



VILLANOVA DATA ADDENDUM

This Villanova Data Addendum (this “Addendum”) describes the terms and conditions applicable to any and all Villanova Data, regardless of whether specifically selected or described below. This Addendum amends the terms and conditions of the Agreement described below. In the event of a conflict between the terms and conditions of this Addendum and the terms and conditions of the Agreement, the terms and conditions of this Addendum will control with respect to the subject matter of this Addendum. For the purpose of this Addendum, “Villanova Data” means any data or information collected, created, received, stored, accessed, processed, transmitted, hosted or otherwise managed for or on behalf of Villanova University (“Villanova”), its employees, students, faculty, agents and representatives.

Company:	_____
	FULL LEGAL NAME
Agreement:	_____
	TITLE & DATE

I. SECURITY AND DATA PROTOCOLS

- a. Company represents, warrants and covenants that all Villanova Data will be stored on infrastructure within the United States. Company shall disclose in writing to Villanova the facility specifications and location where Villanova Data is stored and shall notify Villanova in writing prior to any changes in the location of Villanova Data. Such notification shall be made in advance to Villanova’s Chief Information Security Officer at the address below and via email to ITSecurity@villanova.edu. Company represents, warrants and covenants that Villanova Data will not be stored or managed by any third party or outside the continental United States without Villanova’s prior written consent. Any processing or other act or omission by any person that obtains access to or possession of Villanova Data through Company that would be a breach of this Addendum if committed by Company is deemed a breach of this Addendum by Company and Company shall so be responsible. Company will give Villanova prompt written notice of any material change to the terms and conditions of its storage and management of the Villanova Data. Company will maintain a business continuity plan and implement methods to address disaster recovery of data and shall provide satisfactory testing results of such plan to Villanova upon request.
- b. Company shall maintain a written information security program including documented policies, standards, and operational practices that meet or exceed the applicable requirements and controls set forth in this Addendum to the extent applicable. Upon request, Company shall provide contact information for the individual within the Company responsible for such information security program.
- c. Company will ensure that Villanova Data is stored and processed only as necessary to carry out its obligations under the Agreement and in accordance with commercial best practices, including implementing appropriate administrative, physical, and technical safeguards that are no less rigorous than generally accepted industry practices (such as current NIST (National Institutes of Standards and Technology) Cybersecurity Framework, ISO 27001/27002, or comparable current practices), to secure Villanova Data from unauthorized access, disclosure, alteration, and/or use. Company shall ensure that all such practices and safeguards, including the way Villanova Data is collected, accessed, used, stored, processed, disposed of, and disclosed, comply with all applicable international, federal, and state data protection and privacy laws, regulations, and directives, as well as the terms and conditions of the Agreement and this Addendum. Without limiting the foregoing, and unless expressly agreed otherwise in writing, Company represents and warrants that all electronic Villanova Data will be encrypted when transmitted and stored in compliance with generally accepted industry practices, specifically as follows, or comparable current practices and algorithms:

- i. encrypted in transit via TLS (Transport Layer Security) v.1.2 or higher using a minimum of 256-bit certificates and 2048-bit or better RSA public keys and signed by a trusted CA (certificate authority).
 - ii. encrypted at rest via Advanced Encryption Standard (AES) using 256-bit or better, including all back-up and replication, regardless of media or location.
- d. Under the Agreement or this Addendum, Company will maintain control processes and technologies aligned with industry standards that prevent introduction of any malware, malicious code or programs that may damage the systems or data or prevent the accessibility or use of Villanova Data or may permit unauthorized access to systems or data that may compromise the confidentiality, integrity or authorized accessibility of Villanova Data or associated information systems. In no event shall Villanova be responsible for any damages or loss caused by electronic data transmitted to Company.
 - e. Upon request by Villanova, Company will immediately take down, remove or disable access to any Villanova Data available on website(s) or any other public, private or semi-private platform.
 - f. Company will retain, transfer and destroy all copies of all Villanova Data in accordance with written instructions provided by an authorized representative of Villanova, and as required by the Agreement and this Addendum. As between Villanova and Company, Villanova retains all right, title, and interest in and to Villanova Data.
 - g. Company represents, warrants and covenants that the information provided in connection with Company's HECVAT (Higher Education Community Vendor Assessment Toolkit), SIG (Standardized Information Gathering) assessment, or equivalent questionnaire or assessment is true, correct and complete, and that Company will not materially decrease, reduce or diminish the policies, procedures and practices described therein without providing at least 60 days' advance written notice to Villanova.

