DATA SECURITY AGREEMENT

This Data Security Agreement (Agreement) is agreed upon effective _____(Date) by and between _____ (University) and _____(Contractor).

1. Disclosure of University Data;

   Contractor shall not disclose University Data in any manner that would constitute a violation of state or federal law or the terms of this agreement including, without limitation, by means of outsourcing, sharing, retransfer, or access, to any person or entity, except:

   a. Employees or agents who actually and legitimately need to access or use University Data in the performance of Contractor's duties to University;

   b. Such third parties, such as but not limited to, subcontractors, but only after such third party has agreed in writing and in advance of any disclosure, to be bound by confidentiality terms at least as stringent as the terms of this Agreement; or

   c. Any other third party approved by the University in writing and in advance of any disclosure, but only to the extent of such approval.

   Contractor may also store University Data on servers housed in datacenters owned and operated by third parties, provided the third parties have executed confidentiality agreements with Contractor.

2. Use of, Storage of, or Access to, University Data

   Contractor shall only use, store, or access University Data:

   a. In accordance with, and only to the extent permissible under this Agreement and the Contract; and

   b. In full compliance with any and all applicable laws and regulations, only to the extent applicable to Contractor, but without limitation: Family Educational Rights and Privacy Act (FERPA) and, Health Insurance Portability and Accountability Act (HIPAA),

   c. Any transmission, transportation, or storage of University Data outside the United States is prohibited except on prior written authorization by the University.

3. Safeguarding University Data

   Contractor agrees that use, storage, and access to University Data shall be performed with that degree of skill, care, and judgment customarily accepted as sound, quality, and professional practices. Contractor shall implement and maintain safeguards necessary to ensure the confidentiality, availability, and integrity of University Data. Contractor shall also implement and maintain any safeguards required to be implemented by applicable state and federal laws and regulations.

Such safeguards shall include as appropriate, and without limitation, the following:

a. System Security. A System that is owned or operated by Contractor and contains University Data shall be secured as follows:

i. Contractor shall implement controls reasonably necessary to prevent a breach.

ii. The System shall use secure protocols and encryption to safeguard University Data in transit.

iii. Contractor understands the System may be placed on a public network and shall implement safeguards reasonably necessary to protect its System from compromises and attacks. Contractor will protect the System with firewalls.

iv. Contractor shall:

a. Limit administrative access to the System,

b. Limit remote access to the System,

c. Limit account access and privileges to the least necessary for the proper functioning of the System

d. Remove or disable applications and services that are not necessary for the proper functioning of the System,

e. Use named user accounts and not generic or shared accounts,

f. Use Federated Single Sign On, Kerberos, or other industry compliant services for authentication and authorization, and

g. Enable an appropriate level of auditing and logging for the operating system and applications.

v. The System shall allow the changing of System and user passwords.

b. Product Maintenance and Support

i. Contractor shall have a process for the timely review, testing, and installation of patches essential for safeguarding the confidentiality, integrity, or availability of the System or University Data.

ii. Change management procedures shall be followed.

iii. Contractor shall ensure that the product is supported, provided that University maintains the requisite subscriptions. Contractor shall provide University with notice 12 months before the product becomes unsupported.

iv. If necessary, and provided that University maintains the requisite subscriptions, Contractor shall provide remote support via a secure connection method that includes an audit log of events. Remote access shall be limited to an as needed or as requested basis.

c. Data Protections

i. Contractor shall only use, store, disclose, or access University Data:

1. In accordance with, and only to the extent needed to provide services to University; and

2. In full compliance with any and all applicable laws, and regulations

ii. Contractor shall implement controls reasonably necessary to prevent unauthorized use, disclosure, loss, acquisition of, or access to University Data. This includes, but is not limited to personnel security measures, such as background checks.

iii. All transmissions of University Data by Contractor shall be performed using a secure transfer method

d. Contractor access to University systems

University login credentials may be given to contractors requiring access to secured computer equipment located on-site at the University for the purposes of scheduled troubleshooting, maintenance, or updates to software provided or supplied by Contractor and installed on University-owned computer equipment. In this case, the University will provide the Contractor with credentials for logging in locally or through our secured Virtual Private Network (VPN), if required. Credentials will be created upon entry of a help desk ticket by the University department for which the Contractor will be working. The Contractor credentials will be enabled for the time specified in the help desk ticket and will be disabled once that time has expired. The University Department is responsible for notifying the Help Desk should Contractor access be no longer needed prior to the expiration date specified in the Work Ticket. Passwords will follow normal University password policy, including 90 day password expirations, unless exceptions are granted by Information Technology for the specific case of University credentials which are embedded into a system for automating processing or testing. Contractor is responsible for changing the password per the instructions at http://www.bloomu.edu/technology/passwords prior to password expiration.

