INFORMATION SECURITY AND PRIVACY REQUIREMENTS (THE "REQUIREMENTS")

Note: In these Requirements, the terms "Company" or "McCain" and "Supplier" are used. These terms should be read to mean, as applicable, the parties to the agreement or RFP or other document of which these Requirements form part, howsoever defined therein.

Data Ownership – **"McCain Data"** means any non-public information which is commercially valuable, proprietary, privileged, or personal, the unauthorized disclosure of which could adversely affect Company and/or its employees (e.g., competitively, by waiver of legal privilege, monetary loss, or violation of law or right of privacy). McCain Data includes personally identifiable information of employees, contractors, customers, or potential customers of Company, any classified information Company receives in connection with participation in government programs, and any data the unauthorized disclosure of which could cause significant harm to Company or the individual to whom the information pertains.

Supplier acknowledges that all McCain Data shall at all times remain the sole property of Company and nothing in these Requirements will be interpreted or construed as granting Supplier any license or other right under any patent, copyright, trademark, secret, or other proprietary right to McCain Data.

Compliance with Applicable Privacy Laws – Supplier may have access to specific information that can identify individuals who are Company's consumers, customers, suppliers, business partners, contractors, or employees (known as **"Personally Identifiable Information"**). Supplier shall comply with (i) all applicable federal, provincial, state, and territorial privacy and security laws and regulations (collectively, **"Privacy Laws"**) to which it is subject and shall not by act or omission place Company in violation of any Privacy Laws (e.g. GDPR). Supplier shall stay informed of possible changes to Privacy Laws throughout the course of the agreement. Where local laws appear to prevent compliance with these Requirements, Supplier is responsible for notifying Company to determine appropriate compensating controls.

Data Collection & Use – Supplier warrants that (i) any Personally Identifiable Information it will disclose to Company under its agreement with Company will be collected in accordance with Privacy Laws; (ii) any individual who provides Personally Identifiable Information to Supplier has been informed of Company's identity, how to contact Company, and all other matters required by Privacy Laws; (iii) Company is authorized either by consent of individuals or by law to obtain Personally Identifiable Information from Supplier (if Supplier collects such information in the course of performing its obligations under its agreement with Company) and use and disclose it for the purposes of its agreement with Company; (iv) Supplier shall notify Company of any complaint or request it receives concerning the Personally Identifiable Information under its agreement with Company and comply with any reasonable direction of Company, including providing access by Company to its premises, personnel, materials, and systems; and (v) Supplier shall not collect, access, use, transfer, store, disclose, delete, retain, or make accessible Personally Identifiable Information in any jurisdiction which is not expressly contemplated by its agreement with Company without Company's prior written consent.

Data Processing – Supplier shall execute any necessary agreements and acquire all necessary permits and authorizations pertaining to Processing and handling of McCain Data from relevant regulatory authorities. **"Processing"** or **"Process"** means any operation or set of operations that is performed upon McCain Data, whether or not by automatic means, including without limitation collection, recording, organization, storage, access, adaptation, alteration, retrieval, consultation, use, disclosure, dissemination, alignment, combination, blocking, deletion, erasure, or destruction.

Derivative Data – Supplier shall not create or maintain data which are derivative of data belonging to Company, except for the purpose of performing its obligations under its agreements with Company and as authorized by Company. Any derivative of McCain Data, regardless of how created, shall be deemed McCain Data.

Record Retention and Return of McCain Data – Supplier shall retain McCain Data only for as long as reasonably and legally required to perform any obligations under its agreement with Company. Upon the earlier of (i) expiry or earlier termination of the agreement between the parties; or (ii) Supplier having no further legitimate business need to retain the McCain Data, Supplier shall seek further direction regarding the McCain Data from Company, which direction must be provided by Company within a reasonable period of time. If Company elects disposal or destruction, Supplier shall proceed to permanently dispose of or destroy the McCain Data, including all originals and copies of such McCain Data in any medium and any materials derived from or incorporating such McCain Data, in a manner that prevents content recovery and shall, upon Company's request, provide a certificate to Company attesting to its proper deletion or destruction of the McCain Data. If applicable law prevents or precludes the return or destruction of any McCain Data, Supplier shall notify Company of such reason for not returning or destroying such McCain Data and shall not Process such McCain Data thereafter without Company's prior written consent. If Company elects return of the McCain Data, Supplier shall promptly return all McCain Data subject to these Requirements in the format requested by Company. Company may instruct Supplier in writing to retain certain McCain Data because of pending or anticipated litigation, investigation, audit, or other purposes and Supplier shall follow such instructions. If Company does not provide any direction, Supplier must provide a further 60 days' advance written notice to Company and may then proceed to permanently dispose of or destroy the McCain Data in a manner that prevents content recovery. Supplier's obligations under these Requirements to protect the security of McCain Data shall survive termination of its business relationship with Company.

