CONCORDIA UNIVERSITY

PERSONAL INFORMATION PROCESSING ADDENDUM APPLICABLE TO ALL CONTRACTS ENTERED INTO WITH CONCORDIA UNIVERSITY

Any supplier, consultant, company or any other person or entity (collectively and individually the "**Contracting Party**") that contracts with Concordia University ("**Concordia**") in any manner or form, including without limitation through a purchase order, an agreement, a contract, an amending agreement to an existing contract, a letter of intent, a statement of work, a quotation or any other instrument (collectively or individually, as the case may be, the "**Contract**") irrevocably agrees to the terms of this Personal Information Processing Addendum (the "**Addendum**"). Notwithstanding anything else to the contrary wherever contained, including, without limitation at law or in any Contracting Party terms and conditions, including any "entire agreement" type clause, this Addendum, at all times, prevails over the Contract and, any other terms of Concordia or the Contracting Party. This Addendum and its terms and conditions supersede, and apply to, the Contract, including other Contracting Party terms or purchase order, whether incorporated by reference or not, and whether listed in an agreement with Concordia or not, whether currently in existence or in existence in the future, and whether accepted online by Concordia or not. For greater certainty, the Addendum also prevails over any and all terms and conditions presented on a screen, by email, in a form or otherwise, whether or not such terms and conditions have been accepted by Concordia, an employee, one or more users or a student of Concordia. This Addendum can only be amended expressly, in writing, and any amendment thereto must be signed by an authorized Concordia representative pursuant to Concordia's Policy on Contract Review, Signing and Required Approvals.

WHEREAS, the parties have entered into a Contract;

WHEREAS, to perform its obligations under the Contract, the Contracting Party may be required to hold, host, store, control, possess or process Personal Information (as defined below) on behalf of Concordia;

WHEREAS, pursuant to sections 3 and 6 of the *Act respecting access to documents held by public bodies and the protection of personal information and on the Protection of Personal Information* (CQLR, c. A-2.1), (the "**Access Act**"), Concordia is a public body subject to the Access Act;

WHEREAS, section 67.2 of the Access Act allows Concordia to communicate Personal Information to any person or body without the consent of the persons concerned if such communication is necessary for the carrying out of an agreement, subject to the following conditions:

(a) the agreement must be entrusted in writing;
(b) such agreement must set out the provisions of the Access Act that apply to the information disclosed;
(c) such agreement must indicate the steps that the Contracting Party must take to ensure the confidentiality of the information, that the information is used only for the purpose of the performance of the agreement and that it is not to be retained after the expiry of the agreement;
(d) prior to disclosure, Concordia shall obtain an undertaking of confidentiality by any person to whom the information may be disclosed, unless Concordia's Privacy Officer deems it not necessary.

IN CONSIDERATION OF THE FOREGOING, THE CONTRACTING PARTY IRREVOCABLY AGREES AS FOLLOWS:

1. DEFINITIONS

In this Addendum, capitalized terms have the meaning ascribed to them below:

1.1. "**Concordia Data**" means any confidential information owned, held or controlled by Concordia and all Concordia information, including without limitation any confidential third-party information held by Concordia, any student data, application data, student details, examination and assessment results as well as all data and personal information which may identify individuals such as Concordia students, graduates, donors, professors or employees, collectively considered to be "**Personal Information**" under the Access Act. For greater certainty, but without limiting the generality of the above, all Concordia Data, whether kept in whole or in part locally or in Data Center(s), is considered to be Concordia Data.

1.2. "**Data Center(s)**" means any site or facility used to host and all or part of the Data.

1.3. "**Party**" means either Concordia or Contracting Party and "**Parties**" means Concordia and Contracting Party.

1.4. "**Privacy Officer**" means the person appointed by Concordia to be the person in charge of the protection of Personal Information for the purpose of the Access Act.

1.5. "**Security Incident**" means any breach of security leading to the accidental or unlawful processing, destruction, loss, alteration, copying, storage, damage, unauthorised disclosure of, or access to Concordia Data transmitted, stored or otherwise processed by Contracting Party under this Addendum.

