MBLL IT SECURITY SAFEGUARDS AND MEASURES REQUIREMENTS

This document contains the minimum information technology security safeguards and measures requirements and obligations of the Vendors and of the Vendor's Representatives to safeguard MBLL.

By specifying the minimum requirements set out herein, MBLL is in no way representing that such minimums are adequate to cover all possible security needs of the Vendor and MBLL expressly disclaims such a representation. The specific manner in which a Vendor implements the below minimum requirements may vary depending on the nature of the services, solution architecture, delivery model, and risk profile, provided that the intent and outcomes of these requirements are met and that any material deviations are approved by MBLL in writing.

The Vendor acknowledges and agrees that:

1. it is the Vendor's sole responsibility to determine the appropriate amount and types of safeguards and measures and whether any other safeguards and measures are necessary or advisable;
2. the Vendor's safeguards and measures meet or exceed the minimum requirements set out herein;
3. through the term of its agreement with MBLL the Vendor will ensure that the security safeguards and measures the Vendor has in place will continue to meet or exceed those set out herein and prevailing industry standards; and
4. the Vendor shall ensure all Vendor's Representatives are also compliant with these requirements and the Vendor agrees it shall be wholly responsible for any failures of its Representatives.

For the purposes of this document:
"Confidential Information" includes personal information (as defined in The Freedom of Information and Protection of Privacy Act (Manitoba) or the Personal Information Protection and Electronic Documents Act), personal health information (as defined in The Personal Health Information Act (Manitoba)), third party proprietary information, MBLL proprietary information, other data relating to MBLL or its customers, potential customers, and/or end users, and any other information that MBLL identifies as confidential.

"Relevant Systems" means any system, application, network or device of the Vendor or Representatives which is used to access, store, process or transmit MBLL data, including but not limited to, Confidential Information.

"Representatives" includes the Vendor's officers, employees, agents, business partners and subcontractors that have access to the Relevant Systems.

"Information Security Incident" means any confirmed or reasonably suspected event that results in unauthorized access to, disclosure of, acquisition of, or loss of Confidential Information, or that otherwise compromises the confidentiality, integrity, or availability of Relevant Systems or Vendor Services.

1. Management of Information Security

1.1. The Vendor will have and maintain a formal information security program that includes defined policies, accountabilities, documented procedures, and all appropriate and

necessary legal, organizational, and technical measures, including periodic reviews and executive oversight, to ensure that Confidential Information is protected against harms, including but not limited to unauthorized destruction, alteration, access, disclosure, or propagation and execution of harmful code. The Vendor agrees that its information security program will always meet or exceed prevailing industry standards. The Vendor will not make any changes to its information security program or any part thereof that would materially reduce the protections provided by such program.

1.2. The Vendor will, on an annual basis, at its own expense, have an independent security assessment conducted by a reputable third party against internationally recognized frameworks (e.g., SOC2 Type II, ISO2700x), and will provide to MBLL summaries of all such audit reports promptly upon request. The Vendor will remediate any deficiencies noted in any such report in a timely manner.

Certifications, attestations, or audit reports (e.g., ISO 27001, SOC 2) may be used to demonstrate compliance with applicable requirements of this document; however, such certifications do not automatically replace or supersede MBLL's requirements unless explicitly agreed in writing.

1.3. Where the Vendor can demonstrate that alternative controls, processes, or certifications provide security outcomes that are equivalent to or exceed the requirements set out in this document, MBLL may, acting reasonably, accept such equivalency in writing. In such case the following shall apply:

(a) MBLL may, using either internal or external auditors, carry out inspections or investigations of the Vendor's and its Representative's security practices involving MBLL Confidential Information, as considered necessary to ensure the adequate protection of the information.

(b) The Vendor and its Representatives must cooperate in any inspection or investigation carried out by MBLL. In addition, the Vendor and its Representatives must permit access, at all reasonable times, to their premises, records and information in order to carry out such inspections and investigations and to ensure compliance with this document.

(c) If an inspection or investigation identifies deficiencies in the Vendor's or its Representative's security practices which expose MBLL Confidential Information to risk of unauthorized disclosure, the Vendor must take reasonable steps, acceptable to MBLL, to promptly correct the deficiencies.

1.4. The Vendor's Representatives must encrypt all Confidential Information when:

(a) the Confidential Information is in transit; and

(b) the Confidential Information is at rest or stored.

All Confidential Information required to be encrypted shall be encrypted using currently acceptable strong encryption in accordance with industry standards for secure key and protocol negotiation and key management.

The Vendor will have and maintain policies and procedures covering cryptography, encryption, and key management. The Vendor will review and update the policies and procedures at least annually.