II. ADDITIONAL TERMS FOR CERTAIN VILLANOVA DATA

The following requirements apply only in the event that Company creates, accesses, transmits or stores the specified type of Villanova Data in Company's performance under the Agreement or this Addendum.

- a. **SSN Records.** If Company creates, accesses, transmits or stores Villanova Data containing social security numbers ("SSN Records"), Company represents, warrants, and agrees that it will: (i) hold the SSN Records in strict confidence and will not use or disclose the SSN Records except as permitted or required by the Agreement, required by applicable law, or otherwise authorized by Villanova in writing; (ii) safeguard the SSN Records according to commercially reasonable administrative, physical and technical standards that are no less rigorous than the standards by which Company protects its own records containing SSNs or comparable sensitive data; and (iii) continually monitor its operations and take any action necessary to assure that the SSN Records are safeguarded in accordance with the terms of this Addendum. At Villanova's request, Company will provide Villanova a written summary of the procedures Company uses to safeguard the SSN Records.
- b. **Cardholder Data.** If Company creates, accesses, transmits or stores Villanova Data containing payment card records or cardholder data including credit card numbers, cardholder names, service codes or expiration dates ("Cardholder Data"), Company certifies that their Information Technology practices conform to and meet current Payment Card Industry Data Security Standard (PCI-DSS) requirements as defined by The Payment Card Industry Security Standards Council (PCI-SSC) at: <https://www.pcisecuritystandards.org>. Company will monitor these PCI DSS requirements and its Information Technology practices, and Company will promptly notify Villanova if its practices should not conform to such standards. Company will provide either a letter of certification to attest to meeting this requirement or, if subject to PCI-DSS or Payment Application Data Security Standard (PA-DSS), appropriate validation documentation as defined by the PCI-SSC. Company hereby accepts responsibility for such Cardholder Data that Company possesses, stores, processes, or transmits in accordance with Requirement 12.8.2. Company shall comply with the Payment Card Industry Data Security Standard (PCI-DSS) requirements for Cardholder Data that are prescribed by PCI-SSC member card brands, as they may be amended from time to time (collectively, the "PCI-DSS Requirements"). Company acknowledges and agrees that Cardholder Data may only be used for assisting in completing a card transaction, for fraud control services, for loyalty programs, or as specifically agreed to by PCI-SSC member card brands, for purposes of the Agreement or

as required by applicable law.

- c. **FERPA Records.** If Company creates, accesses, transmits or stores Villanova Data that is subject to the Family Educational Rights and Privacy Act ("FERPA"), 20 U.S.C. Section 1232g ("FERPA Records"), Company acknowledges and agrees that Company is under the direct control of Villanova with respect to the use and maintenance of the FERPA records and further represents, warrants, and agrees that it will:
 - 1. hold the FERPA Records in strict confidence and will not use or disclose the FERPA Records except as permitted or required by the Agreement, required by law, or otherwise authorized by Villanova in writing;
 - 2. safeguard the FERPA Records according to commercially reasonable administrative, physical and technical standards that are no less rigorous than the standards by which Company protects its own comparable confidential information;
 - 3. continually monitor its operations and take any action necessary to assure that the FERPA Records are safeguarded in accordance with the terms of the Agreement and this Addendum;
 - 4. not read the contents of any FERPA Records, and restrict access by Company's employees to FERPA records, except as necessary to process the transactions or store the data as required under the Agreement;
 - 5. use and retain FERPA Records only for the purposes for which they were intended; and
 - 6. at the request of Villanova, provide Villanova with a written summary of the procedures Company uses to safeguard the FERPA Records.
- d. **HIPAA Records.** If applicable, Company will execute a HIPAA Business Associate Agreement ("BAA") with Villanova. By executing a BAA, Villanova makes no representation or acknowledgement that it is a "covered entity", as that term is defined under HIPAA.
- e. **Non-Public Personal Financial Information.** If Company creates, accesses, transmits or stores Villanova Data that is subject to the Federal Trade Commission (FTC)'s Standards For Safeguarding Customer Information, 16 C.F.R Part 314 and the Gramm-Leach Bliley Act, Company will: (i) provide such information as reasonably necessary for Villanova to determine whether Company has appropriate safeguards for such Villanova Data and to oversee Company's handling of such Villanova Data, and (ii) at all times during the term of the Agreement and this Addendum maintain such safeguards as required by Villanova or Villanova's then-current information security plan.
- f. **Identity Theft Protection.** If Company creates, accesses, transmits or stores Villanova Data that is subject to the FTC's "Red Flags" Rules, 16 CFR Part 681, and the Fair and Accurate Credit Transactions Act of 2003, Company will take such actions to detect, mitigate and protect against identity theft as required by Villanova or Villanova's then-current Identity Theft Prevention Program. In the absence of specific instruction by Villanova, Company agrees to safeguard this data according to commercially reasonable administrative, physical and technical standards that are no less rigorous than the standards by which Company protects its own comparable confidential information.
- g. **EU GDPR.** If Company creates, accesses, transmits or stores Villanova Data that is subject to the European Union's Regulation (EU) 2016/679 ("Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data," or the "EU GDPR"), Villanova and Company agree as follows:
 - 1. For purposes of this Section, the terms Process/Processor/Processing, Personal Data, Third Country, International Organization, Member State, and Data Subject shall be defined and construed as set forth in the EU GDPR.
 - 2. Company agrees to implement appropriate technical and organizational measures in compliance with the requirements of the EU GDPR.
 - 3. Company shall not engage another Processor without prior specific or general written authorization of Villanova. If a general written authorization is provided, Company shall inform Villanova of any intended changes concerning the addition or replacement of other Processors and provide Villanova the opportunity