1.6. "**Security Measures**" means the Contracting Party's security measures, which, at minimum comply and meet with those set forth in **Schedule A**.

1.7. "**Sub-contractor**" means any third party that has access to Concordia Data and which is engaged by Contracting Party to assist in fulfilling its obligations under the Contract. Sub-contractors may include Contracting Party affiliates but shall exclude Contracting Party employees, contractors and consultants.

1.8. "**Users**" means, as applicable, any individual to whom Concordia gives access to the Contracting Party's services, including any employee (full-time or part-time), student, consultant, employer, independent contractor or mandatary of Concordia.

2. DATA PROTECTION AND PRIVACY

2.1. Contracting Party agrees to comply with applicable privacy laws, including the Access Act ("**Privacy Laws**").

2.2. The following requirements concerning Personal Information apply and supersede everything, including the Contract and are an essential consideration for Concordia, without which it would not have entered into the Contract:

2.2.1. Acknowledgement. Contracting Party acknowledges that Concordia has obligations under the Access Act regarding the communication of Personal Information and as regards entrusting Personal Information with persons, whether for holding, using, or communicating such Personal Information. Contracting Party acknowledges that the information transmitted or communicated by Concordia may include Personal Information and that sections 53, 54, 56, 59, 63.1, 65, 65.1 and 67.2 of the Access Act apply to all Personal Information. In particular, when collecting Personal Information on behalf of Concordia, Contracting Party shall ensure that it complies with the information and openness requirements of section 65 of the Access Act.

2.2.2. Permitted Use. Concordia Data, including Personal Information, sent to, held by or made available to Contracting Party under the Contract is to be used solely for carrying out Contracting Party's obligations under the Contract and this Addendum. Contracting Party shall gather, keep, communicate, disclose, use, process or dispose of Concordia Data only in compliance with the Contract and this Addendum.

2.2.3. Prohibited Use. Other than as permitted under this Addendum, Contracting Party will not access, distribute, sell, licence, or transfer any Concordia Data, including any Personal Information, for its own purposes or for the benefit of any other party than Concordia.

2.2.4. Security Measures. Contracting Party shall implement and maintain appropriate and reasonable technical and organizational Security Measures designed to protect Concordia Data and safeguard Personal Information from Security Incidents and preserve the security and

confidentiality of Concordia Data, including Personal Information. Such measures shall include, at a minimum, those measures described in **Schedule A**. Contracting Party must take reasonable precautions to preserve the integrity of any Personal Information it processes and to prevent any corruption or loss of the Personal Information, including but not limited to, establishing effective back-up and data restoration procedures in compliance with Privacy Laws or other applicable laws.

2.2.5. Security Incidents. In the event that Contracting Party becomes aware of a Security Incident involving Concordia Data under Contracting Party's care or control, or any of its employees, mandataries or subcontractors, including hosting providers or hosting service providers, Contracting Party undertakes to immediately commence the measures provided for in the Security Measures and notify Concordia promptly of any such Security Incident.

2.2.6. Record Keeping. Contracting Party will maintain records of any Security Incident in accordance with Privacy Laws.

2.2.7. Notification. Contracting Party agrees that Concordia has the sole right to determine whether to provide notice of the Security Incident to any individuals concerned, regulators, law enforcement agencies or others, as required by Privacy Laws or other laws or regulations, or at Concordia's discretion, including the contents and delivery method of the notice.

2.2.8. Cooperation. Contracting Party will forthwith and fully cooperate with Concordia and Concordia's insurers, if applicable, and provide any other information that Concordia or Concordia's insurers may reasonably request including making available all relevant records, logs, files, data reporting, and other materials required to comply with Privacy Laws or as otherwise reasonably required by Concordia. Contracting Party shall give Concordia a confirmation that Contracting Party has also informed its insurers, if so required by Concordia. Contracting Party will restore the compromised data at its own expense.

2.2.9. Signed Undertakings. Contracting Party represents and warrants that all its employees, agents, mandataries and Sub-contractors have signed confidentiality undertakings at least as demanding as the confidentiality undertakings of this Addendum, a copy of which Concordia's Privacy Officer may request.

