THE OHIO STATE UNIVERSITY ADDENDUM TO VENDOR

TERMS AND CONDITIONS

COMPLIANCE WITH OHIO LAW / THIRD PARTY TERMS. Company acknowledges that University is an instrumentality of the State of Ohio and as such is subject to Ohio law, including but not limited to Ohio Revised Code Section 9.27. ORC 9.27 requires that no State contract for goods or services may contain provisions requiring indemnification, choice of law and jurisdiction other than Ohio, binding arbitration, auto-renewals, or other provisions contrary to Ohio law, and if it does, such provisions are void ab initio. Company further acknowledges that neither this Agreement nor any subsequent Addendum or embedded terms may contain any provisions that are contrary to Ohio law, and any such provisions are not applicable to the University.

To the extent that Company requires the use of third-party products or services, it agrees and acknowledges that University cannot accept any third-party terms that are contrary to Ohio Law. Company further agrees that to the extent it determines to use such third-party products and services, Company must accept such terms solely on its own behalf, and not flow down such terms to the University.

The Ohio State University	**Company**
By_____	By_____
Name_____	Name_____
Title_____	Title_____
Date_____	Date_____

ACCESSIBILITY ADDENDUM-IF APPLICABLE

a. SELLER acknowledges and warrants that software conforms and shall continue to conform during the term of the Agreement to the W3C Web Content Accessibility Guidelines, version 2.1. ("WCAG 2.1") at conformance Level AA and the Minimum Digital Accessibility Standards of Purchaser [https://accessibility.osu.edu/digital-accessibility-policy/minimum-digital-accessibility-standards/], as may be modified from time to time. SELLER will make efforts to ensure that the Application is compatible with assistive technologies and features and will include accessibility features in any Application support documentation and instructions for using the Application with assistive technologies. SELLER must provide to PURCHASER a credible, current Voluntary Product Accessibility Template (VPAT) or an equivalent conformance report documenting SELLER'S conformance with the Standards herein.

b. If during the term of the Agreement, SELLER fails to maintain compliance with WCAG 2.1 AA, or PURCHASER, in its sole discretion, otherwise identifies an issue related to accessibility of the Application (the "Accessibility Issue") that renders the Application inaccessible, then PURCHASER shall notify SELLER of non-conformance. Within thirty (30) days of PURCHASER's receipt of a non-compliance notice ("Notice"), SELLER and PURCHASER shall meet and mutually agree upon an appropriate timeline for resolution of the Accessibility Issue(s) ("Initial Meeting").

c. In the event SELLER fails to: (i) acknowledge receipt of the notice within thirty (30) days of receipt of the Notice; or (ii) establish a mutually agreed upon timeline for resolution within thirty (30) days following the Initial Meeting; or (iii) materially resolve the Accessibility Issue(s) within the agreed-upon timeline and provide written proof thereof, then SELLER will provide a credit against PURCHASER's next invoice equal to 1/365 of the annual fees for the impacted software per day of delay, for up to a maximum of thirty (30) days, after which PURCHASER may terminate the Agreement and SELLER shall refund to PURCHASER a pro-rata share of any pre-paid fees. For clarity, credits will not exceed 30/365 of such annual fees per notice.

Data Security and Privacy Addendum -If Applicable

This Addendum ("Addendum") to the _____ Agreement ("Agreement") dated this _____ day of June 2025, is attached to and made a part of the Agreement between _____. ("Provider") and The Ohio State University ("Ohio State"). In the event of any conflict between the terms and conditions of this Addendum and the Agreement, the terms and conditions of this Addendum shall be binding.

a. **Prohibition of Unauthorized Use of Data.**

Ohio State's Data ("Data") includes all information that Ohio State discloses to Provider. Data may include Personal Information that identifies or can be used to identify an individual.

To the extent Provider's performance under this Addendum involves-Personal Information, that is personally-identifiable information, student records, protected health information, or individual financial information and subject to state or federal law or rules restricting the use and disclosure of such information, including, but not limited to; the federal Gramm-Leach-Bliley Act (15 U.S.C. §§ 6801(b) and 6805(b)(2)); the federal Family Educational Rights and Privacy Act (20 U.S.C. § 1232g); and the privacy and information security aspects of the Administrative Simplification provisions of the federal Health Insurance Portability and Accountability Act (45 CFR Part 160 and Subparts A, C, and E of Part 164); or the Payment Card Industry Data Security Standards, Provider agrees to comply with all applicable federal and state laws, regulations or policies restricting the access, use and disclosure of such Personal Information.