to object to such changes. If any other Processor is engaged, Company shall ensure that the Processor shall comply with all data protection obligations as set forth herein and otherwise required by the EU GDPR. Company shall remain fully liable to Villanova for the performance of any other Processor's obligations.

4. Company shall only engage in Processing (including with respect to subject matter, duration, nature and purpose of the Processing) as necessary to carry out its obligations under the Agreement and as set forth in greater detail therein. Company shall reasonably assist Villanova in carrying out any and all of its obligations under the EU GDPR, as applicable and within the scope of the Agreement. Company shall Process Personal Data only on documented instructions from Villanova, including with regard to transfers of Personal Data to a Third Country of International Organization, unless required to do so by European Union or Member State law to which Company is subject; in such a case, Company shall inform Villanova of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest. Company shall immediately inform Villanova if, in its opinion, an instruction infringes the EU GDPR or other European Union or Member State data protection provisions.
5. Company shall ensure that all personal authorized to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
6. Company shall take all measures as required by Article 32 of the EU GDPR. Company shall assist Villanova in ensuring compliance with Articles 32 and 36 of the EU GDPR, taking into account the nature of the Processing and the information available to Company. Company shall assist Villanova in responding to any requests of a Data Subject to the extent Processing occurs within the scope of the Agreement.
7. At the choice of Villanova, Company shall delete or return all Personal Data to Villanova after the end of the provision of services related to the Processing and delete existing copies unless European Union or Member State law requires storage of the personal data.
8. Company shall make available to Villanova all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the EU GDPR, including, but not limited to, participation in an audit.

III. CONFIDENTIALITY

- a. "Confidential Information" shall mean any and all Villanova Data, which may or may not be marked, and other proprietary information which is specifically marked as proprietary or confidential and which is disclosed by or on behalf of Villanova in any form in connection with the Agreement or this Addendum. During the term of the Agreement and indefinitely after the date of termination of the Agreement, Company (i) shall treat as confidential all Confidential Information provided by Villanova, (ii) shall not use such Confidential Information except as expressly permitted under the terms of the Agreement and this Addendum or otherwise authorized in writing by Villanova, (iii) shall implement reasonable procedures to prohibit the disclosure, unauthorized duplication, misuse or removal of such Confidential Information, and (iv) shall not disclose such Confidential Information to any third party. Without limiting the foregoing, Company shall use at least the same procedures and degree of care to prevent the disclosure of Confidential Information as it uses to prevent the disclosure of its own confidential information of like importance and shall in any event use no less than reasonable procedures and a reasonable degree of care.
- b. Notwithstanding the above, Confidential Information will not include information that: (i) was generally available to the public at the time it was disclosed; (ii) was known to Company at the time of disclosure as shown by written records in existence at the time of disclosure; (iii) was developed independently by Company prior to the disclosure, as shown by written records in existence prior to the disclosure; (iv) is disclosed with the prior written approval of Villanova; and (v) becomes known to Company from a source other than Villanova without breach of the Agreement or this Addendum by Company and in a manner which is otherwise not in violation of Villanova's rights. Company may disclose Confidential Information if required by a court order, administrative agency, or other governmental body, provided that Company shall provide reasonable advance notice to enable Villanova to seek a protective order or otherwise prevent such disclosure.

