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, or Service Level Agreement ("SLA") 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.

1 Security Controls

1.1 Network Security: Vendor agrees at all times to maintain network security that – at a minimum – includes: network firewall provisioning, intrusion detection, and regular third party penetration testing. Likewise, Vendor agrees to maintain network security that conforms to the current standards set forth and maintained by the National Institute of Standards and Technology or other generally recognized comparable standard (e.g., ISO/IEC 27001, ISA 62443, COBIT 5, CCS CSC, SANS, PCI-DSS, etc.)

1.2 Risk Assessments: Vendor agrees to conduct a formal penetration test at least once a year. A penetration test is here defined as "the process of using approved, qualified personnel to conduct real-world attacks against a system so as to identify and correct security weaknesses before they are discovered and exploited by others." Vendor further agrees to perform vulnerability assessments at least on a quarterly basis.

1.3 Security Auditing: Vendor agrees to have an independent, industry-recognized third party security audit that conforms to the current standards set forth and maintained by the National Institute of Standards and Technology or other generally recognized comparable standard (e.g., ISO/IEC 27001, ISA 62443, COBIT 5, CCS CSC, SANS, PCI-DSS, etc.) performed at least once a year. The audit results and Vendor's plan for addressing or resolving of the audit results shall be shared with the Institution within 90 days of Vendor's receipt of the audit results.

1.4 Business Continuity Plan: Vendor agrees to present and maintain a business continuity plan with detailed recovery procedures and manual workarounds in the event of a disaster. The plans will 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.

1.5 Cybersecurity Insurance: Vendor agrees to maintain, at all times during the term of this Agreement, a comprehensive program of risk mitigation and cyber liability insurance. 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 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.

2.2 Data Encryption: Vendor agrees to encrypt all UCF data, either in transit or at rest, using 128 bit key AES encryption or better. This includes any backup data as part of its backup and recovery processes. Vendor agrees that any and all transmission or exchange of data with UCF and/or any other parties expressly designated by UCF – solely in accordance with Section 3.4 below – and/or any other transaction Vendor engages in that involves UCF data – shall take place via secure means, e.g. TLS protocol via HTTPS or FTPS.

2.3 Data Storage: Vendor shall adopt a policy that includes the following:

a. Any and all UCF data will be stored, processed, and maintained solely on designated target servers within the United States of America.
b. No UCF data at any time will be processed on or transferred to any portable or laptop computing device or any portable storage medium, except as stated explicitly with a valid business reason in the agreement between UCF and Vendor, or as an exception made on a case-by-case basis as specifically agreed to in writing, in advance, by an authorized agent of UCF.
c. Vendor agrees that any portable or laptop computing devices as part of such agreed-upon exception will employ full-disk encryption as agreed in 2.2 above.

2.4 Data Separation: Vendor agrees that University of Central Florida's data will be separated, either through physical or logical means, from other tenants in Vendor's infrastructure.

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 retains at all times all physical as well as the sole intellectual property ownership of the UCF Data.

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

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

3.4 Data Redistribution: Vendor agrees that no UCF data of any kind shall be transmitted, exchanged or

otherwise passed to other vendors, subcontractors, or other interested third parties except on a case-by-case basis as specifically agreed to in writing in advance by an authorized agent of UCF. Vendor agrees that all such UCF pre-approved vendors, subcontractors, or other interested third parties used by Vendor will be contractually held to standards no less rigorous than those outlined in this Agreement.

3.5 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 two (2) days prior to any such disclosure in order to give UCF an opportunity to oppose any such disclosure.

3.6 End of Agreement Data Handling: Vendor agrees that within 60 days of the termination of the agreement between UCF and Vendor, or the termination of the pertinent records retention period, whichever is later (hereafter referred to as "data retention period"), UCF can reclaim any needed UCF data in a mutually agreed upon format. At the end of the data retention period, Vendor will erase, destroy, and render unreadable all UCF data according to the standards enumerated in DOD 5220.22 or NIST 800-88 and certify in writing that these actions have been completed.

3.7 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. Assume responsibility for informing all such individuals in accordance with applicable law.
d. Indemnify, hold harmless and defend UCF, the UCF Board of Trustees, UCF's officers, agents and employees from and against any claims, damages, or other harm related to such Notification Event.

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 (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 with UCF and as permitted by FERPA.

4.3 PCI Compliance: In cases where Vendor is identified as a PCI third party service provider (TPSP), UCF requires that the Vendor at all times shall maintain compliance with the most current Payment Card Industry Data Security Standard (PCI DSS). 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 is required to abide by UCF's Data Protection Addendum, as well as the GDPR requirements applicable to Vendor.

VENDOR Signature
(Executive / VP level) _____

Print Name _____

Title _____

E-Mail _____

Date _____