Data Security Addendum

Data Security Addendum between (Vendor)

and Virginia Polytechnic Institute and State University (Virginia Tech or University)

This Addendum supplements the

Between Virginia Tech and Vendor. It is applicable only in those situations where Vendor will provide the following Services (as defined below):

to Virginia Tech (if applicable, pursuant to a University purchase order (PO), that necessitates Vendor create, obtain, transmit, use, maintain, process, or dispose of University Data (as defined in the Definitions Section of this Addendum) in order to fulfill its obligations to Virginia Tech. As used herein, the term Agreement means the Vendor document referenced above, this Addendum and, if applicable, the Virginia Tech purchase order.

This Addendum sets forth the terms and conditions pursuant to which University Data will be protected by Vendor during the term of the parties' Agreement and after its termination.

Definitions

a. Brand Features – means the trade names, trademarks, service marks, logos, domain names, and other distinctive brand features of each party, respectively, as secured by such party from time to time.
b. End User – means the individuals authorized by University to access and use the Services provided by Vendor under the Agreement.
c. Personally Identifiable Information – includes but is not limited to: personal identifiers such as name, address, phone number, date of birth, Social Security number, email address, student or personnel identification number, and non-directory information as that term is defined in the Family Educational Rights and Privacy Act (FERPA), 20 USC 1232g, personal information as defined in the Virginia Code, section 18.2-186.6 and/or any successor laws of the Commonwealth of Virginia; personally identifiable information contained in student education records as that term is defined in Family Educational Rights and Privacy Act, 20 USC 1232g; medical information as defined in Virginia Code Section 32.1-127.1:05; protected health information as that term is defined in the Health Insurance Portability and Accountability Act, 45 Code of Federal Regulations (CFR) Part 160.103; nonpublic personal information as that term is defined in the

Gramm-Leach-Billey Financial Modernization Act of 1999, 15 USC 6809; credit and debit card numbers and/or access codes other than cardholder data and sensitive authentication data as those terms are defined in the Payment Card Industry Data Security Standards; other financial account numbers, access codes, driver's license number; and state or federal identification numbers such as passport, visa, or state identity card numbers.

d. Securely Destroy – means taking actions that render data written on media unrecoverable by both ordinary and extraordinary means. These actions must meet of exceed those sections of the National Institute of Standards and Technology (NIST) SP 800-53 Rev. 5 guidelines relevant to data categorized as high security.
e. Security Breach – means a security relevant event in which the security of a system or procedure used to create, obtain, transmit, maintain, use, process, store, or dispose of data is breached, and in which University Data is exposed to unauthorized disclosure, access, alteration, or use.
f. Services – means any goods or services acquired by University from Vendor.
g. University Data – includes all Personally Identifiable Information (PII) and other information that is not intentionally made generally available by University on public websites, including but not limited to business, administrative and financial data, intellectual property, and patient, student, and personnel data.

Applicability to Other Agreements

University and Vendor acknowledge there may be future agreements between the parties, including purchase orders, where Vendor will obtain University Data (Other Agreements) and may contain confidentiality and security provisions of a similar nature as set forth in this Addendum. The parties agree that, to the extent of any conflict between the terms of this Addendum and the terms of Other Agreements, the terms of this Addendum will control. The terms and conditions of this Addendum will apply to Vendor with respect to any performance applicable or relevant to Other Agreements. The terms of this Addendum will apply to Vendor's obligation to keep and safeguard University Data.

Rights and License in and to University Data

The parties agree that as between them, all rights, including all intellectual property rights, in and to University Data will remain the exclusive property of University, and Vendor has a limited, nonexclusive license to use the data as provided in the Agreement solely for the purpose of performing its obligations hereunder. The Agreement does not give a party any

rights, implied or otherwise, to the other's data, content, or intellectual property, except as expressly stated in the Agreement.