IV. DATA BREACH NOTIFICATION

- a. Immediately upon, but not later than 24 hours after becoming aware of a security incident or breach in which

Villanova Data is or may potentially have been accessed, used, altered, deleted or disclosed, Company will report to Villanova any such security incident or breach and take such corrective steps to remedy the incident or breach as requested by Villanova or required by law or applicable industry standards. Such report will be made to the Chief Information Security Officer, in writing at the address below, after a preliminary oral report by phone to 610-519-5605 and via email to ITSecurity@villanova.edu.

- b. Company will be responsible for all costs incurred in investigation and remediation of any security incident or breach in connection with the products or services provided by Company, including but not limited to providing notification to individuals whose personal data was compromised and to regulatory agencies or other entities as required by law or contract; providing credit monitoring to the affected individuals; 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 incident or breach. In addition to any other remedies available to Villanova under the Agreement, this Addendum, law or equity, Company will fully cooperate and reimburse Villanova in full for any costs incurred by Villanova in connection with such security incident or breach.

V. INDEMNIFICATION

- a. Company will indemnify, defend and hold harmless Villanova and its employees, trustees, faculty, students, representatives and agents from and against any and all liability, claim, loss, damages, cost and expense of any kind (including legal fees) for any claim resulting from, attributable to, or arising out of (i) any violation of any laws, statutes or governmental regulation or (ii) the willful misconduct, negligence (whether characterized as gross or otherwise), error, action or omission of Company, its directors, officers, employees, agents, contractors or subcontractors, including but not limited to breach of this Addendum or the Agreement, or (iii) any disclosure or loss of, inability to account for, or unauthorized access to Villanova Data. This indemnification shall not be limited in any way by a limitation of liability or similar clause in the Agreement.

VI. INSURANCE REQUIREMENTS

- a. Company, and any subcontractor thereof, shall, at its own expense, secure and maintain the following insurance during the longer of the term of the Agreement or the time that Villanova Data is stored by Company, in amounts not less than that specified for each coverage below.
 - 1. **Commercial General Liability** insurance including coverage for premises and operations, products and completed operations, contractual liability, and personal injury for all operations, written on an occurrence basis with limits not less than \$3,000,000 Each Occurrence, which must apply to ongoing operations. "Villanova University" must be named as an additional insured and such policy shall be primary and non-contributory to Villanova's insurance. The additional insured, primary, and non-contributory status shall be evidenced on the Certificate of Insurance.
 - 2. **Professional Liability (also known as "Technology Errors & Omissions")** insurance with limits not less than \$3,000,000 per claim for damages caused by acts, errors, omissions and negligent acts of Company's employees and agents arising out of Company's performance of professional services.
 - 3. **Cyber Liability/Network Security & Privacy Liability** coverage with limits not less than \$3,000,000 for liability and damages resulting from any misuse, misappropriation, unauthorized disclosure or other breach of private information and personally identifiable information, arising from the Company's or its subcontractor's performance of services. Such damages shall include notification costs and/or forensics costs, fines, penalties, and related damages.
 - i. In cases where personal health information (PHI), electronic personal health information (ePHI), electronic medical records (EMR) or FERPA records are involved, Cyber Liability/ Network Security & Privacy Liability coverage shall have a limit of not less than \$5,000,000 for liability and damages resulting from any misuse, misappropriation, unauthorized disclosure or other breach of private information and personally identifiable information, arising from the Company's or its subcontractor's performance of services is required. Such damages shall include notification costs and/or forensics costs, fines, penalties, and related damages.

