Florida State University

Information Privacy and Security

Standard Terms and Conditions

March 2026

Version 1.00

I. Information Privacy and Security Requirements

A. The Supplier will ensure the agreed upon products and services will be provided to, or on behalf of, the University in a fully compliant manner to enable the Supplier and University to meet all relevant international, national, state, and local laws and regulations ("Applicable Laws"). All parties agree to handle data and other information with a standard of care at least as rigorous as that specified in the University's minimum standards within the Information Privacy Policy, which is hereby incorporated by reference into this Agreement. The University is bound by the Family Educational Rights and Privacy Act ("FERPA") regarding the release of student education records and, in the event of conflict with the University Policy, FERPA will govern.

B. Notwithstanding any additional Supplier compliance responsibilities which may be specified in this Agreement, and the Supplier requirements included in this FSU Information Privacy & Data Security Addendum, each party shall comply with all Applicable Laws in performing its duties under this Agreement. Each party is responsible for its own compliance with Applicable Laws.

C. In the situation where additional compliance responsibilities are assigned to Supplier, or if applicable to Supplier's agents or third-party providers, Supplier agrees to use commercially reasonable practices to comply with these additional requirements specified in this Agreement. Supplier acknowledges and agrees to include its third-party provider obligations when applicable to the products and services it is providing to FSU under this Agreement.

II. Protection of University Data

A. Supplier shall implement, maintain, and use appropriate administrative, technical, and physical security measures to preserve the confidentiality, integrity, and availability of High or Moderate risk data as defined by the University. Supplier shall ensure that its security measures are reviewed and revised when necessary, at a minimum annually, to address evolving threats and vulnerabilities.

B. All facilities used by Supplier to receive, store, process, or transmit data classified as High or Moderate risk will employ commercial best-practices, including appropriate administrative, physical, and technical safeguards, to secure such University data from unauthorized access, disclosure, alteration, loss and use. Unless otherwise specified in this Agreement, such data may not be stored, processed, received, or transmitted outside of data centers located within the United States.

C. Supplier warrants that all data classified as High or Moderate risk will be encrypted in transmission and at rest where required by law or contractual obligation (including via web interface) and may warrant use of the Advanced Encryption Standard (AES) encryption algorithm or other strong cryptography and/or encryption protocol, as negotiated by the University.

D. Supplier will use industry standard and up-to-date security tools and technologies such as antivirus protections, anti-malware and ransomware protections, and intrusion prevention and detection methods in providing services under this Agreement.

E. For any Artificial Intelligence (AI) services supplied or provided by Supplier, Supplier will only use University data as necessary to provide University with the AI services and comply with Applicable Laws. Supplier will not use University data to develop or improve the AI services, unless University explicitly agrees to such use in writing in this Agreement or by amendment to this Agreement.

F. For AI services, University may provide input and receive output. As between University and Supplier, to the extent permitted by Applicable Laws, University: (a) retains all ownership rights in input; and (b) owns all output. Supplier hereby assigns to University all of Supplier's right, title, and interest, if any, in and to output.

G. Supplier's data security obligations set forth in this Agreement extend specifically to input and output for AI services.

III. Protection of University Records & Personal Information

A. To the extent Supplier comes into contact with or has University's information in its possession, Supplier agrees to implement reasonable and appropriate safeguards to protect personal information, as defined in § 501.171, Florida Statutes and educational records as defined in § 1002.225, Florida Statutes and 20 U.S.C. § 1232g ("Personal Information"), maintain the security of Personal Information, prevent unauthorized use, access, disclosure, alteration and/or destruction of Personal Information, limit access to Personal Information it comes into contact with or possesses on behalf of the University to those of its employees who have a need to access the Personal Information in order to perform their job functions and ensure that such employees are aware of the confidentiality obligations of this Section and have agreed to comply with these obligations.

B. Supplier agrees that if it becomes aware of any unauthorized use, access, or disclosure of the Personal Information, or has a reasonable belief that substantial risk of unauthorized use, access, or disclosure exists, it will provide written notice to the University without unreasonable delay (but in no event, more than 48 hours) from the discovery of such unauthorized use, access, or disclosure. Supplier must cooperate fully to assist the University in identifying individuals potentially affected by such unauthorized use, access, or disclosure. Supplier is responsible for all reasonable costs and expenses actually incurred by the University, including the cost of providing any required notifications, in connection with responding to any incident of unauthorized use, access, or disclosure of the Personal Information to the extent such incident arises from the acts or omissions of Supplier.

IV. Security or Privacy Breach

A. Definition. For purposes of this article, the terms, "breach of security" or "breach," have the same meaning given as in section 501.171, Florida Statutes, applicable state or federal law, rule, regulation, or contractual obligation.

B. Notice will be given to the University of any actual or suspected unauthorized disclosure of access to or other breach of Supplier systems or of the data managed or maintained under control of Supplier within 48 hours of discovery. In the event of actual or suspected unauthorized disclosure of, access to, or other breach of the systems or data, the Supplier will comply with all state and federal laws and regulations applicable to such breach and will cooperate with the University in fulfilling its legal obligations.

C. Supplier agrees it will indemnify the University for an actual or suspected breach of security or violation of the Terms and Conditions herein, including but not limited to the cost of providing appropriate notice to all required parties and credit monitoring, credit rehabilitation, or other credit support services to individuals with information impacted by the actual or suspected breach.

D. Any Security or Privacy Breach may be grounds for immediate termination of this Agreement by the University. Such a determination will be made at the sole discretion of the University.

E. This section and its indemnity will survive the termination of this Agreement.

F. As applicable, Supplier and Supplier's third-party providers shall have and maintain during the term of the Agreement insurance coverage described at FSU Standard Contractor Insurance Provisions.

V. Right to Information Privacy and Security Audit

A. Supplier agrees that the University shall have the option to annually request a technology audit, including obtaining the Supplier's current System and Organization Controls ("SOC") 2 Type 2 report. If the Supplier handles Moderate or High-risk data and has not conducted a SOC 2 Type 2 audit, the University may, in its sole discretion, accept a full Higher Education Community Vendor Assessment Tool ("HECVAT") in its stead. Additionally, the University may, in its sole discretion, require Supplier to complete the university's third-party risk self-assessment on an annual basis. The third-party vendor risk assessment can be viewed here: Vendor

Risk Self-Assessment.

B. Records pertaining to the Supplier's services shall be made available to auditors and the University during normal working hours for this purpose.

VI. Data Return or Destruction Upon Termination or Expiration

A. Unless the University requests in writing that such data be destroyed upon termination, cancellation, expiration, or other conclusion of this Agreement, Supplier shall return the High or Moderate risk University data that is in the possession of Supplier, or subcontractors to, or agents of Supplier. Such destruction shall be accomplished by "purging" or "physical destruction" in accordance with commercially reasonable standards for the type of data being destroyed, e.g., *Guidelines for Media Sanitization*, NIST Special Publication 800-88 Revision 2. The Supplier shall certify in writing to the University that such destruction or return has been completed. Notwithstanding the expiration or termination of this Agreement for any reason, the obligation of confidentiality set forth in this document shall remain in force.

B. All input and output for AI services is to be returned or destroyed, at University's option, upon termination, cancellation, expiration, or other conclusion of this Agreement. Further, if the Parties agree in writing that return or destruction of High or Moderate risk University data, or University input and output for AI services is not feasible, Supplier agrees to maintain necessary information privacy and security protections for any such data, or input and output in accordance with Applicable Laws and this Agreement.