**UNIVERSITY OF MAINE SYSTEM**

 **SAFEGUARDING DATA AGREEMENT**

1. Scope: This Agreement addresses the Contractor’s responsibility for safeguarding Protected University Data. For the purposes of this Agreement, Protected University Data is defined as any data or information owned by Institution that the Contractor creates, obtains, accesses (via records, systems, or otherwise), receives (from Institution or on behalf of the Institution), or uses in the course of its performance of the contract which include, but not limited to: social security numbers; drivers’ license numbers; credit card numbers; and all information whose collection, disclosure, protection, and disposition is governed by state or federal law or regulation, particularly information subject to the Family Educational Rights and Privacy Act (FERPA).
2. Term and Termination: This Agreement shall take effect upon execution and shall be in effect commensurate with the term of the license or agreement for the product or service with the University.
3. Subcontractors and Agents: Contractor shall not provide any Protected University Data to subcontractors, agents, or other third parties without prior written authorization from the University. If Contractor provides any Protected University Data received from the University or created or received by Contractor on behalf of the University, to a subcontractor or agent, the Contractor shall require such subcontractor or agent to agree to the same restrictions and conditions as are imposed on Contractor by this Agreement.
4. Property of University: All Protected University Data is the property of the University and shall be turned over to the University upon request.
5. Return or Destruction of Protected University Data:
6. Within 30 days of termination, cancellation, or expiration of the license or agreement for the product or service, for any reason, Contractor shall cease and desist all uses and disclosures of Protected University Data and shall return all such information received from the University, or created or received by Contractor on behalf of the University, unless the University requests that all such data be destroyed beyond all ability to recover. This provision shall apply to information that is in the possession of subcontractors or agents of Contractor. Contractor shall retain no copies of University information, including any compilations derived from and allowing identification of any individual’s confidential information.
7. In the event that Contractor determines that returning or destroying any such information is infeasible, Contractor shall provide to University notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the Parties that return, or destruction of such information is infeasible, Contractor shall extend the protections of this Agreement to such information and limit further uses and disclosures of such information to those purposes that make the return or destruction infeasible, for so long as Contractor maintains such information.
8. Survival: While any Protected University Data is in the possession or control of the Contractor, its subcontractors or agents, the respective rights and obligations of Contractor pursuant to this Agreement shall survive termination.
9. Reasonable and Appropriate Controls: The Contractor agrees to implement reasonable and appropriate privacy and security measures to preserve the confidentiality, integrity, and availability of all electronically maintained or transmitted Protected University Data furnished by the University, or collected by the Contractor on behalf of the University
10. If information pertaining to student educational records is accessed, transferred, stored or processed by Contractor; Contractor shall protect such data in accordance with FERPA.
11. If information pertaining to protected health information is accessed, used, collected, transferred, stored or processed by Contractor; Contractor shall protect such data in accordance with HIPAA and Contractor shall sign and adhere to a Business Associate Agreement.
12. If Contractor engages in electronic commerce on behalf of the University or cardholder data relating to University activities is accessed, transferred, stored or processed by Contractor; Contractor shall protect such data in accordance with current PCI-DSS requirements.
13. If information pertaining to protected financial customer information is accessed, transferred, stored or processed by Contractor; Contractor shall protect such data in accordance with GLBA.
14. If information pertaining to persons located in the European Economic Area (EEA) is accessed, transferred, stored, or processed by Contractor; Contractor shall protect, collect, store, transfer, and process such data in accordance with the obligations of a data processor, or in accordance with the obligations of a data controller if specified within an underlying license or agreement for the product or service as a data controller, as set forth in the General Data Protection Regulation (GDPR, Regulation (EU) 2016/679) and shall provide reasonable assistance at the request of the University for fulfillment of requests made pursuant to the rights afforded to data subjects in GDPR Chapter III.
15. Prohibition of Unauthorized Use or Disclosure of Information: Contractor agrees to hold all information in strict confidence. Contractor shall not use or disclose information received from, or created or received by, Contractor on behalf of the University except as required to provide the product or service to the University, as required by law, or as otherwise authorized in writing by the University. For the avoidance of doubt, transfers of Protected University Data to another country without the prior written authorization of the University constitute unauthorized use of information in breach of this Section 8.
16. Contractor Employee Data Access Control: All Contractor employees shall be adequately screened, commensurate with the sensitivity of their jobs. Contractor agrees to limit employee access to data on a need-to-know basis. Contractor shall impose a disciplinary process for employees not following privacy procedures. Contractor shall have a process to remove access to Protected University Data immediately upon termination or re-assignment of an employee by the Contractor.
17. Data Breach: Contractor shall report to the University any use or disclosure of Protected University Data not authorized by this Agreement or in writing by the University. Contractor shall make the report to the University not more than one (1) business day after Contractor learns of such use or disclosure. Contractor’s report shall identify; (i) the nature of the unauthorized use or disclosure, (ii) the information used or disclosed, (iii) who made the unauthorized use or received the unauthorized disclosure, (iv) what Contractor has done or shall do to mitigate the effects of the unauthorized use or disclosure, and (v) what corrective action Contractor has taken or shall take to prevent future similar unauthorized use or disclosure. Contractor shall provide such other information, including a written report, as reasonably requested by the University.

