A logo of a university

Description automatically generated

****

**DATA SECURITY ADDENDUM**

This Data Security Addendum to Supplier’s Contract (“DSA”) is between Regents of the University of Minnesota through its [INSERT DEPARTMENT NAME] (“University”) and the party indicated in the signature block (“Supplier”) and is incorporated by reference into the agreement executed simultaneously with this Addendum entitled [Title of Agreement] (the “Agreement”) between University and Supplier.

1. **Purpose and Scope of Application.** 
   1. This DSA is applicable only where the Supplier will create, obtain, transmit, use, maintain, process or dispose of University Data (as defined in herein) in order to fulfill its obligations to the University.
   2. Supplier agrees to be bound by the obligations set forth in this DSA. To the extent applicable, Supplier also agrees to impose the terms and conditions contained in this DSA on any third party retained by Supplier to provide services for or on behalf of the University.
   3. In the event of a conflict between the terms of this DSA and any other agreement related to the services provided to University by Supplier, including, but not limited to written or online terms and conditions, invoice terms, purchase order, or click-through agreement, the terms of this DSA shall control.
2. **HIPAA.** If the selected Supplier will create, receive, or come into non-incidental contact with individually identifiable health information of University patients or University Health Plan participants—“Protected Health Information” as that term is defined in regulations under the Health Insurance Portability and Accountability Act of 1996 ( “HIPAA”), at 45 C.F.R. Part 160.103—the Business Associate Addendum (“BAA”), found at <https://policy.umn.edu/contracts/standard/ogc-sc258> , applies in addition to this Data Protection DSA. If applicable, parties agree to enter into a BAA prior to the start of services. Any such BAA will be incorporated by reference to this DSA. Where noted herein, certain sections of the Business Associate Addendum replace sections of this Data Protection DSA as regards to Protected Health Information.
3. **Definitions.**
   1. “End User” means person(s) accessing and using the Services provided by the Supplier under the Agreement.
   2. “Personally Identifiable Information” includes but is not limited to personal identifiers such as name, address, phone number, date of birth, Social Security number, and student or employee identification number; “private data on individuals” and “nonpublic data” on individuals as defined in Minnesota Statute Chapter 13 and/or any successor laws of the State of Minnesota; personally identifiable information contained in student education records as that term is defined in the Family Educational Rights and Privacy Act, 20 USC 1232g; “protected health information” as that term is defined in the Health Insurance Portability and Accountability Act, 45 CFR Part 160.103; nonpublic personal information as that term is defined in the Gramm-Leach-Bliley Financial Modernization Act of 1999, 15 USC 6809; credit and debit card numbers and/or access codes and other cardholder data and sensitive authentication data as those terms are defined in the Payment Card Industry Data Security Standards; other financial account numbers, access codes, driver’s license numbers; and state- or federal-identification numbers such as passport, visa or state identity card numbers.
   3. “Securely Destroy” means an action that renders data written on physical (e.g., hardcopy, microfiche, etc.) or electronic media unrecoverable by both ordinary and extraordinary means. These actions must meet or exceed those sections of the National Institute of Standards and Technology (NIST) SP 800-88 guidelines relevant to data categorized as high security.
   4. “Security Breach” means a security-relevant event in which the security of a system or procedure used to create, obtain, transmit, maintain, use, process, store or dispose of data is breached, and in which University Data is exposed to unauthorized disclosure, access, alteration, or use.
   5. “Services” means any goods or services acquired by the University of Minnesota from the Supplier.
   6. “University Data” includes all Personally Identifiable Information, and any other information that is not purposefully made available to the public by the University, including but not limited to business, administrative and financial data, intellectual property, research, and patient, student and personnel data.
4. **Compliance with Laws.** Supplier agrees to comply with all applicable state, federal and international laws, as well as industry best practices, governing the collection, access, use, disclosure, safeguarding and destruction of University Data.
5. **Ownership of Data.** All University Data and/or content collected, created or prepared by or for the University in the performance of the Agreement is the exclusive property of the University. Supplier shall not use, willingly allow or cause to have University Data used for any purpose other than the performance of its obligations under the Agreement, without the prior written consent of the University. Supplier is granted a limited, nonexclusive license to use University Data as necessary to provide the Services in the Agreement. This DSA does not give a party any rights, implied or otherwise, to the other’s data, content, or intellectual property, except as expressly stated in the Agreement.
6. **Confidentiality of Data.** 
