Data Protection and Incident Response

1. Definitions:
    a. "End User" means the individuals authorized by Virginia Tech (the "University") to access and use the Services provided by the Selected Firm/Vendor under this agreement.
    b. "Personally Identifiable Information" includes but is not limited to: personal identifiers such as name, address, phone number, date of birth, Social Security number, and student or personnel identification number; "personal information" as defined in Virginia Code section 18.2-186.6 and/or any successor laws of the Commonwealth of Virginia as well as the University's IT Security Office's policy for Protecting Sensitive Data; personally identifiable information contained in student education records, as that term is defined in the 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 CFR Part 160.103; nonpublic personal information as that term is defined in the Gramm-Leach-Bliley Financial Modernization Act of 1999, 15 USC 6809; credit and debit card numbers and/or access codes and other 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 numbers; and state- or federal-identification numbers such as passport, visa or state identity card numbers.
    c. "Securely Destroy" means taking actions that render data written on physical (e.g., hardcopy, microfiche, etc.) or electronic media unrecoverable by both ordinary and extraordinary means. These actions must meet or exceed those sections of the National Institute of Standards and Technology (NIST) SP 800-88r1 guidelines relevant to data categorized as high security.
    d. "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.
    e. "Services" means any goods or services acquired by Virginia Tech from the Selected Firm/Vendor.
    f. "University Data" includes all Personally Identifiable Information and other information that is not intentionally made generally available by the University on public websites or publications, including but not limited to business, administrative and financial data, intellectual property, and patient, student and personnel data.
2. Rights and License in and to the University Data: The parties agree that as between them, all rights including all intellectual property rights in and to University Data shall remain the exclusive property of the University, and Selected Firm/Vendor has a limited, nonexclusive license to use these data as provided in this agreement solely for the purpose of performing its obligations hereunder. This 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.
3. Data Privacy:
    a. Selected Firm/Vendor will use University Data only for the purpose of fulfilling its duties under this agreement and will not share such data with or disclose it to any third party without the prior written consent of the University, except as required by this agreement or as otherwise required by law. In the case data is moved off shore (outside the US) then the University will be notified within 30 days before it happens so that the University can take action if the University deems necessary.

b. Selected Firm/Vendor will provide access to University Data only to its employees and subcontractors who need to access the data to fulfill Selected Firm/Vendor obligations under this agreement. Selected Firm/Vendor will ensure that employees and subcontractors who perform work under this agreement have read, understood, received appropriate instruction on how to comply with, and agreed to the data protection provisions of this agreement.
c. The following provision applies only if Selected Firm/Vendor will have access to the University's education records as defined under the Family Educational Rights and Privacy Act (FERPA): The Selected Firm/Vendor acknowledges that for the purposes of this agreement it will be designated as a "school official" with "legitimate educational interests" in the University education records, as those terms have been defined under FERPA and its implementing regulations, and the Selected Firm/Vendor agrees to abide by the limitations and requirements imposed on school officials. Selected Firm/Vendor will use the education records only for the purpose of fulfilling its duties under this agreement for University's and its End User's benefit, and will not share such data with or disclose it to any third party except as provided for in this agreement, required by law, or authorized in writing by the University.

4. Data Security:
    a. Selected Firm/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 Selected Firm/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, Selected Firm/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 (specifically, SC-28, Protection of Information at Rest, and SC-8, Transmission Confidentiality and Integrity). Selected Firm/Vendor will be prepared to modify or increase data security safeguards when notified by the University of changes to IT security compliance requirements for specific elements of University data.
    b. Selected Firm/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.
5. Employee Background Checks and Qualifications: Selected Firm/Vendor shall ensure that its employees (and any subcontractor's employees) who will have potential access to University Data have passed appropriate, industry standard, background screening and possess the qualifications and training to comply with the terms of this agreement.
6. Data Authenticity and Integrity: Selected Firm/Vendor will take reasonable measures, including audit trails, to protect University Data against deterioration or degradation of data quality and authenticity. The Selected Firm/Vendor will be responsible during the term of this agreement, unless otherwise specified elsewhere in this agreement, for converting and migrating electronic data as often as necessary so that information is not lost due to hardware, software, or media obsolescence or deterioration.

