Third Party Service Provider Privacy and Security Standards

DISTRIBUTED ON JULY 30, 2019
HUMBER COLLEGE INSTITUTE OF TECHNOLOGY & ADVANCED LEARNING
205 HUMBER COLLEGE BLVD, TORONTO, ON M9W 5L7

HUMBER

Table of Contents

1. Definitions

1.1 **Access**: in connection with Personal Information means being accessed by a person, whether or not that person reviews or otherwise uses the Personal Information;

1.2 **Personal Information**: means information in the custody or under the control of Humber College that is defined as personal information in the *Freedom of Information and Protection of Privacy Act* (Ontario) ("FIPPA"), including without limitation, information about identifiable students of Humber College.

1.3 **Services**: means any service provided or technology included in a system or product provided to Humber based upon a predetermined service offering or engagement.

1.4 **Stored:** means held, backed up, collected, saved or archived by any means whatsoever, including in hard and electronic formats and includes storage in a server or database or any form of electronic memory.

1.5 **Third Party Service Provider:** ("Third Party") means any vendor or consultant hired by Humber College to provide products and/or services to the College.

1.6 **Service Agreement:** ("Service Agreement") is an agreement between any vendor and Humber College where the vendor agrees to provide product or services to College.

1.7 **Software Development Life Cycle (SDLC):** ("SDLC") is a framework provided by vendors defining tasks that will be performed at each step in the software development process at Humber College.

1.8 **Change Management:** is the process that aims to control the lifecycle of all Changes. It enables beneficial Changes to be made, with minimum disruption to IT Services.

1.9 **Change Advisory Board (CAB):** ("CAB") is a body that exists at Humber College to support the authorization of change and to assist Change Management in the assessment and prioritization of change.

2. Application of FIPPA, Personal Information

2.1. Humber College is subject to FIPPA, which imposes requirements and limitations in relation to the collection, use, disclosure, protection, retention and destruction of Personal Information and provides individuals with rights in relation to their own Personal Information.

2.2. Third Party Service Providers shall provide the Services in accordance with the Service Agreement and these Standards and more generally, in a manner that permits Humber College to comply with its obligations in relation to Personal Information under FIPPA.

2.2.1. Third party Providers will require access to Personal Information to provide some of the Services.

3. Ownership of Personal Information

3.1. Nothing in the Agreement shall be interpreted or construed to give Third Party any interest in, or right to Personal Information and between Humber College and the Third Party, Humber College owns and shall continue to own Personal Information.

4. Restrictions on Use, Prohibition on Disclosure of Personal Information

4.1. The Third Party may only use Personal Information to the extent necessary for the delivery of the Services being provided to Humber.

4.2. Unless Humber College otherwise expressly directs the Third Party in writing, the Third Party shall not disclose Personal Information. For greater clarity, the use of Personal information in accordance with these Standards by employees and agents of the Third Party does not constitute a disclosure of Personal Information by the Third party to such employees and agents.

4.3. If the Third Party is asked to provide access to Personal information or to correct Personal information by an individual other than Humber College, the Third Party shall advise the individual that Personal Information is under the control of Humber College and direct the person to Humber College.

5. Protection of Personal Information

5.1. Third Party's shall only make Personal Information available to those of its employees, agents and representatives who require access for the purpose of delivering the services, have been informed of the obligations under these Standards, and have agreed to act in accordance with these Standards and any Service Agreement.

5.2. Subject to Section 6.1, except with the express prior written approval of Humber College,

5.2.1. Personal Information held by Third Party in accordance with this Standard shall be held in a secure physical and electronic environment meeting or exceeding industry standards relating to the protection of sensitive personal information.

5.2.2. Personal Information available to the Third Party under this Standard **shall not be transferred or stored off Humber College property or on Third Party's servers.**

5.2.3. The Third Party shall ensure that Personal Information is not transferred to or accessed from outside of Canada, including without limitation transferred to or accessed by the Third Party's employees, agents and representatives who are outside of Canada.

5.3. The Third Party shall cooperate with Humber College, acting reasonably, in providing information and assistance for the completion of assessments including without limitation privacy impact assessments and threat risk assessments in relation to the Services being provided.

5.4. The Third Party shall ensure that any sub-contractor retained to assist it in providing the Services agrees to comply with the restrictions and conditions in relation to Personal Information in this Standard and Third Party shall be responsible for the acts and omissions of its sub-contractors in relation to Personal Information.

5.5. Subject to a written direction from Humber College to securely destroy Personal Information upon the expiry or termination of any Service Agreement or engagement, or at any other time on the written direction of Humber College, the Third Party shall forthwith return all Personal Information to Humber College or transfer it by means directed by Humber College.

5.6. At Humber College's request, the Third Party shall certify in writing over the signature of one of its officers, that all Personal Information, which the Third Party was holding has been securely destroyed in a non-recoverable fashion; securely transferred or securely returned to Humber College.

5.7. The Third Party shall not, and forever waives any right to withhold any Personal Information from Humber College to enforce any alleged payment obligation or in connection with any dispute between the Third Party and Humber College.

5.8. The Third Party shall not transfer Personal Information without written Humber College approval of the means of transfer.

6. Compliance with Law Applicable in Ontario

6.1. Nothing in this Standard shall be interpreted or construed to prohibit the Third Party from complying with any valid Court order made under the laws of Ontario or the laws of Canada applicable in Ontario (but not an order made under the laws of any other jurisdiction) on written notice to Humber College.

