TECHNICAL AND ORGANIZATIONAL MEASURES

1. DEFINITIONS

"Company" means the person that has submitted an application for a business license under Toronto Municipal Code, Chapter 546 or Chapter 547.

"Data Breach" means any unauthorized access, acquisition, or disclosure, destruction, alteration, accidental loss, misuse, or damage of Personal Information.

"Personal Information" means any information which meets the definition of Personal Information contained in MFIPPA, regardless of whether MFIPPA applies to this information; or any information which is required to be protected pursuant to MFIPPA, PHIPA, PIPEDA, or any other Canadian laws (including regulations and common law) pertaining to the protection of personal information

2. APPLICATION

2.1 Application. The Company shall ensure that the Company, and all agents, subcontractors, and third parties involved in the delivery of the services that are to be provided under this proposed license meet or exceed the measures described in this document.

2.2 Compliance. Compliance with the requirements of this document is a condition on which the license is issued. Company is required to maintain compliance with the requirements of this document throughout the licensing period, and shall be required to re-attest to compliance with these requirements as a condition of renewal of license.

3. POLICIES

3.1 Company's Policies. Company shall maintain a set of policies (the "Policies"). At a minimum, these Policies shall include:

- privacy
- cybersecurity
- information technology
- cloud
- access control
- business continuity
- acceptable use
- remote access
- vulnerability management
- network architecture

- user access control management
- Wi-Fi security
- physical security

Company will comply with the Policies as amended from time to time. Company will not amend the Policies in a manner that decreases the protection that they afford to Personal Information collected by the Company, or in the Company's custody or control.

3.2 Training. Company will train its personnel with respect to the Policies on an annual basis, or as additionally required based on industry best practice. Company shall ensure that personnel received cybersecurity training on an annual basis.

4. ADDITIONAL REQUIREMENTS FOR PERSONAL INFORMATION

4.1 Compliance with Privacy Laws. Company will: (i) Handle all Personal Information in accordance with applicable Canadian privacy laws; and (ii) meet the requirements of this document in a manner that complies with Canadian privacy laws.

5. BREACH MEASURES

5.1 Monitoring. Company shall maintain policies, procedures, and governance/technological measures to allow for the prompt detection of Data Breaches, including but not limited to access reviews, audit logging, intrusion prevention/detection, and other measures as required by industry best practice.

5.2 Notice of Data Breach. In the event of a Data Breach, Company shall comply with the notification requirements of PIPEDA, and any other applicable Canadian legislation to which it is subject. This notification may include promptly reporting the Data Breach to the appropriate regulatory body, i.e. the Information and Privacy Commissioner of Ontario and/or the Office of the Privacy Commissioner of Canada. Company shall also take all necessary measures to provide notification to victims of the Data Breach in accordance with the requirements of applicable Canadian law.

5.3 Resolving the Breach. In the event of a Breach, Company will use all commercially reasonable measures to promptly:

(i) investigate, contain, mitigate, and remedy the Data Breach; and

(ii) prevent any recurrence of the Data Breach.

5.4 Records Relating to a Breach. Company shall maintain and preserve all business records related to any Data Breach until all claims relating to the Breach that arise in the 7 year period following the Data Breach are resolved, and in accordance with applicable Canadian Law

6. DATA SECURITY

6.1 Safeguards. Company is responsible for implementing physical, administrative and technical safeguards in alignment with cybersecurity industry best practices. Taking into account the sensitivity of the data, the safeguards will meet or exceed industry standards as they evolve over time, including but not limited to the requirements in this document.

6.2 Encryption. Company will encrypt all Personal Information, both in flight and at rest, using a strong cryptographic protocol that is consistent with cybersecurity industry standards as updated from time to time, such as FIPS 140-2, FIPS 140-3, ISO27001 or NIST SP 800-175B. Under no circumstances shall data be encrypted using a standard weaker than 256-bit. All encryption keys must be unique to the Personal Information. Company will secure and protect all encryption keys using secure methods per cybersecurity industry standards.

6.3 Malware. Company shall maintain processes in line with industry best practice to detect, prevent, and recover from malware, viruses, and spyware. Company shall ensure that anti-virus, anti-malware, and anti-spyware software is regularly updated in accordance with industry best practice.

6.4 Data Residency. Personal Information shall not be stored outside Canada.

6.5 Data Centres. Company's data centres used to provide the Services will meet the following or more stringent requirements of:

(a) a Tier III certification by the Uptime Institute (or its industry equivalent); and

(b) SSAE No. 18 SOC 2 Type II

6.6 Multi-Factor Authentication. Company shall offer users the opportunity to implement Multi-Factor Authentication in accordance with current cybersecurity industry best practices.

7. COMPLIANCE

7.1 Compliance. The Company shall be certified under the following cybersecurity standards:

(a) ISO 27001/27018, ISA/IEC 62443 or SSAE 18/ISAE 3402 SOC 2 Type II; and

(b) Current version of Payment Card Industry – Data Security Standard (PCI-DSS)

7.2 Audit. At least once every 12 months, Company shall engage an accredited auditor to conduct an audit of: (i) the security the Services; (ii) Company's compliance with ISO 27001/27018; (iii) Company's compliance with SSAE 18/ISAE 3402 SOC-1, SOC 2 and SOC 3; and (iv) Company's compliance with any other security standard with which Company claims compliance in any of its published materials.

7.3 **Assessments.** To the extent not otherwise required under the Company's compliance certifications in this section, Company shall conduct annual security assessments on their infrastructure including but not limited to conducting a Privacy Impact Assessment (PIA) and Threat Risk Assessment (TRA).

7.4 **Penetration Testing.** Once per year, or following a significant change, Company shall secure a penetration test performed by a recognized third-party firm, performed pursuant to recognized industry best practices. Company shall promptly remediate any medium-risk or higher findings in accordance with industry best practice.

7.5 **Vulnerability Scanning.** On a quarterly basis, or following a significant change, Company shall conduct both internal and external network scans using recognized industry tools. Company shall promptly remediate any medium-risk or higher findings in accordance with industry best practice.