   1. Supplier will not disclose any University Data. It is understood that the University is a public institution, and, as such, is subject to the Minnesota Government Data Practices Act (“MGDPA”), Chapter 13. The Supplier agrees to maintain and protect data on individuals received, or to which the Supplier has access, according to the statutory provisions applicable to the data. No private, public, or confidential data developed, maintained or reviewed by the Supplier under the Agreement may be released to the public by the Supplier or its employees or representatives. The Supplier shall administer and protect any and all government data according to the provisions of the Minnesota Government Data Practices Act, codified at Minnesota Statutes Chapter 13. Supplier further acknowledges University data may be subject to protections under other federal and state laws and regulations and shall handle any such information in accordance with applicable law.
   2. Supplier shall use commercially reasonable efforts to notify all of its foreseeable agents, employees, subcontractors and assigns who will come into contact with University Data that they shall comply with, and are subject to the confidentiality requirements set forth in the agreement and shall provide each with a written explanation of the requirements for confidentiality before they are permitted to access University Data.
   3. Supplier’s storage of University Data outside the United States is prohibited without prior written consent from the University.
7. **Data Security.** Supplier attests that it has implemented administrative, physical and technical safeguards for its data security that at a minimum meet industry best practices. Supplier shall ensure that all such safeguards, including the manner in which data is collected, accessed, used, stored, processed, disclosed and disposed of, comply with applicable data protection and privacy laws and regulations, as well as the terms and conditions of the Agreement. Without limiting the foregoing, Supplier warrants that all electronic University Data will be encrypted, resting and in transmission (including via web interface), and all University Data will be stored in accordance with the latest version of National Institute of Standards and Technology Special Publication 800-122.
8. **Background Checks and Training.** Supplier will ensure that reasonable and appropriate background investigations are conducted on its employees and contractors in accordance with applicable laws and regulations. Supplier’s employees and contractors must pass background checks prior to being assigned to positions in which they will have access to University Data. Supplier will conduct annual mandatory security awareness training to inform its personnel on procedures and policies relevant to its information security program and of the consequences of violating such procedures and policies. Supplier will immediately remove terminated employee and contractor’s access to University Data.
9. **Notification of Breach.** Supplier will report to the University at security@umn.edu any Security Breach that could result in the unauthorized access, use, or disclosure of University Data immediately upon discovery, but in no event more than three (3) business days after Supplier reasonably believes a Security Breach has or may have occurred. Supplier will fully investigate the incident and cooperate fully with the University’s investigation of and response to the incident. Except as otherwise required by law, Supplier will not provide notice of the incident directly to individuals whose Personally Identifiable Information was involved, regulatory agencies, or other entities, without prior written permission from the University.
10. **Liability for Breach.** Supplier will reimburse the University in full for all costs incurred by the University in investigation and remediation of any Security Breach related to University data in Supplier’s possession or control, including but not limited to providing notification to individuals whose Personally Identifiable Information was affected and to regulatory agencies or other entities as required by law or contract; providing two years’ credit monitoring to the affected individuals if the Personally Identifiable Information exposed from the breach could be used to commit fraud or financial identity theft; and the payment of legal fees, audit costs, fines, and other fees imposed by regulatory agencies or contracting partners as a result of the Security Breach. Supplier further agrees to indemnify, defend, and hold harmless the University, its employees and agents, against any and all claims, damages, liability and court awards including costs, expenses, and attorney fees and related expenses incurred due to the unauthorized access, use, or disclosure of University Data. Liability for breach is excluded from any limits to liability stated elsewhere in any agreement or terms and conditions related to the services provided to University by Supplier.
11. **Termination for Breach.** Any Security Breach that results in the unauthorized access, use or disclosure of University Data is a material breach of the Agreement and the University may immediately terminate the Agreement by giving written notice to the Supplier. If the University terminates the Agreement due to a data security breach by the Supplier, the University shall be entitled to a refund of any monies paid in advance prorated to the effective date of termination.