Protective Controls – Supplier shall use appropriate and reasonable technical, administrative, and organizational security measures in accordance with industry practices and the sensitivity of the information to secure McCain Data and systems to which Supplier has access and prevent unauthorized access, alteration, or destruction thereof.

Upon Company's request, Supplier will provide evidence that it has established and maintains reasonable technical, administrative, and organizational security measures in connection with McCain Data and systems, including, but not limited to the following:

<u>Information Security Policy</u>

- Supplier shall maintain one or more information security policies that meet industry recognized security best practices and apply across its organization; and
- Supplier will review the policy or policies periodically, or if significant changes occur, to ensure continuing suitability, adequacy, and effectiveness.

Security Compliance and Controls Assessment

- Supplier will maintain a practice to regularly test, assess, and evaluate the effectiveness of technical and organizational measures for ensuring the security of Company systems and McCain Data
- Supplier will ensure compliance with such industry standards and best practices including but not limited to CSA-CCM, CIS, CIS benchmarks, NIST CSF, and ISO 27001.
- Supplier shall obtain and provide to Company at least annually an audit report indicating control maturity on its data security practices, such as an SSAE 18 or an ISO 27001 report or as otherwise agreed with Company, from a recognized independent provider of such reports
- Supplier shall provide all answers required to enable Company to perform the required security assessment on Supplier and make recommendations as appropriate; and
- Supplier further acknowledges and agrees that it shall not access any McCain Data or internal network, until such time as it has satisfied Company that it meets an acceptable information security maturity level, and shall remain in compliance or exceed such security maturity level thereafter.

Information Security Risk Management

- Supplier must have an established process that periodically assesses and manages risk within the organization with respect to providing services to Company and the possession and Processing of McCain Data.

Network, Operating System and Application Controls

- Supplier must ensure that Supplier networks, operating systems, and/or applications that Process or store McCain Data, employ industry best-practice safeguards and controls to ensure the confidentially and integrity of McCain Data, including the Protective Controls herein.

System Security

- Supplier will maintain an inventory of information assets (i.e. physical, software, information, services, and people) utilized to provide services to Company
- Supplier will establish and maintain configuration standards to address currently known security vulnerabilities and industry best practices for all network devices and hosts
- Supplier will ensure that software, operating systems, firmware and networks used in operational systems maintains up-to-date patching
- Supplier will remove or disable non-essential functionality (i.e. hardening each system), such as scripts, drivers, features, subsystems, or file systems (e.g. unnecessary web servers, default, or sample files, etc.)
- Supplier will deploy malware protection on all IT systems that access McCain Data. Supplier must ensure malware protection technology has the latest and up-to-date manufacturer's signatures, definition files, software, and patches
- Supplier will conduct regular scanning to identify systems security vulnerabilities (control weaknesses); critical and high vulnerabilities will be appropriately documented and remediated
- Supplier will perform systems penetration tests or similar techniques tests on a regular basis
- Supplier will have a documented change management procedure for applications and networks that support Company processes or for housing McCain Data; segregation of duties shall be in place

- Supplier will have a documented change management procedure for applications and networks that support Company processes or for housing McCain Data; segregation of duties shall be in place
- Supplier will ensure secure backup copies of McCain Data and software are maintained and tested regularly for the purpose of data recovery
- Supplier will utilize media handling standards which require that removable computer media be physically and logically protected against unauthorized access, that confidential and sensitive information on such media be available to authorized users only and that removable computer media be disposed of in a secure manner
- Supplier will maintain adequate business continuity and disaster recovery controls and test such controls to ensure effectiveness
- Supplier will implement reasonable measures to detect and prevent data loss/leakage
- Supplier will ensure a separation between production and non-production (development and test) environments; and
- Supplier will ensure that intra-tenant access is appropriately segmented and segregated, monitored and restricted from other tenants.

Security Awareness

- Prior to and regularly after providing access to information, network, data and/or physical assets, Supplier shall train personnel concerning the implementation of, compliance with, and enforcement of Supplier's information and physical security controls and information and physical security policies, which shall at a minimum meet security best practices.