- ii. The Cyber Liability/Network Security & Privacy Liability coverage can be satisfied by a stand-alone policy or via an endorsement to the Commercial General Liability or the Professional Liability/Technology Errors & Omissions policy. The Cyber Liability/Network Security & Privacy Liability coverage and its corresponding limits must be specifically evidenced on the Certificate of Insurance.
- b. If Company will be on Villanova's premises under the Agreement or this Addendum, Company, and any subcontractor thereof that will be on Villanova's premises, shall, at its own expense, secure and maintain the following insurance during the term of the Agreement in amounts not less than that specified for each coverage below. Company warrants and represents that any subcontractors will maintain Workers' Compensation, and Company further agrees to indemnify Villanova for any loss, cost, liability, expense and/or damage suffered by Villanova as a result of the failure of its subcontractors to maintain such insurance.
 1. **Automobile Liability** insurance (Bodily Injury Liability and Property Damage Liability) for all owned, leased, hired, non-owned vehicles with limits not less than \$3,000,000 Each Accident.
 2. **Workers' Compensation** for statutory obligations imposed by workers' compensation and occupational disease laws and include a waiver of subrogation in favor of Villanova, as permitted by law. The waiver of subrogation shall be evidenced on the Certificate of Insurance.
 3. **Employers' Liability** insurance shall be provided with limits of not less than \$500,000 for each subcategory of coverage.

If Company is a sole proprietor or otherwise not required by law to carry Workers' Compensation coverage, Company certifies that in lieu of Workers' Compensation coverage Company has health insurance to cover him/herself/themself, and anyone Company hires to provide services to Villanova on Company's behalf, to meet any and all needs for payment of medical costs for any injuries occurring on Villanova property or arising out of the services and/or products Company is providing.

Please initial here if Company is not required by law to carry Workers' Compensation: _____

- c. The limits required may be satisfied through primary insurance or any combination of primary and umbrella/excess liability insurance.
- d. Company or its insurers agrees to provide thirty (30) days advanced written notice to Villanova of any cancellation or material reduction in their or their subcontractor's required insurance.
- e. All insurance coverage must be written with an insurer rated not less than A- by A. M. Best.
- f. Villanova University (Villanova University, Attn: Insurance and Risk Management, 800 Lancaster Avenue, Villanova, PA 19085) shall be listed as the Certificate Holder on the Certificate of Insurance.
- g. A Certificate of Insurance evidencing the above coverages must be provided to Villanova at least one week prior to commencing work/providing services and/ or products to Villanova under the Agreement and as insurance policies renew during the term of the Agreement.
- h. Failure of Company, or any subcontractor thereof, to procure this insurance or of Villanova in securing a Certificate of Insurance shall not relieve Company, and any subcontractor thereof, of any obligation or liability assumed under the Agreement or this Addendum, nor of any obligation or liability imposed by law. In no event shall the liability of Company, or any subcontractor thereof, be limited to the extent of any insurance or the minimum limits required herein. Any self-insured retentions, deductibles, and exclusions in coverage in the insurance required shall be assumed by and at the sole risk of Company.

VII. CONFLICTS AND MODIFICATIONS

With respect to the Villanova Data, the terms and conditions of this Addendum supersede any conflicting terms and conditions in the Agreement, or any purchase order, work order, statement of work, terms of use, click-through, clickwrap or browse wrap terms or other terms made available, proposed or signed in connection with the Agreement or this Addendum or the products, services, equipment or technology provided in connection therewith. Any modifications must be agreed to in writing by Villanova or they shall be void and shall not apply.

VIII. TERMINATION

Company shall, in accordance with Villanova’s request, (a) no later than the effective date of any termination or expiration of the Agreement, in the form and format requested by Villanova, return or securely transmit to Villanova’s designee identified in writing by Villanova, all copies of Villanova Data, and/or (b) permanently destroy all copies of Villanova Data within sixty days of such termination or expiration, after providing notice to Villanova of Company’s intent to destroy such Villanova Data. In all instances, no Villanova Data shall be stored on or accessible via Company’s systems after sixty days following termination or expiration of the Agreement. At Villanova’s request, Company shall provide sufficient written verification of compliance with these obligations or permit a third-party company engaged by Villanova to conduct an audit to verify the Villanova Data has been appropriately handled. If such third-party audit shows Company has not complied with this Section, then Company shall reimburse Villanova for the cost of the first and subsequent audits until Company has complied.

IX. NOTICES

Unless otherwise directed in this Addendum or the Agreement all notices shall be sent to Office of the Vice President and General Counsel at the following address:

Villanova University
800 Lancaster Avenue
Villanova, PA 19085

For good and valuable consideration and intending to be legally bound, Company and Villanova have caused their duly authorized representatives to execute this Addendum below. This Addendum is effective as of the date of final signature below.

VILLANOVA UNIVERSITY

By: _____

By: _____

Name: _____

Name: _____

Title: _____

Title: _____

Date: _____

Date: _____