12. **Return and Destruction of Data Upon Termination.** Regardless of cause, within 30 days of the termination, cancellation, expiration or other conclusion of the underlying agreement, Supplier will return any University data to the University and destroy any University Data remaining in Supplier’s possession thereafter. At the University’s sole discretion and election, the University may request in writing that Supplier (a) transfer all University Data to a third party and destroy any University Data remaining in Supplier’s possession thereafter; or (b) destroy all University Data in Supplier’s possession in lieu of returning such data to the University. Regardless of the disposition of University Data pursuant to this section, Supplier shall have no rights in or to University Data following termination, cancellation, expiration or other conclusion of the underlying Agreement. Transfer will occur without significant interruption in service. Supplier will ensure that such transfer/migration uses facilities and methods that are compatible with the relevant systems of the University or its transferee. University will have reasonable access to University Data during the transition. In the event the University elects to have its data destroyed, Supplier shall provide verified confirmation of the disposal of all University Data. Supplier will notify the University of any impending cessation of its business or that of a tiered provider. Supplier shall implement an exit plan and take all actions necessary to ensure a smooth transition of service with minimal disruption to University.  In the event that returning or destroying University Data is not feasible, Supplier must provide notification of the conditions that make return or destruction not feasible, in which case, the Supplier must continue to protect all University Data that it retains to the same level as its own confidential data and agree to limit further uses and disclosures.
13. **Response to Legal Requests for Data.** Except as otherwise expressly prohibited by law, Supplier will immediately notify the University of any subpoenas, warrants, or other legal orders, demands or requests received by Supplier seeking University data and consult with the University regarding its response. Supplier will cooperate with the University’s reasonable requests in connection with efforts by the University to intervene and quash or modify the legal order, and upon the University’s request, provide the University with a copy of its response. Supplier will take reasonable measures to ensure that UMN data is not included in a response to government, third party or legal requests for other cloud tenant's data.
14. **Data Integrity.** Supplier will take reasonable measures, including audit trails, to protect University Data against deterioration and degradation of data quality and authenticity. The Supplier will be responsible during the term of the Agreement, to collect and migrate electronic data as often as necessary so that University Data is not lost due to issues with Supplier’s hardware, software, or media obsolescence or deterioration.
15. **Data Segmentation**. Supplier will maintain University Data in instances that are logically separated from other customers' data.
16. **Log management**. Supplier will implement and maintain comprehensive log management practices, that at a minimum meet or exceed the University's Log Management Standard (https://policy.umn.edu/it/securedata-appm) and will ensure all access and activity logs are securely stored, regularly reviewed, and retained for a minimum of one year to facilitate security audits and incident investigations and make such logs available to the University upon University's reasonable request.
17. **Network Security.** Supplier agrees at all times to maintain network security that, at a minimum, includes network firewall provisioning, intrusion detection, regular third-party penetration testing and vulnerability scanning.  Supplier will ensure that security measures are regularly reviewed and revised to address evolving threats and vulnerabilities while Supplier has responsibility for University Data
18. **Data Access.** Supplier shall strictly control access to University Data and limit access to authorized personnel only. Supplier shall ensure employees and contractors with access to University Data authenticate using multi-factor authentication and Supplier must adhere to the principle of least privilege, ensuring employees and contractors only access University Data necessary for their role. Supplier shall conduct regular audits to monitor access patterns and ensure compliance with security policies.
19. **Data Loss Prevention.** Supplier agrees to implement and maintain robust Data Loss Prevention (DLP) measures to prevent the inadvertent or intentional compromise of University Data. Controls must exist to track activity, inspect network traffic, including email and other protocols, and filter/block certain user actions to ensure University Data remains secured.
20. **Patching.** Supplier agrees to maintain secure environments that are patched and up to date by installing all high risk or higher patches as soon as they can safely be installed, but in any event within 30 days from release of the patch from the vendor or open-source community.