Network Controls

- Supplier shall implement, maintain, comply with, and enforce network information security policies and information security controls with respect to Supplier systems that meet or exceed security best practices and that include:
    - Demilitarized zones
    - Intrusion detection and prevention
    - Network and system segmentation for critical systems
    - Enforced path controls that prevent users from accessing portions of the network
    - Authentication controls for external network connections and automatic network connections
    - Controls to prevent unauthorized access and use of remote network diagnostic ports
    - Network access controls that restrict unauthorized access with respect to electronic mail; and
    - Routing controls across interconnected networks.

Access Controls

- Supplier will maintain accurate and complete logs of personnel accessing McCain Data

- Supplier will ensure that personnel accessing Company systems or McCain Data are permitted only on a need to know basis and under the proper authority
- Supplier shall implement safeguards and controls to prevent any unauthorized access
- Supplier will prohibit its users from sharing passwords; and
- Supplier will ensure that systems accessed on behalf of Company employ strong password complexity rules, including the following configurations:
    - Passwords set to expire every 90 days or less
    - Passwords set to a minimum length of eight characters and be a non-trivial combination of letters, numbers, and special characters
    - Passwords enabled to system lockout after failed login attempts
    - Systems enabled O/S screen saver locks after a period of inactivity; and
    - Encrypt authentication credentials during storage and transmission.

Access to Internal Department Network and Systems

- As a condition of gaining remote access to any internal Company network and systems, Supplier shall comply with Company policies and procedures; Company's remote access request procedures shall require Supplier to submit a remote access request form for Company's review and approval
- Supplier will ensure that unless it is absolutely necessary, its personnel will use non-privileged accounts or roles when accessing non-privilege functions relating to Company's data
- Remote access technologies provided by Supplier shall be approved by Company
- Individuals who are provided with access to the Company network may be required to attend or review Company's security awareness training on an annual basis
- Supplier shall secure its own connected systems in a manner consistent with Company requirements
- Company reserves the right to audit the security measures in effect on Supplier's connected systems without prior warning; and
- Company also reserves the right to immediately terminate network and system connections not meeting such requirements.

Physical and Environmental Security

- Supplier's operation centers, server rooms, wiring closets, and other critical infrastructure areas shall have restricted access with logged authentication processes.

Cryptography

- Supplier shall encrypt all transmissions and storage of McCain Data, including but not limited to information deemed confidential, highly confidential, or sensitive by Company, such as Personally Identifiable Information, authentication credentials, and cryptographic keys; and
- Supplier will employ best practice encryption standards and technologies for each system resource or service. These technologies could include disk encryptions on end user computing devices using device level encryption, File and Folder encryptions, network encryptions using IPsec, AES256-SHA 256, data transmission over SSHv2, TLS 1.2 and Backup tape encryptions using RSA Cipher standards, in addition to implementing native encryption standards within each application system.

Supplier shall comply with any specific data processing and handling requirements reasonably requested by Company or recommended by legal advisors for compliance with applicable laws and regulations. Supplier shall provide Company with reasonable advance notice in writing of any planned changes to the hosting location of McCain Data, use of third party providers, or other security policies, standards, and practices related to McCain Data.

Company and Supplier shall collaborate on security monitoring and incident response, define points of contact on both sides, establish monitoring and response procedures and timelines, set escalation thresholds, and conduct training. Supplier shall, at the request of Company, or, in the absence of any request from Company, at least quarterly, provide Company with a report of the incidents that it has identified and taken measures to resolve.

To the extent of a conflict between Supplier's policies, standards, and practices and these Requirements, these Requirements will govern for all Processing and other Supplier activities relating to the McCain Data and any failure to meet such Requirements will constitute a material breach under any agreement incorporating these Requirements.

Incident Response – Supplier shall collect and record information, maintain and protect logs, planning documents, audit trails, records and reports with respect to data security breaches, information security risk increases, information security controls, the storage, Processing, and transmission of information, and the accessing and use of Company systems. Supplier shall implement, maintain, comply with, and enforce Information Security Practices and information security controls with respect to information security and/or data breach responses. Supplier shall provide notice to Company as soon as possible following Supplier's discovery or reasonable belief that there has been unauthorized exposure, access, disclosure, compromise, or loss of sensitive or confidential McCain Data or systems (**"Security Incident"**). Supplier shall notify the McCain Global IT Service Department immediately of any security incidents via the McCain 24x7 Security Hotline at: +1 (506)-392-8100 and/or in writing via email to: GlobalISSecurityTeam@mccain.ca or DataSecurityIncidentResponseTeam@mccain.ca. As available, Supplier's notification should include a description of the nature of the Security Incident, the type of McCain Data involved, who may have obtained the McCain Data, what steps Supplier has taken or will take to investigate and mitigate the Security Incident, and a point of contact for additional information.