2.2.10. Audit and Verification. To verify Contracting Party's compliance with this Addendum, security requirements or Privacy Laws, following a confirmed Security Incident or where a regulatory authority requires it, Concordia may provide Contracting Party with 30 days' prior written notice requesting that a third-party conduct an audit of Contracting Party's facilities, equipment, documents and electronic data relating to the processing of Concordia Data under the Contract and the Addendum ("**Audit**"), provided that: (a) the Audit shall be conducted at Concordia's expense; (b) the Parties shall mutually agree upon the scope, timing and duration of the Audit; and (c) the Audit shall not unreasonably impact Contracting Party's regular operations. Concordia acknowledges that any written responses or Audit described in this article 2.2 shall be subject to the confidentiality provisions of the Contract and the Addendum.

2.2.11. Termination. Upon the termination for any reason of the Contract, or upon Concordia's request, Contracting Party must immediately return to Concordia all Concordia Data, including Personal Information (physical or digital) or, at Concordia's discretion, safely destroy all Concordia Data, including all Personal Information (physical or digital) in Contracting Party's control or possession. Subject to section 2.2.12, Contracting Party must not retain any copy of any Concordia Data, including Personal Information. Upon Concordia's request, Contracting Party must provide a solemn declaration, having the same force and effect as if made under oath, from an authorized officer of Contracting Party, either (i) that all Concordia Data, including Personal Information, has been remitted to Concordia, and that no copy remain

in its possession, and/or (ii) that all Concordia Data, including Personal Information has been destroyed.

2.2.12. Legal Requirements. If any law, regulation, or government or regulatory body requires Contracting Party to retain any documents or materials that Contracting Party would otherwise be required to return or destroy, it will notify Concordia in writing of that retention requirement, giving details of the documents or materials that it must retain, the legal basis for retention, and establishing a specific timeline for destruction once the retention requirement ends. Contracting Party may only use this retained Concordia Data for the required retention reason or audit purposes.

3. PRIVACY RIGHTS

3.1. Access and Rectification Requests. To the extent that Concordia is unable to independently access, delete or retrieve the relevant Concordia Data, Contracting Party shall, taking into account the nature of the processing, provide reasonable cooperation to assist Concordia in responding to any requests from individuals relating to their processing of Concordia Data as part of this Addendum. In the event that any such request is made to Contracting Party directly, Contracting Party shall promptly notify Concordia and shall not respond to the request directly (except to refer the individual to Concordia) without Concordia's prior authorization, unless legally compelled to do so.

3.2. General Cooperation**.** Each Party will reasonably cooperate with the other in any activities contemplated by this Addendum and to enable each Party to comply with its respective obligations under Privacy Laws.

4. SUB-CONTRACTORS

4.1. Authorization to Sub-Contract. If Contracting Party sub-contracts, in whole or in part, any of the Contracting Party obligations under the Addendum, then Contracting Party undertakes and agrees to solely use Sub-contractors whose Data Center(s) are located in Quebec and who process Data solely in Quebec or in a State or jurisdiction deemed acceptable by Concordia pursuant to the Access Act, as set out in **Schedule B**.

4.2. Responsibility. Contracting Party is solely responsible for ensuring compliance with the above requirement. Contracting Party will restrict Sub-contractors' access to Concordia Data to what is necessary to assist Contracting Party in performing the Contract and will remain responsible for any acts or omissions of Sub-contractors to the extent they cause Contracting Party to breach its obligations under this Addendum. Contracting Party shall enter or has entered into written agreements with its Sub-contractors that contain terms substantially the same as those set out in this Addendum and, upon Concordia's written request, shall provide Concordia with copies of such agreements.

5. DATA CENTER(S)

Contracting Party agrees, represents and warrants that the Data (including any back up) will be hosted in Data Center(s) located in Quebec or in a State or jurisdiction deemed acceptable by Concordia pursuant to the Access Act, as set out in **Schedule B** (the "**Acceptable Jurisdictions**") and that any Data processing will, at all times, be carried out in Acceptable Jurisdictions.