Contractor shall take appropriate steps to remedy such data breach and mitigate, to the extent practicable, any harmful effect that is known to Contractor of a security breach or use or disclosure of Protected University Data by Contractor in violation of the requirements of this Agreement. Contractor shall keep University informed on the progress of each step of the incident response. Contractor shall indemnify and hold University harmless from all liabilities, costs and damages arising out of or in any manner connected with the security breach or unauthorized use or disclosure by Contractor of any Protected University Data. Contractor shall mitigate, to the extent practicable, any harmful effect that is known to Contractor of a security breach or use or disclosure of Protected University Data by Contractor in violation of the requirements of this Agreement. In addition to the rights of the Parties established by this Agreement, if the University reasonably determines in good faith that Contractor has materially breached any of its obligations, the University, in its sole discretion, shall have the right to terminate the license or agreement to use the product or service immediately.

1. Mobile Devices: If mobile devices are used by the Contractor in the performance of this Agreement to access Protected University Data, Contractor shall install and activate authentication and encryption capabilities on each mobile device in use.
2. Contractor Hosted Data: If Contractor hosts Protected University Data in or on Contractor or subcontractor facilities, the following additional clauses apply.
	1. Computers that host Protected University Data shall be housed in secure areas that have adequate walls and entry control such as a card-controlled entry or staffed reception desk. Only authorized personnel shall be allowed to enter, and visitor entry will be strictly controlled.
	2. Contractor shall design and apply physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disasters. Contractor shall protect hosted systems with Uninterruptible Power Supply (UPS) devices sufficient to meet business continuity requirements.
	3. Contractor shall backup systems or media stored at a separate location with regular scheduled incremental and full back-ups with sufficient retention of backup files to restore data. Contractor shall test restore procedures not less than once per year.
	4. Contractor shall provide for reasonable and adequate protection on its network and system to include firewall and intrusion detection/prevention.
	5. Contractor shall use strong encryption and certificate-based authentication on any server hosting on-line and e-commerce transactions with the University to ensure the confidentiality and non-repudiation of the transaction while crossing networks.
	6. Contractor shall require strong passwords for any user accessing Protected University Data. Strong passwords shall be at least eight characters long; contain at least one upper and one lower case alphabetic characters; and contain at least one numeric or special character.
	7. The installation or modification of software on systems containing Protected University Data shall be subject to formal change management procedures and segregation of duties requirements.
	8. Contractor who hosts Protected University Data shall engage an independent third-party auditor to evaluate the information security controls not less than every two (2) years. Such evaluations shall be made available to the University upon request.
3. Records and Compliance: Contractor shall maintain records and other compilations of data pertaining to the use, access, collection, storage, and transfer of Protected University Data and make such available to the University or regulatory authorities (including, without limitation, the Secretary of the U.S. Department of Health and Human Services and public authorities in the EEA) upon request as reasonably necessary to demonstrate compliance with applicable laws, regulations, and lawful orders.
4. System Development: If the Contractor provides system development, Protected University Data shall not be used in the development or test environments. Records that contain these types of data elements may be used if that data is first de-identified, masked or altered so that the original value is not recoverable. For programs that process Protected University Data, initial implementation as well as applied updates and modifications must be produced from specifically authorized and trusted program source libraries and personnel. Contractor shall provide documentation of a risk assessment of new system development or changes to a system.

**UNIVERSITY**

By: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature Date

Printed

Title Address

**CONTRACTOR**

By: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature Date

Printed

Title Address