unless that storage medium is in use as part of the Vendor's designated backup and recovery processes.
5. Data Encryption. Vendor agrees to store all Northwestern backup data as part of the its designated backup and recovery processes in encrypted form, using no less than 128 bit key.
6. Data Re-Use. Vendor agrees that any and all data exchanged shall be used expressly and solely for the purposes enumerated in the Current Agreement and this Third Addendum. Data shall not be distributed, repurposed or shared across

other applications, environments, or business units of Vendor. Vendor further agrees that no Northwestern data of any kind shall be transmitted, exchanged or otherwise passed to other vendors or interested parties except on a case-by-case basis as specifically agreed to in writing by the Northwestern Project Manager as designated in Section To Come

7. End of Agreement Data Handling. The Vendor also agrees that upon termination of this Agreement it shall erase, destroy, and render unreadable all Northwestern data according to the standards enumerated in D.O.D. 5015.2 and certify in writing that these actions have been complete within 30 days of the termination of this Agreement or within 7 days of the request of an agent of Northwestern, whichever shall come first.
8. Vendor agrees to comply with all applicable laws that require the notification of individuals in the event of unauthorized release of personally-identifiable information or other event requiring notification. In the event of a breach of any of Vendor's security obligations or other event requiring notification under applicable law ("Notification Event"), Vendor agrees to assume responsibility for informing all such individuals in accordance with applicable law and to indemnify, hold harmless and defend Northwestern and its trustees, officers, and employees from and against any claims, damages, or other harm related to such Notification Event.