# Northwestern University - Information Security Addendum

**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 (three or more annually) third party vulnerability assessments. Likewise, Vendor agrees to maintain network security that conforms to generally recognized industry standards (see "11. Industry Standards") and best practices that Vendor then applies to its own network.

2. Application Security.
Vendor agrees at all times to provide, maintain and support its Software and subsequent updates, upgrades, and bug fixes such that the Software is, and remains secure from those vulnerabilities as described in:
a) The Open Web Application Security Project's (OWASP) "Top Ten Project" - see http://www.owasp.org; or
b) The CWE/SANS Top 25 Programming Errors - see http://cwe.mitre.org/top25/ or http://www.sans.org/top25-programming-errors/; or
c) Other generally recognized and comparable industry practices or standards.

3. Data Security.
Vendor agrees to preserve the confidentiality, integrity and accessibility of Northwestern data with administrative, technical and physical measures that conform to generally recognized industry standards (see "11. Industry Standards") and best practices that Vendor then applies to its own processing environment. Maintenance of a secure processing environment includes but is not limited to the timely application of patches, fixes and updates to operating systems and applications as provided by vendor or open source support.

4. Data Storage.
Vendor 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 device or storage medium is in use as part of the Vendor's designated backup and recovery processes and encrypted in accordance with "6. Data Encryption".

5. Data Transmission.
Vendor agrees that any and all electronic transmission or exchange of system and application data with Northwestern and/or any other parties expressly designated by Northwestern shall take place via secure means (using HTTPS or SFTP or equivalent) and solely in accordance with "7. Data Re-Use".

6. Data Encryption.
Vendor agrees to store all Northwestern backup data as part of its designated backup and recovery processes in encrypted form, using a commercially supported encryption solution. Vendor further agrees that any and all Northwestern data defined as personally identifiable information under current legislation or regulations stored on any portable or laptop computing device or any portable storage medium be likewise encrypted. Encryption solutions will be deployed with no less than a 128-bit key

for symmetric encryption and a 1024 (or larger) bit key length for asymmetric encryption.

7. 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 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 Northwestern University.

8. End of Agreement Data Handling.
Vendor agrees that upon termination of this Agreement it shall erase, destroy, and render unrecoverable all Northwestern data and certify in writing that these actions have been completed 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. At a minimum, a "Clear" media sanitization is to be performed according to the standards enumerated by the National Institute of Standards, Guidelines for Media Sanitization, SP800-88, Appendix A - see http://csrc.nist.gov/.

9. Security Breach Notification.
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, Vendor agrees to:

a. Notify Northwestern by telephone and e-mail of such an event within 24 hours of discovery, and
b. Assume responsibility for informing all such individuals in accordance with applicable law, and
c. 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.

10. Right to Audit
Northwestern University or an appointed audit firm (Auditors) has the right to audit the Vendor and the Vendor's sub-vendors or affiliates that provide a service for the processing, transport or storage of Northwestern University's data. Northwestern University will announce their intent to audit the Vendor by providing at a minimum two weeks (10 business days) notice to the Vendor. This notice will go to the Vendor that this contract is executed with. A scope document along with a request for deliverables will be provided at the time of notification of an audit. If the documentation requested cannot be removed from the Vendor's premises, the Vendor will allow the Auditors access to their site. Where necessary, the Vendor will provide a personal site guide for the Auditors while on site. The Vendor will provide a private accommodation on site for data analysis and meetings; the accommodation will allow for a reasonable workspace, with appropriate lighting, electrical, a printer and Internet connectivity. The Vendor will make necessary employees or contractors available for interviews in person or on the phone during the time frame of the audit. In lieu of Northwestern or its appointed audit firm performing their own audit, if the Vendor has an external audit firm that performs a certified Type II SAS 70 review, Northwestern has the right to review the controls tested as well as the results, and has the right to request additional controls to be added to the certified Type II SAS 70 review for testing the controls that have an impact on Northwestern data. Audits will be at Northwestern University's sole expense, except where the audit reveals material noncompliance with contract specifications, in which case the cost will be borne by the vendor.

11. Industry Standards

Generally recognized industry standards include but are not limited to the current standards and benchmarks set forth and maintained by the:

a. Center for Internet Security - see http://www.cisecurity.org
b. Payment Card Industry/Data Security Standards (PCI/DSS) - see http://www.pcisecuritystandards.org/
c. National Institute for Standards and Technology - see http://csrc.nist.gov
d. Federal Information Security Management Act (FISMA) - see http://csrc.nist.gov
e. ISO/IEC 27000-series - see http://www.iso27001security.com/
f. Organization for the Advancement of Structured Information Standards (OASIS) - see http://www.oasis-open.org/

12. Vendor Warranty

Vendor (i) warrants that the services provided in this agreement will be in substantial conformity with the information provided in Vendor's [**Insert Security Provider Security Assessment Questionnaire Completed Date**] response to the Northwestern University Service Provider Security Assessment questionnaire ("Response to NUSPSAQ"); (ii) agrees to inform Northwestern promptly of any material variation in operations from that reflected in the Response to NUSPSAQ; and (iii) agrees that any material deficiency in operations from those as described in the Response to NUSPSAQ will be deemed a material breach of this agreement.