6. INDEMNITY AND LIMITATION OF LIABILITY

6.1. The Contracting Party shall indemnify and hold Concordia harmless (the "**Indemnifying Party**") and take up Concordia's (the "**Indemnified Party**") defense from and against any Claims,

which may be made against the Indemnified Party or which Indemnified Party may incur as a result of, arising from or relating to: (i) a breach of this Addendum; (ii) any negligence or fault of the Indemnifying Party; (iii) any security breach for which the Indemnifying Party is responsible and which results, in whole or in part, in the loss, transmission, disclosure, corruption, or other adverse effects, of the Indemnified Party's information, including without limitation, the Concordia Confidential Information. There is no limitation of liability of the Contracting Party with regards to these indemnifications.

For the purposes of this Section, the Indemnifying Party shall, in each instance, indemnify, defend and hold the Indemnified Party harmless from and against any and all Claims incurred by it with respect to all acts, omissions, negligence, fault, breaches and the like of the Indemnifying Party and those for whom in law the Indemnifying Party is responsible.

6.2. This section 6 (Indemnity and Limitation of Liability) supersedes and supplements the sections regarding liability in the Contract and shall survive the expiration or termination of the Contract and the Addendum for any reason whatsoever.

6.3. Subject to the terms of this Addendum, any limitation of liability applicable to the Contracting Party is mutual and applies to Concordia's liability towards the Contracting Party.

7. TERM AND TERMINATION

7.1. Term. Contracting Party shall be bound by this Addendum for as long as Contracting Party holds, stores, hosts, controls, possesses or maintains any Concordia Data received, accessed, collected, generated, or otherwise processed on behalf of Concordia for the performance of the Contract or the Addendum. For clarity, notwithstanding anything else in the Contract, the termination of the Contract or this Addendum does not relieve Contracting Party of its obligations and commitments obligations and commitments regarding the protection of Personal Information. Failure to comply with this Addendum shall constitute a default entitling Concordia to terminate the Contract subject to all of Concordia's recourses hereunder or at law.

7.2. Effect of Termination Survival. If the Contract is terminated, Contracting Party shall refer to section 7.1 of this Addendum.

8. NOTICES

8.1. Notices. All notices or other communication required or permitted to be given under this Addendum may be given via email transmission, or first-class mail, sent to the designated representatives identified on the first page of this Addendum.

9. MISCELLANEOUS

9.1. Priority of Agreements. Except for the changes made by this Addendum, the Contract remains unchanged and in full force and effect. If there is any conflict between this Addendum and the Contract, this Addendum shall prevail to the extent of that conflict.

9.2. Severability. In case any provision in this Addendum shall be invalid, illegal or unenforceable, the validity, legality and enforceability of the remaining provisions shall not in any way be affected or impaired thereby and such provision shall be ineffective only to the extent of such invalidity, illegality or unenforceability.

9.3. Governing Laws. This Addendum shall be governed by the laws of Quebec and the laws of Canada applicable in the province of Quebec, to the exclusion of any other, and the Parties attorn to the sole jurisdiction of the courts of the province of Quebec, Canada, District of Montreal.

9.4. Waiver. No delay or omission by either party to exercise any right under this Addendum shall be construed as a waiver of any such right and both parties reserve the right to exercise any such right from time to time, as often as may be deemed expedient.

9.5. Language. It is the express wish of the parties that this Addendum be drawn up in English only. *Il est de la volonté expresse des parties que le présent Addendum soit rédigé en anglais seulement.*

SCHEDULE A

SECURITY MEASURES

ID	Control Domain	Requirement
EG-GOV-1	Governance framework	A documented security management framework is in place.
EG-GOV-2	Governance framework	A Contracting Party information security policy is drafted, published and regularly updated.
EG-GOV-3	Governance framework	Contracting Party has diagrams of the overall architecture of the Solution, including a complete description of Concordia Data flow.
EG-GOV-4	Governance framework	Contracting Party has a documented and currently implemented employee onboarding and offboarding policy.
EG-GOV-5	Governance framework	Contracting Party has a documented change management process that includes at a minimum authorization, impact analysis, testing, and validation before putting changes into production.
EG-GOV-6	Governance framework	The organization chart, mission statement and policies of Contracting Party's information security unit are documented.
EG-GOV-7	Governance framework	Contracting Party has a policy and procedure, currently implemented and up-to-date, to manage how critical patches are applied to all systems and applications.
EG-GOV-8	Governance framework	Contracting Party has a policy and procedure, currently implemented and up-to-date, governing risk assessment and mitigation for Contracting Party's organization and supply chain.
EG-GOV-9	Governance framework	Information security principles are integrated into the Solution lifecycle and documented.
EG-GOV-10	Governance framework	A physical security policy is documented, implemented and regularly updated.
EG-GOV-11	Governance framework	Contracting Party has a vulnerability management program/process.
EG-GOV-12	Governance framework	Contracting Party has an implemented an up-to-date data media and data carrying material handling process that meets business needs and regulatory requirements, including end-of-life, reuse and remediation procedures.

EG-HR-1	Human Resources Security	Contracting Party requires new employees to complete non-disclosure agreements and read Contracting Party information security policies.
EG-HR-2	Human Resources Security	Contracting Party has an information security awareness program.
EG-HR-3	Human Resources Security	Security awareness training is mandatory for all Contracting Party employees and consultants. It is carried out regularly and participation is monitored.
EG-CONSU-1	Consultants	Contracting Party's contractual relations with its consultants are supervised and documented.
EG-CONSU-2	Contracting Party, consultants, sub-contractors and sub-processors	Access by Contracting Party and its consultants, sub-contractors and sub-processors to Concordia's Data will be limited to what is strictly necessary for the accomplishment of Contracting Party's obligations under the Contract, in accordance with the terms of this Addendum.
EG-SEC-1	Solution security	Contracting Party's solution does not require access to Concordia's location data or GPS data.
EG-SEC-2	Solution security	Contracting Party has a web application firewall (WAF).
EG-SEC-3	Solution security	Antivirus protection is deployed on all Contracting Party workstations and the distribution of signatures is managed centrally.
EG-SEC-4	Solution security	If the Contracting Party solution is an app, it is available from a trusted source (e.g. App Store, Google Play Store, company portal).
EG-SEC-5	Solution security	A separation of tasks between security administration, system administration and standard user functions is maintained.
EG-SEC-6	Solution security	Development, test and operating environments are strictly separated.
EG-SEC-7	Solution security	Contracting Party's developers are trained in secure coding techniques.
EG-SEC-8	Solution security	Contracting Party's solution was developed using secure coding techniques.
EG-SEC-9	Solution security	Contracting Party's code has undergone static code analysis and/or static application security testing before release.
EG-SEC-10	Solution security	Contracting Party's software testing processes (dynamic or static) are established and followed.
EG-SEC-11	Solution security	Penetration tests are carried out regularly.
EG-DATH-1	Data hosting	All of Contracting Party's hosting providers (Data Centers) have a SOC 2 Type 2 report.
EG-NSEC-1	Network security	Contracting Party uses a modern firewall configured to deny by default and fail secure.

EG-NSEC-2	Network security	Contracting Party has a documented policy for firewall change requests, including roles and responsibilities.
EG-NSEC-3	Network security	Contracting Party uses a network-based and host-based intrusion detection or prevention systems
EG-NSEC-4	Network security	Contracting Party monitors intrusions 24/7/365.
EG-NSEC-5	Network security	Contracting Party's audit logs are available for all changes to the network, firewall, IDS, and IPS systems.
EG-NSEC-6	Network security	Multi-factor (MFA) authentication must be used including privileged access to the solution and related components.
EG-A&C-1	Audits and certifications	Contracting Party carries out internal audits framed and documented in policies and procedures.
EG-A&C-2	Audits and certifications	Contracting Party carries out external audits supervised and documented in policies and procedures.
EG-A&C-3	Audits and certifications	Safety audits of third-party business with which Contracting Party shares data are carried out and are part of a global third-party management process.
EG-INC-1	Incident Management	Contracting Party has a formalized incident management process
EG-INC-2	Incident Management	Contracting Party has an internal or external incident response team.
EG-INC-3	Incident Management	Contracting Party has the capacity to respond to incidents 24 hours a day, 7 days a week and 365 days a year.

EG-INC-4	Incident Management	In the event of unauthorized loss, destruction, access, modification or use of sensitive or confidential information, Concordia Data, including Personal Information (a "**Security Incident**"), the Contracting Party must provide to Concordia the following detailed information regarding the Security Incident to be reported or reported without delay: - Where and when did the incident occur? - Who reported it and to whom and when was it reported? - What information/data was targeted? - Who provided the information/data? - How long has the information/data or electronic device been vulnerable to unauthorized access and who could have accessed it in this way? - Is there any information/data that has been extracted or has had its integrity compromised? Is there any electronic device which had its integrity compromised?
EG-VULN-1	Vulnerability management	Contracting Party systems and applications are regularly subject to an external analysis to detect vulnerabilities.
EG-VULN-2	Vulnerability management	Contracting Party systems and applications have been the subject of a security evaluation by a third party over the past year.
EG-VULN-3	Vulnerability management	Contracting Party systems and applications are analyzed using an authenticated user account to detect vulnerabilities that will be corrected before new versions.
EG-VULN-4	Vulnerability management	Contracting Party monitors and protects against vulnerabilities in web applications (for example, SQL, XSS, XSRF injection, etc.).
EG-VULN-5	Vulnerability management	Contracting Party has pre-determined remediation deadlines in correlation with the CVSS score of vulnerabilities.
EG-VULN-6	Vulnerability management	Contracting Party, or an external partner, actively manages the deployment of patches and associated processes (software updates, security fixes).
C-GOV-1	Governance framework	Contracting Party has appointed a data protection officer.
C-GOV-2	Governance framework	Contracting Party's organization has a documented Data privacy policy.
C-ACC-1	Access and authentication	Access control is based on roles (RBAC), attributes (ABAC), or on policies (PBAC).
C-ACC-2	Access and authentication	The entire life cycle of access to Confidential Information, including Personal Information, is supervised and documented.
C-ACC-3	Access and authentication	Privileged access is subject to different management and controls compared to standard access.

C-ACC-6	Access and authentication	The complexity of the passwords of Concordia's organization are supported by Contracting Party solution.
C-ACC-9	Access and authentication	All stored passwords are encrypted.
C-ENC-1	Encryption	All Concordia Data, including Personal Information, is encrypted at rest and in transit. The Contracting Party Solution must utilize 256-bit SSL encryption, or latest higher standards, between user sessions and application tier for any module or sub-module for non-public information. Encryption must be maintained at rest and in transit.
C-ENC-2	Encryption	All Contracting Party backups must be encrypted to an industry standard and at a minimum utilizing 256-bit SSL encryption.
C-DATH-1	Data hosting	The Data entrusted by Concordia is stored in Quebec or in a state/country listed in Schedule B of the Personal Information Addendum.
C-PHY-2	Physical security	Physical access is controlled and secure by means of badge, cameras, security staff. They are logged and recorded so that they can be traced and audited at any time.
C-PHY-3	Physical security	Clean desk and clear screen policies are applied by Contracting Party at all times.

SCHEDULE B

ACCEPTED JURISDICTIONS

As of March 25, 2024

Canada
USA
Any provider that has certified its participation in the EU-US Data Privacy Framework and is registered as a participant in the program.

Andorra
Austria
Belgium
Bulgaria
Croatia
Cyprus
Czech Republic
Denmark
Estonia
Faroe Islands
Finland
France
Germany
Greece
Guernsey
Hungary
Iceland
Ireland
Isle of Man
Israel
Italy
Japan
Jersey
Latvia
Liechtenstein
Lithuania
Luxembourg
Malta
Netherlands
New Zealand
Norway
Poland
Portugal
Romania
Slovakia
Slovenia
South Korea
Spain
Sweden
Switzerland
United Kingdom