21. **Security Audit.**Supplier will audit the security of the systems and processes used to provide the Services, including those of any data centers or third parties used by Supplier to provide the Services. This security audit (1) will be performed at least once every calendar year; (2) will be performed according SSAE-18 SOC2, International Organization for Standardization (“ISO”) 27001/27002, or FedRAMP; (3) will be performed by third party security professionals at Supplier’s election and expense; (4) will result in the generation of an audit report (“Audit Report”), which will, to the extent permitted by applicable law, be deemed confidential information and as not public data under the Minnesota Government Data Practices Act; and (5) may be performed for other purposes in addition to satisfying this section. Upon University’s reasonable, advance written request, Supplier will provide to the University a copy of the Audit Report, such as SSAE-18 SOC2 Type II. Supplier will make best efforts to remediate any control deficiencies identified in the Audit Report in a commercially reasonable timeframe. If University becomes aware of any other Supplier controls that do not substantially meet University’s requirements, University may request remediation from Supplier. Supplier will make best efforts to remediate any control deficiencies identified by University or known by Supplier, in a commercially reasonable timeframe.
22. **Right to Audit.** Supplier grants permission to the University to perform an assessment, audit, examination or review, at its own expense, to ensure compliance with the terms of this DSA. Supplier shall reasonably cooperate with such assessment. If necessary, Supplier will promptly modify its security measures as needed based on those results in order to meet its obligations under the Agreement.
23. **Service Levels.** If the Services provided under the Agreement are subscription-based SaaS services, or other cloud-based hosting or other services, the attached Service Level Agreement is incorporated. Supplier warrants that the Services will be performed in a professional and workmanlike manner consistent with industry standards reasonably applicable to such Services. Supplier further warrants that the services will be operational at least 99.99% of the time in any given month during the term of the Agreement, meaning that the outage or downtime percentage will be not more than .01%. In the event of a service outage, Supplier will (a) promptly and at Supplier’s expense use commercial best efforts to restore the services as soon as possible, and (b) unless the outage was caused by a force majeure event, refund or credit the University, at the University’s election, the pro‐rated amount of fees corresponding to the time Services were unavailable.
24. **Privacy Policy.** Language in the Supplier’s privacy policy, if applicable, reserving to Supplier the right to change the privacy policy without notice at any time is hereby amended to provide University with written Notice of any material change to the privacy policy no less than thirty (30) days prior to the date such language takes effect.  Supplier warrants that any privacy policy change will not materially reduce the level of protection afforded to University  or its end users.
25. **PCI-DSS Service Provider.** In the event Supplier may have access to credit or debit card information and/or may affect the security of a credit or debit card transaction, Supplier agrees to the Payment Card Industry Data Security Standards (PCI DSS) set out at [Cardholder Data Security](https://drive.google.com/file/d/1-3pbppzE83Pg5IuOkH-s56m3gp6Fg94G/view).
26. **CAN-SPAM Act.** If Supplier services involve email solicitation or email communication, the Controlling the Assault of Non-Solicited Pornography and Marketing Act (15 U.S.C. § 7701-13) (CAN-SPAM Act) regulates the transmission of all commercial e-mail messages. To the extent that the Supplier designs or initiates e-mail messages, Supplier agrees to comply with the requirements of the CAN-SPAM Act.
27. **Message Sending.** If Supplier sends messages (email, SMS, MMS, or similar) on the University’s behalf, Supplier agrees to (i) have a Domain-based Message Authentication, Reporting & Conformance (DMARC) policy in place and enforced and (ii) provide a Domain Keys Identified Mail (DKIM) signature to the University for any service that sends messages on its behalf. Supplier further agrees to adhere to the University’s message authentication standards throughout the duration of this Agreement.
28. **Additional Insurance.** In addition to the insurance required under the Agreement, Supplier at its sole cost and expense will obtain, keep in force, and maintain an insurance policy (or policies) that provides coverage for privacy and data security breaches. This specific type of insurance is typically referred to as Privacy, Technology and Data Security Liability, Cyber Liability, or Technology Professional Liability. Supplier must have limits of no less than $5,000,000 per occurrence or claim and $5,000,000 aggregate for the cyber policy. Coverage shall be sufficiently broad to respond to the duties and obligations as is undertaken by Supplier in the Agreement and shall include, but not be limited to, claims involving infringement of intellectual property, including but not limited to infringement of copyright, trademark, trade dress, invasion of privacy violations, information theft, damage to or destruction of electronic information, release of private information, alteration of electronic information, extortion and network security. The policy shall provide coverage for breach response costs as well as regulatory fines and penalties as well as credit monitoring expenses with limits sufficient to respond to these obligations.

**AGREED:**

|  |  |
| --- | --- |
| **Regents of the University of Minnesota**  By:  Name:  Title:  Date: | **Supplier** [INSERT SUPPLIER NAME]  By:  Name:  Title:  Date: |