1.5. The Vendor will have and maintain a process for classification of data (including Confidential Information) which classifies data based on sensitivity, and which ensures

that security controls that are commensurate with the sensitivity of the data (including the Confidential Information) are applied.

The Vendor will have and will maintain an appropriate data loss prevention program to be able to detect and prevent Confidential Information from leaving the Vendor's network in an unauthorized manner.

2. Physical Security

2.1. The Vendor will meet industry practices for physical and environmental security controls of facilities in which Relevant Systems are located.

3. Confidential Information Return and Destruction

3.1. Upon expiration or termination of the Contract for any reason, or at any earlier time at the request of MBLL, the Vendor will:

(a) return all Confidential Information to MBLL in a mutually agreeable format and time frame;

(b) if requested by MBLL in writing, promptly destroy, delete, and render unrecoverable all tangible and electronic instances of Confidential Information from the Vendor's and where applicable, its Representatives' systems in accordance with prevailing industry standards for data and media sanitization; and

(c) if requested by MBLL, promptly provide written confirmation of its compliance with the requirements of this section and a copy of data destruction certificate(s), where applicable.

3.2. Upon expiration or termination of the Contract for any reason, the Vendor will provide MBLL with any encryption or decryption procedures and keys used to encrypt Confidential Information, without any copy being retained by the Vendor.

3.3. All records of Confidential Information, including physical or electronic media, must be destroyed in a manner that makes it impossible to read or reconstruct the information.

4. Business Continuity, Disaster Recovery and Backup

4.1. The Vendor will maintain a business continuity plan in accordance with prevailing industry standards to ensure the continuity of business operations aimed at limiting any impact on delivery of the services under the Contract.

4.2. The Vendor must have and maintain disaster planning and recovery plans in place, acceptable to MBLL, acting reasonably, that enable it to recover, restore availability, and access to Confidential Information and the services under the Contract. The Vendor will test its disaster recovery plans no less than once every year and will ensure that the scope of all such tests includes the Relevant Systems. The Vendor will promptly remediate any deficiencies noted in any such tests. Upon request, the Vendor will provide to MBLL summaries of its disaster recovery plans, test results, and any applicable remediation undertaken by the Vendor.

4.3. The Vendor shall define, document, and maintain Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) for all Relevant Systems that support the services under the Contract. RTOs and RPOs shall:

(a) be commensurate with the criticality, sensitivity, and business impact of the applicable services and Confidential Information;

(b) be established based on a documented business impact analysis or equivalent assessment; and
(c) reflect the technical and architectural characteristics of the solution provided.

4.4. The Parties acknowledge that RTOs and RPOs may vary depending on the solution, service model, or system architecture. Accordingly, the applicable RTOs and RPOs for the services shall be:
(a) documented in a statement of work, service level agreement, appendix, or similar contractual document; and
(b) agreed to in writing by MBLL prior to service commencement or material change.

4.5. The Vendor shall test its business continuity and disaster recovery capabilities, including the ability to meet the agreed RTOs and RPOs, no less than annually or following a material change to the Relevant Systems. Upon request, the Vendor shall provide MBLL with:
(a) a summary of the applicable RTOs and RPOs;
(b) results of disaster recovery tests, including whether recovery objectives were met; and
(c) details of any remediation plans where recovery objectives were not achieved.

4.6. The Vendor shall review and update its recovery objectives, plans, and capabilities as necessary to reflect changes in services, technology, threat landscape, or business requirements, and shall not materially degrade agreed recovery objectives without MBLL's prior written approval.

5. Representative Awareness and Training

5.1. The Vendor must make its Representatives aware of its written security policies and procedures and the Vendor's obligations under this document and ensure its Representatives comply with same.

5.2. The Vendor will ensure that its Representatives have undergone security awareness training before being granted access to Confidential Information, and that its Representatives are informed of disciplinary measures that will be imposed by the Vendor for violations of the Vendor's information security policies. An annual refresh of the security training for its Representatives who have access to Relevant Systems or Confidential Information will be implemented and tracked.

6. Payment Card Industry (PCI) Compliance

6.1. If the Vendor is processing, transmitting, or storing Cardholder Data on behalf of MBLL, the Vendor will annually certify and maintain PCI compliance, at its own expense, and will promptly provide MBLL, upon request, with an attestation of PCI compliance.

7. Confidential Information Use, Access and Rights

7.1. The Vendor will use Confidential Information only to the extent required and for the sole purpose of performing the services under the Contract. The Vendor will not, and will not permit any Representative to, copy, or otherwise reproduce the Confidential Information, or disclose, disseminate, distribute, make available or share any Confidential Information, in whole or in part, with third parties, other than approved third party Representatives engaged in connection with the Contract. Confidential Information will only be disclosed to those Representatives that have a need to know such information in connection with the Contract.

