UNIVERSITY OF MARY WASHINGTON | Procurement Services

UNIVERSITY OF MARY WASHINGTON
Hosted Technology Services Addendum

VENDOR NAME: _____

VENDOR PRODUCT/SOLUTION: _____

This Addendum shall be included in any procurement deemed necessary requiring hosted technology services for the purpose of ensuring that the Commonwealth of Virginia and University of Mary Washington, technology standards are complied with for the duration of the agreement between the University and the Vendor (also referred to herein as "Contractor").

Definitions:

- Agreement: The "Agreement" includes the contract, this addendum and any additional addenda and attachments to the contract, including the Contractor's Form.
- University: "University" or "the University" means University of Mary Washington, its trustees, officers and employees. The point of contact for the University is the contract administrator for this Agreement.
- University Data: "University Data" is defined as any data that the Contractor creates, obtains, accesses, transmits, maintains, uses, processes, stores or disposes of in performance of the Agreement. It includes all Personally Identifiable Information and other information that is not intentionally made generally available by the University on public websites and any data processed using bookstore systems operated by Contractor on behalf or in support of the University.
- Personally Identifiable Information: "Personally Identifiable Information" (PII) includes but is not limited to: Any information that directly relates to an individual and is reasonably likely to enable identification of that individual or information that is defined as PII and subject to protection by University of Mary Washington under federal or Commonwealth of Virginia law.
- Security Breach: "Security Breach" means a security-relevant event in which the security of a system or procedure involving University Data is breached, and in which University Data is exposed to unauthorized disclosure, access, alteration, or use.
- Service(s): "Service" or "Services" means any goods or services acquired by the University from the Contractor.

1. **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 shall remain the exclusive property of the University, and Contractor has a limited, nonexclusive license to use these data as provided in this Agreement solely for the purpose of performing its obligations hereunder.

2. **Nonvisual Access To Technology:** All information technology which, pursuant to this Agreement, is purchased or upgraded by or for the use of any Commonwealth agency or institution or political subdivision of the Commonwealth (the "Technology") shall comply with Section 508 of the Rehabilitation Act (29 U.S.C. 794d), as amended. If requested, the Contractor must provide a detailed explanation of how compliance with Section 508 of the Rehabilitation Act is achieved and a validation of concept demonstration. The requirements of this Paragraph along with the Non-Visual Access to Technology Clause shall be construed to achieve full compliance with the Information Technology Access Act, §§2.2-3500 through 2.2-3504 of the Code of Virginia. Compliance may be determined by the degree to which the product meets the recommendations described in the VPAT (Voluntary Product Accessibility Template) and/or WCAG 2.0 Level AA guidelines.

3. Data Privacy:

a. Contractor 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.

b. University Data will not be stored outside the United States without prior written consent from the University.

c. Contractor will provide access to University Data only to its employees and subcontractors who need to access the data to fulfill obligations under this Agreement. The Contractor will ensure that the Contractor's employees who perform work under this Agreement have read, understood, and received appropriate instruction as to how to comply with the data protection provisions of this Agreement.

i. If the Contractor will have access to the records protected by the Family Educational Rights and Privacy Act (FERPA), Contractor acknowledges that for the purposes of this Agreement it will be designated as a "school official" with "legitimate educational interests" in such records, as those terms have been defined under FERPA and its implementing regulations, and Contractor agrees to abide by the limitations and requirements imposed on school officials. Contractor will use such 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 this Agreement, required by law, or authorized in writing by the University.

4. Data Security:

a. Contractor 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 Contractor'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.

b. Contractor will store and process University Data in a secure site and will provide a SAS 70, SAS 70 Type II, SSAE 16, SOC 2 or SOC 3, or other security report deemed sufficient by the University, from a third party reviewer along with annual updated security reports. If the Contractor is using a third-party cloud hosting company such as AWS, Rackspace, etc., the Contractor will obtain the security audit report from their hosting company and give the results to the University.

c. Contractor will use industry-standards and up-to-date security tools, technologies and practices such as network firewalls, anti-virus, vulnerability scans, system logging, intrusion detection, 24x7 system monitoring and third-party penetration testing in providing services under this Agreement.

d. Without limiting the foregoing, Contractor warrants that all electronic University Data will be encrypted in transmission (including via web interface) and stored at AES 256 or stronger.

5. Data Authenticity, Integrity and Availability:

a. Contractor will take reasonable measures, including audit trails, to protect University Data against deterioration or degradation of data quality and authenticity. Contractor shall 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."

b. Contractor will ensure backups are successfully completed at the agreed interval and that restoration capability is maintained for restoration to a point-in-time and\or to the most current backup available.
c. Contractor will maintain an uptime of 99.99% or greater, or as negotiated and accepted by the University, as agreed to for the contracted services via the use of appropriate redundancy, continuity of operations and disaster recovery planning and implementations, excluding regularly scheduled maintenance time.

6. Employee Qualifications:

a. Contractor shall ensure that its employees have undergone appropriate background screening and possess all needed qualifications to comply with the terms of this agreement including but not limited to all terms relating to data and intellectual property protection.

7. Security Breach:

a. Response. Immediately upon verification of a Security Breach resulting in unauthorized access to or disclosure or use of University Data or any bookstore systems operated by Contractor on behalf or in support of the University, Contractor will notify the University if and to the extent legally permitted to do so, fully investigate the incident, and cooperate fully with the University's investigation of and response to the incident. Except as otherwise required by law, Contractor 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. In addition to any other remedies available to the University under law or equity, when applicable to the type services being provided, Contractor will pay for or reimburse the University in full for all costs incurred by the University in investigation and remediation of such Security Breach caused by Contractor, 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 caused by Contractor. Contractor agrees to indemnify, hold harmless and defend the University from and against any and all claims, damages, or other harm related to such Security Breach caused by Contractor.

