Union Theological Seminary Data Security Rider

Last Updated: December 2023

Background

This contract rider must be added to all contracts with any service provider (also known as “vendor” and “data processor”), if the service provider, in connection with its services creates, obtains, accesses (via records, systems, or otherwise), receives from or on behalf of Union Theological Seminary or uses in the course of its performance of the contract UTS restricted data which includes, but is not be limited to:

- Social Security numbers,
- Credit card numbers, data protected by the Payment Card Industry Data Security Standard (PCI DSS), or other financial account information,
- Data protected by the Family Educational Rights and Privacy Act, as set forth in 20 U.S.C. §1232g ("FERPA"),
- Data protected by the Gramm-Leach-Bliley Act (GLBA), Public Law No: 106-102, or data protected by any other applicable federal or state law or regulation.
- If Protected Health Information (PHI) as defined by HIPAA is being accessed, a Business Associate Agreement is required. Contact the university Director of Privacy for assistance.

UTS represents that it has necessary rights to provide the Covered Data and Information (CDI) to the vendor for the processing to be performed in relation to the services. The service provider agrees to the terms of this contract rider.

Data Definition: Covered data and information (CDI) includes paper and electronic data classified as “Restricted”, or otherwise sensitive data as defined by the

Union Theological Seminary. This includes information supplied by the university or any individuals to the service provider.

Security Standards: UTS will determine the scope, purposes, and manner by which the CDI may be accessed and processed by the vendor. The vendor will process the CDI only as set forth in UTS's written instructions. All of the service provider's systems storing or processing CDI must comply with federal, state and local laws concerning data privacy, UTS's Data Governance and Classification Policy, Vendor Minimum Safeguards, and where applicable, the European Union's General Data Protection Regulation (GDPR).

Service provider shall develop, implement, maintain and use appropriate administrative, technical and physical security measures to preserve the confidentiality, integrity and availability of all electronically maintained or transmitted CDI received from, or on behalf of university or any individuals. The service provider will extend these security standards obligations to all subcontractors by contract.

- Service provider must supply documentation of compliance with any applicable laws and regulations upon request.
- All systems and applications shall undergo vulnerability assessments, such as testing patch level, password security, and application security in accordance with industry best practices, or will provide reports upon request if conducted by a third party.
- Service provider agrees to allow UTS to perform regular pen testing/vulnerability scans (operating system, patch, and application) in accordance with industry best practices.
- Routine event monitoring will be performed by the service provider; the service provider will immediately identify events related to unauthorized activity and unauthorized access.
- Service provider shall agree to forward unmodified system (and other appropriate) logs to the UTS Director of Technology.
- The service provider shall agree to undergo regular security audits, preferably by certified third parties, occurring at least annually, and any identified issues must be resolved within 90 days of the audit report. UTS may demand written proof of this audit at any time during the term of the contract.
- All services gathering Restricted data, or otherwise sensitive data as defined by UTS's policies must utilize secure communication methods, such as TLS, and use a certificate from an approved independent authority.
- All file transmissions involving CDI, or otherwise sensitive data as defined

by the seminary, must utilize secure communication methods; for example, TLS, SSH, SFTP.

- Service provider agrees to allow the use of Shibboleth authentication (or comparable authentication mechanism with seminary approval) if and when appropriate as requested by the university.
- Physical access to facilities where data is stored, whether production or backup, must reside within the continental United States. Any damage or unauthorized access to facilities must be reported to UTS within 24 hours of its discovery. If any unauthorized access to UTS's CDI occurred, the service provider must consult with UTS officials before notifying those affected by the unauthorized access.

Acknowledgment of Access to CDI: Service provider acknowledges that the Agreement allows the service provider access to CDI. Data access shall be limited to those with a "need to know" and controlled by specific individual(s). As required by law, at no time will UTS data be physically or logically accessible to a foreign national. The service provider must have procedures and solutions implemented to prevent unauthorized access, and the procedures will be documented and available for UTS to review upon request. All of the service provider's employees with access to UTS's CDI must be identified with names provided to the university upon request.

Prohibition on Unauthorized Use or Disclosure of CDI: Service provider agrees to hold CDI in strict confidence. Service provider shall not use or disclose CDI received from or on behalf of UTS (or any individuals) except as permitted or required by the Agreement, as required by law, or as otherwise authorized in writing by UTS. Service provider agrees not to use CDI for any purpose other than the purpose for which the disclosure was made.

International Data Transfers: In accordance with GDPR Article 44, Processor shall rely on a Valid Transfer Mechanism to transfer Personal Data for Processing (whether performed by Processor or by a Subprocessor) from the European Economic Area to another country.

Retention, Return or Destruction of CDI: Upon termination, cancellation, expiration or other conclusion of the Agreement, service provider shall return all CDI to UTS or, if return is not feasible, destroy any and all CDI. Destruction of CDI shall be carried out in accordance with UTS's data retention policies. UTS shall approve the method of data destruction prior to destruction. If the service provider destroys the information, the service provider shall provide UTS with a certificate confirming the date and method of destruction of the data.

Maintenance of the Security of Electronic Information: Service provider shall develop, implement, maintain and use appropriate administrative, technical and

physical security measures to preserve the confidentiality, integrity and availability of all electronically maintained or transmitted CDI received from, or on behalf of UTS or its students. These measures will be extended by contract to all subcontractors used by service provider.

Reporting of Unauthorized Disclosures or Misuse of Covered Data and Information: Service provider shall, within one day of discovery, report to UTS any use or disclosure of CDI not authorized by this Agreement or in writing by university. Service provider's report shall identify:

- The nature of the unauthorized use or disclosure,
- The CDI used or disclosed,
- Who made the unauthorized use or received the unauthorized disclosure,
- What service provider has done or shall do to mitigate any deleterious effect of the unauthorized use or disclosure,
- The corrective action service provider has taken or shall take to prevent future similar unauthorized use or disclosure,
- Service provider shall provide such other information, including a written report, as reasonably requested by UTS.

Remedies: If UTS reasonably determines in good faith that service provider has materially breached any of its obligations under this contract, UTS , in its sole discretion, shall have the right to require service provider to submit a plan of monitoring and reporting; provide service provider with a fifteen (15) day period to cure the breach; or terminate the Agreement immediately if cure is not possible. Before exercising any of these options, UTS shall provide written notice to service provider describing the violation and the action it intends to take. Service provider shall defend and hold UTS harmless from all claims, liabilities, damages, or judgments involving a third party, including UTS's costs and attorney fees, which arise as a result of service provider's failure to meet any of its obligations under this contract. Nothing in this paragraph limits any other remedies available to UTS.

Note: Inclusion of data provided by individuals into the terms of the contract will depend upon the contract and may not be needed.