Data Privacy

a. Vendor will use University Data only for the purpose of fulfilling its duties under the Agreement and will not share such data with or disclose it to any third party without the prior written consent of University, except as required by the Agreement or as otherwise required by law.
b. Vendor may not store University Data outside the United States without prior written consent from University.
c. Vendor will provide access to University Data only to its employees and subcontractors who need to access the data to fulfill Vendor obligations under the Agreement. Vendor will ensure that employees who perform work under the Agreement have read, understood, and received appropriate instruction as to how to comply with the data protection provisions of the Agreement.
d. If Vendor will have access to University's education records, as defined under the Family Educational Rights and Privacy Act (FERPA). Vendor acknowledges that for the purposes of the Agreement it will be designated as a school official with legitimate educational interests in University education records, as those terms have been defined under FERPA and its implementing regulations, and Vendor agrees to abide by the limitations and requirements imposed on school officials. Vendor will use the education records only for the purpose of fulfilling its duties under this Agreement for University's and its End Users' benefit and will not share such data with or disclose it to any third party except as provided for in the Agreement, required by law, or authorized in writing by University.

Data Security

a. Vendor will store and process University Data in accordance with commercial best practices, including appropriate administrative, physical, and technical safeguards, to secure such data from unauthorized access, disclosure, alteration, and use. Such measures will be no less protective than those used to secure Vendor's own data of a similar type, and in no event less than reasonable in view of the type and nature of the data involved. Without limiting the foregoing, Vendor warrants that all electronic University Data will be encrypted in transmission (including via web interface) and at rest in accordance with latest version of National Institute of Standards and Technology Special Publication 800-53, Rev. 5 (specifically, SC-28, Protection of Information at Rest, and SC-8, Transmission Confidentiality and Integrity). Vendor will be prepared to modify

or increase data security safeguards when notified by University of changes to Information Technology (IT) security compliance requirements for specific elements of University Data.

b. Vendor will use industry-standard and up-to-date security tools and technologies such as anti-virus protections and intrusion detection methods in providing Services under this Agreement.

Employee Background Checks and Qualifications

Vendor will ensure that its employees have passed reasonable and appropriate background screening and possess all needed qualifications and training to comply with the terms of this Addendum including, but not limited to, all terms relating to data and intellectual property protection.

Data Authenticity and Integrity

Vendor will take reasonable measures, including audit trails, to protect University Data against deterioration or degradation of data quality and authenticity. Vendor will be responsible for ensuring that University Data, per the Virginia Public Records Act, is preserved, maintained, and accessible throughout their lifecycle, including converting and migrating electronic data as often as necessary so that information is not lost due to hardware, software, or media obsolescence or deterioration.

Security Breach

a. Response. Immediately upon becoming aware of a Security Breach, or of circumstances that could have resulted in unauthorized access to or disclosure or use of University Data, Vendor will notify University, fully investigate the incident, and cooperate fully with University's investigation of and response to the incident. Except as otherwise required by law, Vendor will not provide notice of the incident directly to individuals whose Personally Identifiable Information was involved, regulatory agencies, or other entities, without prior written permission from University.

b. Liability. In addition to any other remedies available to the University under law or equity, Vendor will reimburse University in full for all costs incurred by University in investigation and remediation of such Security Breach, including but not limited to providing notification to individuals whose Personally Identifiable Information was compromised and to regulatory agencies or other entities as required by law or contract; providing one year's credit monitoring to the affected individuals if the Personally Identifiable Information exposed during the breach could be used to commit

financial identity theft; and the payment of legal fees, audit costs, fines, and other fees imposed by regulatory agencies or contracting partners as a result of the Security Breach.

Response to Legal Orders, Demands, or Requests for Data

a. Except as otherwise expressly prohibited by law, Vendor will:
   - Immediately notify University of any subpoenas, warrants, or other legal orders, demands, or requests received by Vendor seeking University Data;
   - Consult with University regarding its response;
   - Cooperate with University's reasonable requests in connection with efforts by University to intervene and quash or modify the legal order, demand, or request; and
   - Upon University's request, provide University with a copy of its response.

b. If University receives a subpoena, warrant, or other legal order, demand (including request pursuant to the Virginia Freedom of Information Act (FOIA)) or request seeking University Data maintained by Vendor, University will promptly provide a copy to Vendor. Vendor will promptly supply University with copies of data required for University to respond and will cooperate with University's reasonable requests in connection with its response.