Provider maintains an Information Security Program ("ISP") made up of policies, procedures, technical and organizational safeguards, and training designed to protect Data against unauthorized loss, destruction, alteration, access or disclosure. Provider shall not use or disclose Data received from or on behalf of Ohio State except as appropriate to perform the services under the Agreement; as required by law, order, regulation, subpoena or other legal process; or as otherwise authorized in writing by Ohio State.

Provider agrees to require this same compliance in any of its subcontractor or agency agreements providing services under this Addendum.

b. **Security Standards.** Provider's ISP protects Data by implementing an industry security and privacy standard and including, at minimum:

I. **Network Security.** Provider maintains network security that includes network firewall provisioning, intrusion detection, network device logging and alerting, and vulnerability scans on externally facing systems in accordance with industry standards.

II. **Data Security.** Provider complies with applicable standards governing the patch management criticality rankings and patching time frame requirements for its systems and applications including, but not limited to, switches, routers, appliances, servers, workstation PC's, commercial software, and open-source software.

III. **Data Transmission.** Provider implements secure transmission protocols such as SFTP, SSH, TLS/SSL, and HTTPS when transmitting sensitive data.

IV. **Identity and Access Management.** Provider implements access standards designed to authenticate users, permit authorized access to Data, maintain segregation of duties, and revoke access as part of employee termination or transition.

V. **Data Storage:** Provider maintains appropriate policies, procedures, and controls reasonably designed to secure Data stored by Provider, its employees, and its suppliers. Provider or employee mobile devices, portable or laptop computing devices, or portable media that stores Data must use appropriate encryption designed to reduce the risk of compromise or misuse. Additionally, the access to Data through such devices must be approved by Ohio State.

VI. **Return or Destruction of Data.** Provider maintains a record retention policy that determines how records are retained, managed, stored and, where appropriate, destroyed. Since certain information cannot be erased or deleted from electronic systems, Provider maintains the confidentiality of all retained information until such time as the information is destroyed. Where appropriate, the Provider will maintain a record of destruction, shared with Ohio State, for all types of Data in its possession.

VII. **Resiliency:** Provider maintains appropriate and effective business continuity and disaster recovery plans to ensure resiliency of Data and business operations.

VIII. **US Storage** of Data must be stored in the United States.

IX. **Privacy:** Provider maintains a privacy policy, which includes, at minimum, processes for accessing, correcting, and requesting deletion of Personal Information. If required by regulation to fulfill the terms of this agreement, implement processes to obtain individual's consent and requests to opt out. Provider may not sell Personal Information or re-identify Personal Information that has been de-identified.

X. **Notification of Network or Data Breach.** Provider shall immediately report in writing to Ohio State any network breach and/or use or disclosure of Data not authorized by the Agreement, including any reasonable belief that unauthorized access to or acquisition of the Data has occurred. Provider shall make the report to Ohio State at security@osu.edu not more than two (2) business days after Provider reasonably believes there has been such unauthorized use or disclosure. Provider's report shall identify: (i) the nature of the unauthorized use or disclosure; (ii) the network element(s) and/or Data used or disclosed; (iii) who made the unauthorized use or received the unauthorized disclosure; (iv) what Provider has done, or shall do, to mitigate any negative effect of the unauthorized disclosure; and, (v) what corrective action Provider has taken, or shall take, to prevent future unauthorized use or disclosure.

Provider shall comply with all applicable laws that require the notification of individuals in the event of unauthorized release of personally identifiable information, any other event requiring such notification ("Notification Event"). OSU may, in its sole discretion, choose to provide notice to any or all parties affected by a Network or Data Breach, but the Provider shall reimburse OSU for the cost of providing such notification. Provider further agrees to provide, or to reimburse OSU for its costs in providing, any credit monitoring or similar services that are necessary as a result of Provider's Network or Data Breach.

c. **Auditing.** Ohio State reserves the right to perform audits as necessary. Ohio State will provide its request in writing and will work with the Provider to schedule time to conduct the audit.

IN WITNESS WHEREOF, the parties have executed this Addendum as of the day and year set forth above.

For The Ohio State University:

_____

Michael Papadakis Sr.
Vice President for
Business & Finance and CFO

_____

Date

For Supplier.:

_____

Name (please print)

_____

Title/Department

_____

Signature

_____

Date