8. Requests for Data, Response to Legal Orders or Demands for Data:

a. Except as otherwise expressly prohibited by law, Contractor will:
    i. immediately notify the University of any subpoenas, warrants, or other legal orders, demands or requests received by Contractor seeking University Data;
    ii. consult with the University regarding its response;
    iii. cooperate with the University's 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. Contractor will make itself and any employees, contractors, or agents assisting in the performance of its obligations under the Agreement, available to the University at no cost to the University based upon claimed violation of any laws relating to security and\or privacy of the data that arises out of this agreement. This shall include any data preservation or eDiscovery required by the University.
c. The University may request and obtain access to University Data and related logs at any time for any reason and at no extra cost.

9. Data Transfer Upon Termination or Expiration:

a. Contractor's obligations to protect University Data shall survive termination of this Agreement until all University Data has been returned or Securely Destroyed, meaning taking actions that render data written on media unrecoverable by both ordinary and extraordinary means.

b. Upon termination or expiration of this Agreement, Contractor will ensure that all University Data are securely transferred, returned or destroyed as directed by the University in its sole discretion within 90 days of termination of this Agreement (except as may be required by applicable law or regulation or Contractor's customary document retention policies, or if contained in computer files maintained pursuant to Contractor's customary archiving or back-up procedures). Transfer/migration to the University or a third party designated by the University shall occur without significant interruption in service. Contractor shall ensure that such transfer/migration uses facilities, methods, and data formats that are accessible and compatible with the relevant systems of the University or its transferee, and to the extent technologically feasible, that the University will have reasonable access to University Data during the transition.

c. In the event that the University requests destruction of its data, Contractor agrees to Securely Destroy all data in its possession and in the possession of any subcontractors or agents to which Contractor might have transferred University data. Contractor agrees to provide documentation of data destruction to the University and to complete any required Commonwealth of Virginia documentation regarding the destruction of University Data.

d. Contractor will notify the University of impending cessation of its business and any contingency plans. This includes immediate transfer of any previously escrowed assets and data and providing the University access to Contractor's facilities to remove and destroy University-owned assets and data. Contractor shall implement its exit plan and take all necessary actions to ensure a smooth transition of service with minimal disruption to the University. The Contractor 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 the University. Contractor will work closely with its successor to ensure a successful transition to the new equipment, with minimal downtime and effect on the University, all such work to be coordinated and performed in advance of the formal, final transition date.

10. Audits:

a. Upon reasonable advance written notice and no more than once per calendar year, the University reserves the right in its sole discretion to perform audits of Contractor at no additional cost to the University to ensure compliance with the terms of this Agreement. Contractor shall reasonably cooperate in the performance of such audits. This provision applies to all agreements under which Contractor must create, obtain, transmit, use, maintain, process, or dispose of University Data. The audit shall be limited to only those books and records directly relevant to Contractor's performance hereunder.

b. If Contractor must under this 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, Contractor will at its expense conduct or have conducted at least annually a(n):

   i. Security audit with audit objectives deemed sufficient by the University, which attests Contractor's security policies, procedures and controls;

   ii. vulnerability scan, performed by a scanner approved by the University, of Contractor's electronic systems and facilities that are used in any way to deliver electronic services under this Agreement; and

   iii. formal penetration test, performed by a process and qualified personnel approved by

the University, of Contractor's electronic systems and facilities that are used in any way to deliver electronic services under this Agreement.

c. Additionally, Contractor will provide the University upon request the results of the above audits, scans and tests, and will promptly modify its security measures as needed based on those results in order to meet its obligations under this Agreement.

11. Compliance:

a. Contractor will comply with all applicable laws and industry standards in performing services under this Agreement. Any Contractor 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 Contractor upon request.

b. Contractor agrees that the service it will provide to the University is fully compliant with applicable law and, as required by applicable law, will enable the University to be compliant with relevant requirements of all laws, regulation, and guidance applicable to the University and/or Contractor, including but not limited to: the Family Educational Rights and Privacy Act (FERPA) as stated in Section 3(c)(i) above, Payment Card Industry Data Security Standards (PCI-DSS),and Americans with Disabilities Act (ADA).

12. **No End User Agreements:** Any agreements or understandings, whether electronic, click through, verbal or in writing, between Contractor and University employees or other end users under this Agreement that conflict with the terms of this Agreement, including but not limited to this Addendum, shall not be valid or binding on the University or any such end users.

To the extent allowed by Virginia law and as further described in the parties' Agreement for Bookstore Services at Section 25(a), the University of Mary Washington will keep any information provided by Contractor hereunder confidential.

This Addendum and any other related and attached documents constitute the entire agreement between the parties and may not be waived of modified except by written agreement between the parties.

This Agency does not discriminate against faith-based organizations.

IN WITNESS WHEREOF, the parties have caused this contract to be duly executed, intending thereby to be legally bound.

AGENCY **University of Mary Washington**	**CONTRACTOR**
SIGNATURE: _____	SIGNATURE: _____
PRINTED NAME: _____	PRINTED NAME: _____
TITLE: _____	TITLE: _____
DATE: _____	DATE: _____