7. Security Breach:
    a. Response. Upon becoming aware of a Security Breach, or of circumstances that are reasonably understood to suggest a likely Security Breach, Selected Firm/Vendor shall notify the University within 7 business days, fully investigate the incident, and cooperate fully with the University's investigation of and response to the incident. Except as otherwise required by law, Selected Firm/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 the University.
    b. Liability:
        i. If Selected Firm/Vendor must under this agreement create, obtain, transmit, use, maintain, process, or dispose of the subset of University Data known as Personally Identifiable Information, the following provisions apply. In addition to any other remedies available to the University under law or equity, Selected Firm/Vendor will reimburse the University in full for all costs incurred by the University in investigation and remediation of any Security Breach caused by Selected Firm/vendor, 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.
        ii. If Selected Firm/Vendor will NOT under this agreement create, obtain, transmit, use, maintain, process, or dispose of the subset of University Data known as Personally Identifiable Information, the following provisions apply. In addition to any other remedies available to the University under law or equity, Selected Firm/Vendor will reimburse the University in full for all costs reasonably incurred by the University in investigation and remediation of any Security Breach caused by Selected Firm/vendor.
8. Response to Legal Orders, Demands or Requests for Data:
    a. Except as otherwise expressly prohibited by law, Selected Firm/Vendor will:
        i. immediately notify the University of any subpoenas, warrants, or other legal orders, demands or requests received by Selected Firm/Vendor seeking University Data;
        ii. consult with the University regarding its response;
        iii. cooperate with the University's reasonable requests in connection with efforts by the University to intervene and quash or modify the legal order, demand or request; and
        iv. upon the University's request, provide the University with a copy of its response.
    b. If the University receives a subpoena, warrant, or other legal order, demand (including request pursuant to the Virginia Freedom of Information Act), or request seeking University Data maintained by Selected Firm/Vendor, the University will promptly provide a copy to Selected Firm/Vendor. Selected Firm/Vendor will promptly supply the University with copies of data required for the University to respond, and will cooperate with the University's reasonable requests in connection with its response.
9. Data Transfer Upon Termination or Expiration:
    a. Upon termination or expiration of this agreement, Selected Firm/Vendor will ensure that all University Data are securely returned or destroyed as directed by the University in its sole

discretion. In the event that the University requests destruction of University Data, Selected Firm/Vendor agrees to Securely Destroy all University Data in its possession and in the possession of any subcontractors or agents to which the Selected Firm/Vendor might have transferred University Data. The Selected Firm/Vendor agrees to provide documentation of data destruction to the University.

10. Audits: If the Selected Firm/Vendor must under this agreement create, obtain, transmit, use, maintain, process, or dispose of University Data, Selected Firm/Vendor will, at its expense, conduct or have conducted, on an annual basis, an American Institute of CPAs Service Organization Controls (SOC 2) Type II audit, or other security audit with audit objectives deemed sufficient by the University, which attests the Selected Firm/Vendor's security policies, procedures and controls. Additionally, the Selected Firm/Vendor will provide the University the results of the above audits, scans and tests upon request, and will promptly modify its security measures as needed based on those results in order to meet its obligations under this agreement. Further, whether the selected firm/vendor uses University Data or not, they will allow for the University to conduct their own security audit with audit objectives and procedures deemed sufficient by the University.
11. Compliance:
    a. Selected Firm/Vendor will comply with all applicable laws and industry standards in performing services under this agreement. Any Selected Firm/Vendor personnel visiting the University's facilities will comply with all applicable University policies regarding access to, use of, and conduct within such facilities. The University will provide copies of such policies to Selected Firm/Vendor upon request.
    b. Selected Firm/Vendor warrants that the service it will provide to the University is fully compliant with relevant laws, regulations, and guidance that may be applicable to the service, such as: the Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH), Gramm-Leach-Bliley Financial Modernization Act (GLB), Payment Card Industry Data Security Standards (PCI-DSS), Americans with Disabilities Act (ADA), Federal Export Administration Regulations, and Defense Federal Acquisitions Regulations.
    c. If the Payment Card Industry Data Security Standards (PCI-DSS) are applicable to the Selected Firm/Vendor service provided to the University, the Selected Firm/Vendor will, upon written request, furnish proof of compliance with PCI-DSS within 10 business days of the request.
12. Survival: The Selected Firm/Vendor's obligations under Section 9 shall survive termination of this agreement until all University Data has been returned or Securely Destroyed. This contract and associated addenda are binding upon, and inures to the benefit of, the parties and their respective permitted successors and assigns.