7. Notice of Non-Compliance, Breach, Investigation

7.1. If for any reason, the Third Party does not comply, or anticipates that it will be unable to comply with this Standard in any respect, the Third Party shall promptly notify Humber College of the particulars of non-compliance or anticipated non-compliance and of the steps, it proposes to take to address non-compliance, prevent its recurrence and prevent the anticipated non-compliance.

7.2. The Third Party shall notify Humber College within twenty-four (24) hours upon learning of:

7.2.1. any breach or attempted breach of security or privacy that could impact Personal Information, including any theft, loss, or unauthorized access, use, modification, disclosure or destruction of Personal Information; and/or

7.2.2. A complaint or investigation involving Personal Information.

8. Relief

8.1. Any material breach of this Standard by the third party shall constitute grounds for termination of the Service Agreement or engagement by Humber College without cost, penalty, or liability to Humber College.

8.2. Without limiting the generality of section 8.1 above, the Third Party agrees that in addition to any other rights or remedies Humber College may have for material breach of the Standard, Humber College has the right to seek an injunction or other equitable relief in the Courts of Ontario enjoining a threatened or actual breach of this Standard by the Third Party.

9. Survival

9.1. Notwithstanding the termination of the Service Agreement or engagement, to the extent that the Third Party continues to have access to Personal Information for any reason, the Third Party shall continue to govern itself in accordance with the terms of this Standard.

10. Minimum Security Requirements

10.1. The Third Party shall share SDLC methodology for Humber's review to ensure adherence to appropriate security controls and standards.

10.2. The Third Party shall ensure that Humber College security requirements are captured into the design of the application or Service. Requirements gathering activities must include information security requirements related to functional, technical and user requirements.

10.3. Security must be designed into all architecture layers (business, information, applications and technology), balancing the need for information security with the need for accessibility.

10.4. The Third Party shall ensure that access to program source code and associated items (such as designs, specifications, verification plans, and validation plans) must be restricted to authorized individuals, based on the principle of least privilege, as determined by job function or role.

10.5. Introduction of new application changes and upgrades must follow the Humber web CAB approval process.

10.6. The Third Party will complete an application testing process as part of the Services. The application testing process must consist of the following minimal test phases following the initial product risk assessment and approval to initiate the project.

10.6.1. Source code analysis to perform the security review (includes manual and automated source reviews);
10.6.2. Component testing (i.e. unit testing and run-time verification to test functionality);
10.6.3. Integration testing (includes regression testing after changes have been made to previously tested code);
10.6.4. Acceptance testing (includes acceptance testing of business and security functionality);
10.6.5. Penetration testing (includes penetration testing at the end of major code developments and prior to moving into production);
10.6.6. Load testing for major releases; and
10.6.7. Final security review (includes sign-off by Humber College information security team that identified vulnerabilities have been addressed).

10.7. The Third Party shall provide evidence of the following:
10.7.1. The design and security technologies used to establish minimum acceptable levels of security and privacy quality;
10.7.2. That sufficient testing has been applied to guard against the absence of both intentional and unintentional malicious content upon delivery; and
10.7.3. That sufficient testing has been applied to guard against the presence of known vulnerabilities.

10.8. The Third Party shall provide details of their third party subcontracting arrangements and ensure compliance with security requirements.

10.9. The Third party shall ensure that no Personal Information is stored in non-production environments.

10.10. If Personal Information is required in a non-production environment, the data must be anonymized or sanitized prior to being utilized.

10.11. Personal Information should only be kept as long as it is required to support the business requirement for which it was collected. If the data needs to be retained for more than a year, it needs to be anonymized.

10.12. Permission must be granted and documented from the Web Oversight Committee or its designate prior to data and/or any Personal Information in the custody of Humber being transferred or stored outside of Humber owned assets.

10.13. All development activities must be completed on non-production systems and the promotion to production including to staging environments must go through the web CAB approval process.

10.14. All access to Humber web systems for the purpose of development, administration and support must utilize Humber approved remote access systems.

10.15. All Third Parties accessing Humber resources must utilize uniquely identifying credentials and may not be shared between employees and agents of Third Party.

10.16. Passwords stored must be different in non-production, production and staging environments.

10.17. All data points to be collected from students shall be documented (including justification, storage locations, data types, and retention policy) and approved by the Web Oversight Committee or its designate prior to promotion into production.

10.18. Responsibilities for the maintenance of systems, remediation of identified vulnerabilities must be clearly identified in writing.

10.19. Vulnerabilities identified by Humber College, shall be remediated using an agreed upon approach and timeframe based upon associated risks.

ACKNOWLEDGEMENT AND ACCEPTANCE OF STANDARDS

By my signature hereunder and on behalf of my company, _____ ("Company"), I confirm that we have read and agree to all terms and conditions in the Standards and that I have the authority to bind the Company.

Any Services provided hereunder shall be in compliance with these Standards and Humber College policies and procedures, which can be found at https://humber.ca/legal-and-risk-management/policies.html

COMPANY NAME AND ADDRESS:

Name and address:

Telephone Number: **Fax Number:**

Contact's Email Address:

Company's Email Address:

Submitted by: **Title:**

(please print name)

Signature: **Date:**

I have the authority to bind the Company.