**Form for Review of a Contract for Cloud Services:**

**Questions To Be Asked Re Privacy and Security for Personal Information**

Personal information (“PI”) means any information that can, directly or indirectly, identify someone. The law, especially Ontario’s *Freedom of Information and Protection of Privacy Act* (“FIPPA”), generally, with some limited exceptions, prohibits disclosure of PI without the consent of the individual to whom the PI relates. The protection of PI from unauthorized access and disclosure in cloud systems is of major concern. Accordingly, great care should be taken in reviewing contracts involving the collection, use, transfer, retention, and disposal of PI in cloud systems.

Following are standard questions that University units (“Units”) contemplating cloud service contracts involving PI should ask. If assistance is required, please consult:

* the University’s General Counsel via the Law Clerk on general matters;
* the Director of the Technology Services Centre regarding security and technical matters; and
* the Director of Risk Management and Access to Information regarding privacy matters

Please email to all three officers a copy of this form, completed to the best of your ability, along with a full copy of the contract including all appendices or schedules if applicable, and any supporting documentation relevant to the cloud service provider’s operations. If this is a contract renewal, please ensure that a signed copy of the agreement being renewed is included or has been provided in the past.

**I. Questions Concerning the Cloud Service Provider and Its Services:**

(The cloud service provider whose services you are considering should be able to assist you with answers to most of the questions in Part I):

|  |
| --- |
| (1) Please provide a summary of the services (“Services”) that the cloud service provider (the “Vendor”) will provide under the contract:*Answer*: |
| (2)(a) Does the Vendor have a Privacy Policy(-ies)? |  Yes | No |
|  (b) Does the Vendor have a Security Policy(-ies)? | Yes | No |
|  (c) Does the Vendor have a Data Retention Policy (-ies)? | Yes | No |
|  (d) Does the Vendor have an Incident Management Protocol? | Yes | No |
|  (e) Does the Vendor have a Disaster Recovery Protocol? | Yes | No |
|  (f) Does the Vendor require users of its services to agree to terms and conditions prior to use? | Yes | No |
|   (g) If the answer to any of (a), (b), (c), (d), (e), and (f) is “Yes”, the policies, protocols, and terms & conditions should be included in the contract review. If they have links, copy them here:*Comment*: |
| (3) How does the Vendor authenticate users of its system?*Answer*: |
| (4) Is the PI encrypted both in transmission and at rest - or only in transmission?*Answer*: |
| (5) What is the level of encryption (should be at least industry standard)? *Answer*: |
| (6) What processes does the Vendor employ to "harden" their Services system/platform (to improve their system's/platform’s security).*Answer*: |
| (7) Does the Vendor have at least System and Organization Controls (“SOC”) Type 2 certification or some other independent and comprehensive audit of the Vendor’s cloud security and privacy controls (for example, the Higher Education Community Vendor Assessment Toolkit (“HECVAT”))? | Yes | No |
| (a) *If the audit report is not SOC 2 or HECVAT please describe it here*: |
| (b) If there is certification or audit of any kind, has it been attached to, or supplied with, this Report? | N/A | Yes | No |
| (8) What PI, if any, does the Vendor pass on to third parties - and for what purposes?*Answer*: |
| (9) What internal security measures does the Vendor have in place - with regard to both its own employees' and its subcontractors' (if any) access to and handling of PI?*Answer*: |
| (a) In particular, does the Vendor give employees and sub-contractors access only to PI that they need to carry out their duties vis-à-vis services to the | Yes | No |
| University, the Vendor’s essential internal operations, and compliance with legal requirements?*Comment*: |
| (b) In particular, what security measures does the Vendor have in place at the point of recruiting its personnel (e.g. criminal records checks)?*Answer*: |
| (c) In particular, does the Vendor have Non-Disclosure Agreements (“NDA’s”) with its employees and contractors to preserve the confidentiality of the PI? | Yes | No |
| *Comment*: |
| (10) What is the Vendor’s protocol, especially vis-à-vis the Unit, for responding to statutory or other legal requirements (e.g. court orders) to disclose PI to a government agency or other third party?*Answer*: |
| (11) Where is the Vendor’s equipment storing the PI physically located?*Answer*: |
| (12) What security measures for its hardware/equipment (e.g. servers) does the Vendor have in place?*Answer*: |
| (13) For how long does the Vendor preserve PI in its system?*Answer*: |
| (14) How does the Vendor discard PI - and with what security?*Answer*: |
| (15) What are the Vendor’s processes for backup and disaster recovery?*Answer*: |
| (16) What protocol(s) does the Vendor have in place to respond to a breach of its system?*Answer*: |
| (17) What processes does the Vendor have in place to handle user queries regarding their PI, including without limitation the right to be forgotten if applicable?*Answer:* |
| (18) If the cloud service is likely to be extended to University clients, including students or prospective students, in the European Union, does the Vendor’s treatment of the PI meet GDPR requirements? | N/A | Yes | No |
| *Comment*: |

**II. Questions for the University Unit Seeking the Vendor’s Services:**

(Questions in Part II should be answered primarily by the University unit seeking the Vendor’s services)

|  |
| --- |
| (19) Exactly what Unit/University PI will the Vendor’s system collect, use, and store?*Answer*: |
| (20) What processes will the Unit have in place to ensure security of PI collected for the Services?*Answer*: |
| (21) What processes will the Unit have in place to ensure security of PI collected and used from the Services (in e.g. reports, summaries, analyses, etc.)?*Answer*: |
| (22) What processes will the Unit have in place to ensure security of logins into the Vendor’s system/platform (e.g. which Lakehead staff will have authority to log into the system/platform - and by what confidentiality and security rules will they be bound?)?*Answer*: |

|  |  |  |
| --- | --- | --- |
| (23) Will integration of the Vendor’s system in the Unit’s operations open any exposures to the University’s own computer systems and databases? (Consultation with TSC will be necessary to answer this question) | Yes | No |
| *(a) If the answer is “Yes” please elaborate:* |
| (*b) If the answer is “Yes” please describe how such exposures will be reduced to the level of acceptable risk*: |
| (24) If the Unit adopts the cloud system, will it, at the point where Unit clients use the system, provide the clients with a Collection Notice (see FIPPA  | Yes | No |
| section 39(2)) briefly but clearly indicating the purpose(s) of PI collection and the contact information of a University officer who can answer questions on the collection? Provide a draft of the Collection Notice under “Comment” (the Director of Risk Management and Access to Information can help here):*Comment*: |
| (25) Does the Unit have an exit strategy should the Vendor suddenly: |
| (a) go out of business? | Yes | No |
| (b) cease to offer the contracted services? | Yes | No |
| (c) require unacceptable terms at the time of renewal? | Yes | No |
| *Comment:* |

|  |  |  |
| --- | --- | --- |
| (26) Does the Unit understand that the contract with the Vendor does **not** remove the Unit’s and University’s ultimate responsibility and liability for protecting and securing PI should the Vendor’s system be breached - even though the Unit no longer has complete control over that PI? | Yes | No |