As a condition of the Contractor's access to University computing equipment the Contractor represents that they will not attempt to access any system(s) other than the one(s) designated in the help desk ticket nor will the Contractor use any computer equipment for any purpose that is unlawful.

All work performed by the Contractor while connected to University computing equipment is subject to monitoring by University staff and verification by the University Department or Division requesting the access.

4. Oversight

The University reserves the right to request security information reasonably necessary to ascertain University's own compliance with state and federal data privacy laws. Upon the

University's request, Contractor shall provide a copy of its most recent SOC 2 audit report, and that of any data center in which University's Data is stored.

5. Data Breach

If Contractor becomes aware that University Data may have been accessed, disclosed, or acquired without proper authorization and contrary to the terms of this Agreement or the Contract, Contractor shall use reasonable efforts to alert the University of any Data Breach within two business days, and shall immediately take such actions as may be necessary to preserve forensic evidence and eliminate the cause of the Data Breach. Contractor shall give highest priority to immediately correcting any Data Breach and shall devote such resources as may be required to accomplish that goal. Contractor shall provide the University information necessary to enable the University to fully understand the nature and scope of the Data Breach. If required by applicable law, such as the Pennsylvania Breach of Personal Notification Act (73 P.S. §§ 2301, et seq), Contractor shall provide notice and credit monitoring to parties affected by any Data Breach. Upon request, Contractor shall provide University information about what Contractor has done or plans to do to mitigate any deleterious effect of the unauthorized use or disclosure of, or access to, University Data. In the event that a Data Breach requires Contractor's assistance in reinstalling software, such assistance shall be provided at no cost to the University. The University may discontinue any services or products provided by Contractor until the University, in its sole discretion, determines that the cause of the Data Breach has been sufficiently mitigated.

6. No Surreptitious Code

Contractor warrants that, to the best of its knowledge, the System is free of and does not contain any code or mechanism that collects personal information or asserts control of the System without University's consent, or which may restrict University's access to or use of University Data. Contractor further warrants that it will not knowingly introduce, via any means, spyware, adware, ransomware, rootkit, keylogger, virus, trojan, worm, or other code or mechanism designed to permit unauthorized access to University Data, or which may restrict University's access to or use of University Data.

7. Compelled Disclosure

If Contractor is served with any subpoena, discovery request, court order, or other legal request or command that calls for disclosure of any University Data, Contractor shall promptly notify the University in writing and provide the University sufficient time to obtain a court order or take any other action the University deems necessary to prevent disclosure or otherwise protect University Data. In such event, Contractor shall provide University prompt and full assistance in University's efforts to protect University Data. Where Contractor is prohibited by law from notifying the University of a legal request for University Data, Contractor will comply with all applicable laws and regulations with respect to the requested University Data.

8. Termination Procedures

Upon expiration or termination of the Contract, Contractor shall ensure that no Data Breach occurs and shall follow the University's instructions as to the preservation, transfer, or

destruction of University Data. The method of destruction shall be accomplished by "purging" or "physical destruction", in accordance with National Institute of Standards and Technology (NIST) Special Publication 800-88. Upon request by the University, Contractor shall certify in writing to University that return or destruction of data has been completed. Prior to such return or destruction, Contractor shall continue to protect University Data in accordance with this Agreement.

9. Survival; Order of Precedence

This Agreement shall survive the expiration or earlier termination of the Contract. However, upon expiration or termination of the Contract, either party may terminate this Agreement. In the event the provisions of this Agreement conflict with any provision of the Contract, or Contractors' warranties, support contract, or service level agreement, the provisions of this Agreement shall prevail.

10. Definitions

a. University Data: University Data is any and all data that the University has disclosed to Contractor. For the purposes of this Agreement, University Data does not cease to be University Data solely because it is transferred or transmitted beyond the University's immediate possession, custody, or control.

b. Data Breach: The unauthorized access and acquisition of computerized data that materially compromises the security or confidentiality of confidential or sensitive personal information maintained by the University as part of a database of personal information regarding multiple individuals and that causes or the University reasonably believes has caused or will cause loss or injury to any University constituent.

c. System: An assembly of components that supports an operational role or accomplishes a specific objective. This may include a discrete set of information resources (network, server, computer, software, application, operating system or storage devices) organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

d. Change Management: A formal process used to ensure that changes to a system are introduced in a controlled and coordinated manner. This reduces the possibility that unnecessary changes will be introduced to a system, that faults or vulnerabilities are introduced to the system, or that changes made by other users are undone.

e. Contract. Shall mean Contractors terms and conditions of sale and service.

UNIVERSITY	CONTRACTOR
Signature: _____	Signature: _____
Printed Name: _____	Printed Name: _____
Job Title: _____	Job Title: _____
Date:_____	Date:_____