Data Transfer Upon Termination or Expiration

a. Upon termination or expiration of the Agreement, Vendor will ensure that all University Data are securely returned or destroyed as directed by University in its sole discretion. Transfer to University or a third party designated by University will occur within a reasonable period of time, and without significant interruption in Services. Vendor will ensure that such transfer/migration uses facilities and methods that are compatible with the relevant systems of University or its transferee, and to the extent technologically feasible, that University will have reasonable access to University Data during the transition. In the event University requests destruction of its data, Vendor agrees to Securely Destroy all data in its possession and in the possession of any subcontractors or agents to which Vendor might have transferred University Data. Vendor agrees to provide documentation of data destruction to University.

b. Vendor will notify University of impending cessation of its business and any contingency plans. This includes immediate transfer of any previously escrowed assets and data and providing University access to Vendor's facilities to remove and destroy University-

owned assets and data. Vendor will implement its exit plan and take all necessary actions to ensure a smooth transition of Services with minimal disruption to University. Vendor will also provide a full inventory and configuration of servers, routers, other hardware, and software involved in service delivery along with supporting documentation, indicating which if any of these are owned by or dedicated to University. Vendor will work closely with its successor to ensure a successful transition to the new equipment, with minimal downtime and effect on University, all such work to be coordinated and performed in advance of the formal, final transition date.

Audits

a. University reserves the right, in it sole discretion, to perform audits of Vendor, at University's expense, to ensure compliance with the terms of this Addendum. Vendor will reasonably cooperate in the performance of such audits. This provision applies to all agreements under which Vendor must create, obtain, transmit, use, maintain, process, or dispose of University Data.

b. If Vendor must, under the Agreement, create, obtain, transmit, use, maintain, process, or dispose of the subset of University Data known as Personally Identifiable Information or financial or business data which has been identified to Vendor as having the potential to affect the accuracy of University's financial statements, Vendor will, at its expense, conduct of have conducted at least annually a/n:

- American Institute of CPAs Service Organization Controls (SOC) Type II audit, or other security audit with audit objectives deemed sufficient by University, which attests Vendor's security policies, procedures, and controls;
- Vulnerability scan, performed by a scanner approved by University, of Vendor's electronic systems and facilities that are used in any way to deliver electronic services under this Agreement; and
- Formal penetration test, performed by a process and qualified personnel approved by University, of Vendor's electronic systems and facilities that are used in any way to deliver electronic Services under the Agreement.

Additionally, upon request, Vendor will provide University the results of the above audits, scans, and tests and will promptly modify its security measures as needed based on those results to meet obligations under this Addendum. University may require, at University's expense, Vendor to perform additional audits and tests, the results of which will be provided promptly to University.

Institutional Branding

Each party will have the limited right to use the other party's Brand Features only in connection with performing the functions provided in the Agreement, after the other party's review of the intended use of the Brand Features and in accordance with that party's trademark identity and guidelines. Any use of a party's Brand Features will ensure the benefit of the party holding intellectual property rights in and to those features.

Compliance

a. Vendor will comply with all applicable laws and industry standards in performing Services under this Addendum. Any Vendor personnel visiting University's facilities will comply with all applicable University policies regarding access to, use of, and conduct within such facilities. University will provide copies of such policies to Vendor upon request.
b. Vendor warrants that the Services it will provide to University are fully compliant with and will enable University to be compliant with relevant requirements of all laws, regulations, and guidance applicable to University and/or Vendor, including but not limited to: the Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), Health Information Technology for Economic and Clinical Health Act (HITECH), Gramm-Leach-Billey Financial Modernization Act (GLB), Payment Card Industry Data Security Standards (PCI-DSS), Americans with Disabilities Act (ADA), Federal Export Administration Regulations (EAR), and Defense Federal Acquisition Regulation Supplement (DFAR).
c. If the Payment Card Industry Data Security Standards (PCI-DSS) are applicable to Vendor Services provided to University, Vendor will furnish proof of compliance with PCI-DSS within ten (10) business days of University's written request.

Indemnity

Vendor will indemnify, defend, and hold University harmless from all claims, liabilities, damages, or judgments involving a third party, including University's costs and attorneys' fees, which arise because of Vendor's failure to meet any of its obligations under this Addendum.

No End User Agreements

This Agreement is the entire agreement between University (including University employees and other End Users) and Vendor. In the event Vendor enters into terms of use agreements or other agreements or understandings, whether electronic, click-through, verbal or in writing,

with University employees or other End Users, such agreements will be null, void, and without effect, and the terms of the Agreement will apply.

Survival

Vendor's obligations under Section 10 will survive termination of the Agreement until all University Data has been returned or Securely Destroyed.

In Witness Whereof, this Addendum has been executed by an authorized representative of each party as of the date set forth beneath such party's designated representative's signature.

By:

Title:

Date:

Virginia Tech

By:

Title:

Date: