Secure Handling of UCF Data Agreement

Purpose

University of Central Florida ("UCF" or "Institution") requires vendors and other third parties ("Vendor") to review, accept, and integrate the following requirements ("Agreement") as part of any contract, agreement, Service Level Agreement ("SLA"), or other transaction document that involves the storage, transmission, processing, or collection of UCF Data, or access to UCF Data, by the Vendor. This Agreement is intended to ensure that UCF's security and compliance requirements are outlined and followed by the Vendor.

Definitions

Comparable Standard – A standard or framework similar to the current standards set forth and maintained by the National Institute of Standards and Technology (NIST), such as ISO/IEC 27001, ISA 62443, COBIT 5, CCS CSC, SANS, PCI-DSS, or any other generally recognized security standard or framework used to address and/or manage risk.

FERPA - Family Educational Rights and Privacy Act. A federal law that protects the privacy of student education records. The law applies to all institutions that receive funds under an applicable program of the U.S. Department of Education.

Florida State Statutes - UCF is an entity of the state and certain data is subject to statutes defined by the state for information handling regarding personal and public record data.

GDPR – General Data Protection Regulation. A European Union law that requires organizations to safeguard personal data and uphold the privacy rights of residents within the European Economic Area (EEA).

HIPAA - Health Insurance Portability and Accountability Act. A federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge.

NIST - National Institute of Standards and Technology. NIST provides definitions, standards, and recommended security controls for information systems at federal agencies.

PCI DSS - Payment Card Industry Data Security Standards. A security standard for organizations that process or handle credit card data.

Penetration Test - The process of identifying risks and vulnerabilities in computer networks, system, hardware, applications, and other parts of the environment using real-world attacks.

UCF Data – All data that is created, collected, maintained, recorded, or managed by the university, its staff, and agents working on its behalf, while conducting university business, that vendor has access to as a result of their relationship with UCF. This includes information that is processed and resides on privately owned devices that are used for university purposes as well as personal data which equates to any information related to a natural person or "Data Subject", that can directly or indirectly identify an individual.

Vulnerability Assessment – Defined by NIST as "a systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation."

1 Security Program

1.1 Data Security: Vendor shall develop, implement, maintain, and use appropriate administrative, technical, and physical security measures based on the latest industry security standards and best practices and in accordance with all applicable law, to preserve the confidentiality, integrity, and availability of all electronically maintained or transmitted UCF Data received from, or on behalf of Institution or its students.

1.2 Network Security: Vendor agrees to always maintain network security that conforms to the current standards set forth and maintained by NIST or other generally recognized comparable standard.

1.3 Penetration Testing: Vendor agrees to conduct a formal penetration test at least once a year.

1.4 Vulnerability Testing: Vendor agrees to perform vulnerability assessments at least on a quarterly basis.

1.5 Security Auditing/Risk Assessment: Vendor agrees to have an independent, industry-recognized third-party security audit that conforms to the current standards set forth and maintained by NIST or other generally recognized comparable standard performed at least once a year. Upon request, the vendor will share the audit results.

1.6 Business Continuity Plan: Vendor agrees to maintain a business continuity plan with detailed recovery procedures and manual workarounds in the event of a disaster. The plans must include emergency and contingency plans for the facilities in which Vendor information systems that process UCF Data are located. Vendor's redundant storage and its procedures for recovering data shall serve to reconstruct UCF Data in its original or last-replicated state from before the time it was lost or destroyed.

1.7 Cyber Insurance: Vendor agrees to maintain during the term of this Agreement, a cyber insurance policy for privacy and network security liability including coverage for:

1. Theft, dissemination, use and/or wrongful disclosure of data, including any business confidential information, personally identifiable information, or protected health information as defined by applicable law.
2. Breach of security, including unauthorized access and use of computer systems or databases, or extortion.
3. Introduction of malicious software code causing damage to, alteration of or destruction of electronic information.
4. Infringement of intellectual property, including copyright, trademark, and/or trade dress, and invasion of privacy.
5. Regulatory defense, fines, and penalties.
6. Breach response services, including notification and credit monitoring.

UCF shall have the right to request copies of such certificates of insurance and/or other evidence of the adequacy of the above insurance coverage from Vendor.

2 Data Protection

2.1 Data Encryption at-rest: Vendor agrees to encrypt all UCF Data at rest using 128-bit key AES encryption or better. This includes any backup data as part of its backup and recovery processes.

2.2 Data Encryption in-transit: Vendor agrees to encrypt all UCF Data in transit using 128-bit key AES encryption or better. Vendor also agrees that all transmission or exchange of data with UCF or any other transaction Vendor engages in that involves UCF Data, including sub-processors – shall take place via secure means, e.g., TLS protocol via HTTPS or SFTP.

2.3 Portable Data Storage: Any portable or laptop computing device used to process UCF Data must employ full-disk encryption.

2.4 Data Separation: Vendor agrees to employ physical and/or logical means to separate UCF Data from other customers in Vendor's infrastructure. Logical separation may include user access level controls, database/application-level controls, and monitoring or other tools.

2.5 Audit Trail: Vendor must log access and use of systems containing UCF Data, registering the access ID, time, authorization granted or denied, and relevant activity.

3 Data Stewardship

3.1 Data Ownership: Vendor acknowledges that all UCF Data shared with Vendor, or made accessible to Vendor's systems or personnel, remains the sole property of UCF as defined by existing UCF regulation and/or UCF policy. Sole property ownership by UCF shall mean that UCF always retains all physical as well as the sole intellectual property ownership of the UCF Data.

3.2 Data Use: Vendor agrees that all data exchanged shall be used expressly and solely for the purposes enumerated in the agreement or other transaction document between UCF and Vendor. Data shall not be distributed, repurposed, or shared across other applications, environments, or business units of Vendor except solely for the purposes of this agreement.

3.3 Data Location: Vendor agrees that no UCF Data will be outsourced or housed outside the United States of America without prior written UCF authorization.

3.4 Third Party Data Redistribution: Vendor agrees that no UCF Data of any kind shall be shared with any third parties except in service of this agreement. Vendor also agrees to submit a list of third parties upon request.

3.5 Third Party Contractual Obligations: Vendor agrees that any third parties used in service of UCF Data shall be contractually held to standards no less rigorous than those outlined in this Agreement.

3.6 Legal Requests: If required by law or a court of competent jurisdiction or an administrative body to disclose UCF Data, Vendor will notify UCF in writing within seven (7) days prior to any such disclosure in order to give UCF an opportunity to oppose any such disclosure.

3.7 End of Agreement Data Handling: Vendor agrees that within 60 days of the termination of the agreement or other transaction document between UCF and Vendor, whichever is later, per Florida statute 119.0701, Vendor shall transfer, at no cost to UCF, all UCF Data in possession of the Vendor. Once the Vendor transfers all UCF Data to UCF, the Vendor shall erase, destroy, and render unreadable all duplicate UCF Data still in Vendor's possession. Additionally, Vendor will certify in writing that these actions have been completed. All Vendor records stored electronically must be provided to UCF upon request from UCF's custodian of public records in a format that is compatible with the information technology systems of UCF.

3.8 Data Breach: In the event of a breach of any of Vendor's security obligations, unauthorized access to, disclosure, or loss of UCF Data or other event requiring notification under applicable law ("Notification Event"), Vendor agrees to:

a. Notify UCF within twenty-four (24) hours of the discovery of the breach by providing notice via email to UCF's Security Incident Response Team (sirt@ucf.edu).
b. Comply with all applicable federal and state laws such as, but not limited to, Florida's data breach notification law (FL State Statutes 501.171, Senate Bill 1524, FIPA) that require the notification of affected individuals.
c. In the event of a breach of any of Vendor's security obligations that results in the unauthorized access to, disclosure, or loss of UCF Data ("Breach Event"), Vendor agrees to assume responsibility for informing all such individuals in accordance with applicable law and indemnify, hold harmless, and defend UCF and the UCF Board of Trustees against any claims, damages, or other harm related to such Breach Event.

3.9 Handling of Data Subject Requests: If Vendor receives a Data Subject Request or complaint from a Data Subject regarding the Processing of Personal Data, Vendor will promptly, yet within no greater than twenty-four (24) hours, forward such request or complaint to UCF Privacy Compliance, via privacy@ucf.edu, provided the Data Subject has given sufficient information for Vendor to identify an existing relationship between the Data Subject and UCF.

3.10 Non-disclosure: Vendor agrees to hold in strict confidence and not disclose to anyone, unless required by law, all UCF Data which the vendor will have access to or will generate on UCF's behalf.

4 Compliance

4.1 Data Classification Addendum: Vendor agrees to abide by all legal and regulatory compliance requirements that apply due to the nature of the UCF Data being shared (e.g., FERPA, HIPAA, PCI, GDPR, etc.)

4.2 FERPA Regulations: If Vendor is provided access to any student data defined by the Family Educational Rights and Privacy Act ("FERPA") as non-directory information (such as personally identifiable information (PII) or educational records), or directory information, Vendor acknowledges that it will comply with the regulations outlined in FERPA for the handling of such information to the extent such regulations apply to Vendor. Vendor will not disclose or use any student information, except to the extent necessary to carry out its obligations under its agreement or other transaction document with UCF and as permitted by FERPA.

4.3 PCI Compliance: If the Vendor stores, processes, or transmits cardholder data, or can affect the security of the cardholder data environment (including redirects), Vendor agrees to maintain compliance with the most current Payment Card Industry Data Security Standard (PCI DSS). Additionally:

a. if the Vendor is the Merchant of Record, they will annually submit their latest PCI Attestation of Compliance (AoC) to UCF.
b. If the Vendor is a PCI third party service provider (TPSP), as defined by the PCI Council, Vendor must also agree to UCF's PCI Addendum.

4.4 HIPAA Compliance: If Vendor is provided potential access to any data defined as Protected Health Information (PHI) under HIPAA and the Vendor meets the definition of a business associate under HIPAA, the Vendor is required to enter into a Business Associates Agreement with UCF.

If Vendor is provided access to data defined as Protected Health Information (PHI) under HIPAA but the Vendor is not considered a business associate under HIPAA, then Vendor must implement HIPAA-compliant security safeguards consistent with the NIST Cybersecurity Framework.

4.5 GDPR Compliance: If the transfer of personal data to the Vendor is required and is subject to the GDPR, Vendor must abide by all GDPR requirements applicable to Vendor.

VENDOR Signature
(Executive / VP level) _____

Print Name _____

Title & Organization _____

E-Mail _____

Date _____