7.2. The Vendor acknowledges that it does not, and will not, have any right, title, or interest in any Confidential Information, received, learned, or otherwise obtained by it, as a result of performance of the services under the Contract.

7.3. The Vendor will provide MBLL with access to all or any of the Confidential Information in the Vendor's custody or control within 48 hours following any request by MBLL for such access. The Vendor cannot deny MBLL's access request for any reason, including but not limited to any breach or late or disputed payment under the Contract.

8. Data Residency

8.1. All data (including Confidential Information) will be stored, processed, transferred, and accessed only in Canada, USA, the United Kingdom, or European Union unless authorized in writing by MBLL. Data (including Confidential Information) may be accessed by the Vendor or its Representatives to the minimum extent required to perform the Services and only to perform the Services. Any changes made by the Vendor in relation to access, storage, processing, or transfer of Confidential Information from locations authorized in writing by MBLL is subject to MBLL's prior written approval and must be documented in a statement of work, appendix, or similar contractual document.

9. Access Control and Authentication

9.1. The Vendor will ensure that all Relevant Systems comply with the following minimum access control requirements:

(a) all access is formally approved and based on the principle of least privilege;
(b) individual accountability is maintained at all times, including when super user and generic accounts are used;
(c) Representatives' access is promptly revoked on resignation, termination, or when such access is no longer needed;
(d) access is promptly suspended when required to contain further damage during an information security incident;
(e) periodic reviews are performed to validate that access privileges have been appropriately provisioned or revoked;
(f) super-user accounts, including any utility programmes with elevated privileges, are continuously monitored and managed;
(g) passwords are implemented with length, complexity and enforcement of periodic changes while limiting password re-use or using the latest NIST 800-63 guidance;
(h) enables user accounts to lock-out after a defined number of failed attempts or progressively increase the time between logins after each failed login attempt; and
(i) multi-factor authentication for remote access and for privileged access to systems.

9.2. If MBLL requires access to Vendor hosted or managed systems, the Vendor will support integration using MBLL approved authentication mechanisms.

10. Technology Asset Management

10.1. The Vendor will have and maintain an asset management process that maintains a complete and accurate inventory of technology assets and manages technology assets throughout their lifecycle.

10.2. The Vendor will have and maintain a policy for mobile computing and telecommuting that contains appropriate security measures to ensure protection of Relevant Systems and Confidential Information.

11. Change Management

11.1. The Vendor will have and maintain a change management process incorporating involvement and integration with relevant information security stakeholders and teams to mitigate information security risks changes may pose.

12. Threat and Vulnerability Management

12.1. The Vendor will apply all vendor-recommended security updates to all Relevant Systems in a timely manner, not to exceed 30 days from date of release for vulnerabilities identified by the applicable vendor as “critical”, and 90 days for non-critical vulnerabilities.

12.2. The Vendor will have and maintain policies and procedures to ensure that all of the following requirements are met:

(a) up-to-date malware protection software are installed on all computer systems ;
(b) firewalls are installed to segregate the Vendor’s internal networks from the internet and host based firewalls installed on laptops or desktop computers;
(c) appropriate intrusion prevention and detection technologies are applied;
(d) regular network vulnerability assessments are conducted, as per information security industry practices and applicable regulatory requirements;
(e) penetration tests aligned with information security industry practices on externally facing systems and infrastructure are conducted at least annually or when there is a system change that may impact security posture of the system or infrastructure; and
(f) controls to assess risk of, manage, and audit the introduction of software into the environment are implemented.

13. Secure Development Life Cycle (SDLC)

13.1. To the extent that the Vendor develops applications or application code on behalf of MBLL, or on Relevant Systems, the Vendor will:

(a) ensure that, at a minimum, the application code is secure against the vulnerabilities described in Open Web Application Security Project (OWASP) Top Ten List;
(b) follow a formal SDLC program that includes secure practices in code development and use automated security testing tools to scan the code and applications and remediate vulnerabilities before going into production; and
(c) adequately protect source code and discourage modification to software packages unless absolutely required.

13.2. The Vendor will segregate its development and testing environments from the operational or production environment used to access, store, process and/or transmit Confidential Information or provide the contracted service. Segregation controls will include, at a minimum, the following:

(a) users will have separate profiles for testing and operational environments; and
(b) Confidential Information will not be used in development or testing environments unless the testing environment has production level security controls.