Asset Management and Equipment – Where applicable, Supplier must have processes in place to inspect all Supplier-supplied computing or data storage equipment used in providing services to Company to ensure that data is securely overwritten prior to disposal. Supplier must physically destroy storage media or overwrite information using industry standard techniques to make the original information unrecoverable (e.g., "wiped" or degaussed).

Subcontractor and Third Party Access. Supplier shall not subcontract any data Processing operations under its agreement with Company or otherwise provide a third party with access to McCain Data without Company prior written consent. When Company has provided such consent, Supplier shall take all reasonable steps to ensure the reliability of such third parties and shall require their compliance with its agreement with Company (and, if Company requires, they will execute a separate non-disclosure or other agreement with protections similar to those in its agreement with Company). Supplier shall be responsible for any noncompliance of a third party and this noncompliance will constitute a breach of Supplier's agreement with Company, as if committed directly by Supplier.

Non-Repudiation – Supplier agrees to protect the confidentiality, data integrity, authentication, and non-repudiation of Company devices and data flows in the underlying system. Supplier also agrees to protect all signing systems that support the integrity of information and user transactions.

Data Jurisdiction – Supplier agrees that all data centers, access points, WAN access points, and other relevant ingress and access points for McCain Data shall only reside in jurisdictions approved by Company.

Background and Screening Checks – To the extent permitted by local law, Supplier shall conduct appropriate background and screening checks prior to permitting any employee or contractor of Supplier to have access to McCain Data. Supplier shall in no event expose Company to a level of risk which is commercially unreasonable or which is higher than that to which Supplier would be comfortable exposing itself. Company may at its sole option require more extensive background checks for any employee or contractor of Supplier who will have access to Personally Identifiable Information or other information deemed highly sensitive by Company.

Source Code Review – Where applicable, Supplier shall provide to Company summary documentation of its secure product development life cycle, including the standards, practices (including continuous improvement), and development environment (including the use of secure coding practices) used to create or modify McCain Data and/or systems. At Company's request, Supplier shall agree that all code, prior to delivery, be analyzed by a reputable third party that specializes in application security.

Defect Resolution – For the avoidance of doubt, failure to comply with these Requirements is a failure to perform under the agreement between Company and Supplier and subject to any provisions for breach set forth therein. In addition to any remedies otherwise available, Supplier, at its sole expense, will be responsible for and redress any damages or costs caused by, and take all reasonable steps to cure, such failure to perform, and will implement all corrective actions reasonably required to prevent such deficiencies and occurrences applicable to Supplier's further performance under these Requirements.

Acceptable Use Policy – Company computing systems shall only be used for lawful purposes. When using or accessing Company systems or equipment, Supplier shall not knowingly transmit, retransmit, or store content, information, or material in violation of any federal or state laws or regulations, or any which may be offensive, obscene, or defamatory, or may infringe the trademarks or copyrights of others. When using or accessing Company systems or equipment, Supplier shall comply with the McCain Acceptable Use Policy and any other applicable acceptable use requirements as provided by Company and shall use its best efforts to ensure compliance by all of its employees and affiliates. Without limiting Company's access to all other remedies available at law or equity, the parties agree that Company shall have the right to immediately and without notice terminate the computing systems access of any Supplier employees or affiliates found to be in violation of Company acceptable use policies.

Right to Audit

During the term of this Agreement and not more than twice per year (unless circumstances warrant additional audits as described below), Company or its designate may audit the performance of the SLAs, information

security requirements, Supplier's information security posture, and Supplier's SLO performance, to ensure compliance with this Agreement. Unless the circumstances require immediate access, Company shall provide at least 10 business days' notice of such audit. In addition, Supplier agrees that findings from the audit will be remediated upon notification by Company. Notwithstanding the foregoing, the parties agree that Company or its designate may conduct an audit at any time, in the event of

i. audits required by Company's governmental or regulatory authorities,

ii. investigations of claims of misappropriation, fraud, or business irregularities of a potentially criminal nature, or

iii. Company reasonably believes that an audit is necessary to address an operational or material change, or issue in the relationship.

Non-Disclosure Agreement – Supplier has signed or agrees to sign a mutually agreed upon non-disclosure agreement with Company or to include equivalent confidentiality clauses within contracts signed with Company. Supplier also agrees to implement non-disclosure agreements with any employees, permitted sub-processors, or affiliates who will have access to McCain Data before they gain access to any confidential McCain Data.