14. Cloud and Virtualization Security

14.1. The Vendor will extend all security requirements and measures to cloud computing environments that contain Confidential Information to protect against unauthorized access, modification, use or disclosure of said data. In addition, the Vendor will:

(a) establish, implement, and maintain policies and procedures for the application of Shared Security Responsibility Model (SSRM); and

(b) apply the SSRM throughout the service offering, including tenants and suppliers.

14.2. In cases where the Vendor provides MBLL with services in a multi-tenant environment, the Vendor will have the necessary segmentation controls in place and be able to demonstrate the appropriate level of isolation and segregation of user accounts, data, databases, applications, infrastructure, and networks from other organizations in the same environment.

15. Logging and Monitoring

15.1. The Vendor will install and configure the necessary tools to log, monitor and alert on information security events on 24/7 basis.

15.2. The Vendor will maintain log files containing security events for a period of no less than 1 year, with a minimum of 3 months immediately available. The Vendor will restrict access to log files to support accountability, serve as evidence for incident management, and support legal and compliance requirements. This is inclusive of all administrator and operator activities which in addition require regular reviews.

15.3. The Vendor will implement necessary controls to protect logs against unauthorized or accidental access, tampering or loss.

16. Third Party Security Management

16.1. The Vendor shall ensure that the security controls implemented by any third party Representatives are in compliance with the requirements of the Vendor under this document.

16.2. The Vendor will have, maintain, and enforce a Third-Party Security Management Program, which at a minimum includes the following controls with respect to any third party Representatives:

(a) the Vendor's due diligence review of any third party Representatives;

(b) written agreements with its third party Representatives that contain information security requirements for access, processing, storing, or transmission of data, and for providing IT infrastructure components that are, to the extent applicable to the Representative aligned to this agreement and appropriate in the circumstances given the sensitivity of the applicable information;

(c) written confidentiality or non-disclosure agreements with third party Representatives; and

(d) appropriate levels of regular monitoring, reviewing, and auditing of any third party Representatives' service delivery and compliance by such Representatives with the applicable agreement between the Vendor and the third party Representative.

17. Incident Management

17.1. The Vendor shall establish, implement, and maintain a formal information security incident management capability with suitably defined policies, accountabilities, roles, responsibilities, procedures, escalation paths, and reporting requirements to effectively

identify, respond to, manage, and remediate Information Security Incidents affecting Confidential Information or Relevant Systems.

17.2. The Vendor shall maintain a defined and documented approach for:
(a) assessing, classifying, and prioritizing Information Security Incidents;
(b) identifying, collecting, acquiring, and preserving information and evidence that may be required for investigation, regulatory compliance, or legal proceedings; and
(c) supporting MBLL's investigation, response, and remediation activities.
Such approach shall be consistent with applicable regulatory requirements, recognized industry standards, and security investigation industry practices.

17.3. The Vendor shall notify MBLL of any Information Security Incident in accordance with the notification timelines set out in this document. Notifications and ongoing status updates shall include sufficient detail to enable MBLL to understand the nature, scope, impact, and remediation status of the Information Security Incident and to meet its own legal, regulatory, and contractual obligations.

17.4. Where MBLL has established a Vendor Incident Management Process, Incident Communication Protocol, or similar document applicable to the services provided under the Contract (each an "Incident Management Process"), the Vendor agrees to comply with such Incident Management Process as notified by MBLL in writing. Any Incident Management Process referenced by MBLL shall be deemed incorporated by reference into this document, without the need for further amendment.

17.5. In the event of any conflict or inconsistency between this document and any applicable Incident Management Process:
(a) the provision that provides the higher or more protective standard of security shall apply; and
(b) nothing in an Incident Management Process shall be interpreted to reduce or limit the Vendor's obligations under this document.

17.6. Except where disclosure is expressly required by Applicable Law, the Vendor shall not communicate with regulators, law enforcement authorities, affected individuals, media, or other external parties regarding an Information Security Incident involving MBLL Confidential Information without MBLL's prior written approval. Where Applicable Law requires direct disclosure by the Vendor, the Vendor shall provide MBLL with prior written notice of such disclosure unless prohibited by law.

18. Compliance by the Vendor and Representatives

18.1. The Vendor will implement, maintain, and comply with the information security controls, obligations and other requirements set out in this document or elsewhere in the Contract, and will cause each Representative to do so, as applicable.

19. Order of Precedence

19.1. If there is a conflict between this document the Contract, the terms and conditions of this document shall govern and control. Notwithstanding the foregoing, the Contract may supersede this document solely for the services covered under the Contract provided that the Contract states that the parties intend for the Contract terms to supersede this document, and the specific sections of this document to be superseded are referenced in the Contract.