Maple Leaf Foods Data & Cybersecurity Policy

All Suppliers who have access to data related to, provided by, or belonging to Maple Leaf Foods ("MLF Data") are expected, on request to demonstrate and certify their security policies, processes, and procedures and prove that they are able to provide adequate protection of such data, including meeting the following criteria:

POLICIES AND PROCEDURES

Suppliers must establish, implement, and maintain information security policies and a program of cyber security measures that is appropriate to prevent any access to confidential information of Maple Leaf Foods, including that they must maintain the currency of all software versions and security patch levels, managed anti-virus and malware detection.

COMPLIANCE AND ACCREDIATION

Suppliers are expected to comply with all applicable laws, including but not limited to the relevant Canadian and United States privacy legislation, Sarbanes-Oxley Act (SOX), General Data Protection Regulation (GDPR), Payment Card Industry Data Security Standard (PCI-DSS), and Statement on Standards for Attestation Engagements 16 (SSAE16) Service Organization Controls (SOC) Type I or II.

If confidential information of MAPLE LEAF FOODS is stored, then Suppliers must conduct routine security related audits and certifications. Supplier datacenters or hosted colocations must have recently completed a Statement on Standards for Attestation Engagements 16 (SSAE16) Service Organization Controls (SOC) 2 audit and must furnish any corresponding reports to Maple Leaf Foods on request. Suppliers that use a third party to store data, must ensure that all such third parties that maintain best in class certification equivalent to SSAE 16, ISAE 3402, SOC 2 and SOC 3 auditing standards for data centers and must be prepared to certify such compliance annually or on request.

PHYSICAL AND ENVIRONMENTAL SECURITY

Suppliers must ensure that all of Supplier's systems containing or accessing MLF Data contain access and authorization restrictions, and that all MLF Data is stored and located only in Canada or the United States or in environments under the jurisdiction of Canadian and United States legal authorities.

ACCESS CONTROL

Suppliers must maintain password and security protocols to control access to MLF Data, including, in the case of remote access, multi-factor authentication. Suppliers must maintain reasonable procedures to terminate access of their employers to MLF Data when it is no longer needed or relevant to the performance of their obligations. Suppliers must have safeguards in place to ensure that no employee or contractor can copy, move, or store the confidential information belonging to Maple Leaf Foods on to any storage device.

SYSTEM SECURITY

Suppliers must conduct periodic internal vulnerability assessment scans including, but not limited to, networks, servers, applications and databases, with applicable industry-standard security vulnerability scanning software to uncover security vulnerabilities.

Maple Leaf Foods Data & Cybersecurity Policy

AUDITING AND MONITORING

Suppliers must maintain an automated audit trail that documents system security events as well as any change management event that results in the access, modification, and/or deletion of information belonging to Maple Leaf Foods.

NETWORK SECURITY

Suppliers must maintain a formal process for approving, testing, and documenting all network connections and changes to the firewall and router configurations. Suppliers must configure firewalls to deny and log suspicious packets and restrict network connections that only allow appropriate and authorized traffic, denying all other traffic through the firewall. Firewall rules must be reviewed on a recurring basis.

DATA PROTECTION, SANITATION, AND DESTRUCTION

Suppliers must use encryption to protect MLF Data that is stored outside of their network environment, including in the case of MLF Data that is on a portable storage device such as a backup tape, laptop, memory stick, dvd or cd. Suppliers must not store Maple Leaf Foods Confidential Information on removable media (e.g., USB flash drives, thumb drives, memory sticks, tapes, CDs, or external hard drives) except: (a) for backup, business continuity, disaster recovery, and data interchange purposes as allowed and required under the Agreement and (b) using Strong Encryption.

INCIDENT REPONSE AND NOTIFICATION

Suppliers must maintain an incident management procedure that includes notification of Maple Leaf Foods immediately upon becoming aware of any potential destruction, loss, alterations, unauthorized disclosure of, or access to or accidental or actual destruction, loss, alteration, unauthorized disclosure of, or access to Suppliers' systems. Suppliers must follow incident response best practices and make reasonable efforts to identify the cause of incidents and take appropriate steps in order to remediate the cause of any incident. Under no circumstances shall Supplier, without the prior written consent of Maple Leaf Foods, make any public statement regarding Maple Leaf Foods' information technology systems or any incident or breach affecting Maple Leaf Foods information systems, or other resources.

CYBER-SECURITY INSURANCE

Suppliers shall be required to disclose to Maple Leaf Foods whether or not they maintain a cyber security insurance policy and if so, to provide Maple Leaf Foods with the relevant details of the policy. At Maple Leaf Foods' discretion, Suppliers shall be required to maintain a cyber security insurance policy with coverages and limits acceptable to Maple Leaf Foods.

Maple Leaf Foods Data & Cybersecurity Policy

BUSINESS CONTINUITY MANAGEMENT AND DISASTER RECOVERY

Suppliers must develop, operate, manage, and revise business continuity and disaster recovery plans that features daily back-up of data and systems, off-site storage of backup media and records, record protection and appropriate contingencies. Suppliers must have documented procedures for the secure backup and recovery of data and information, which must include, at a minimum, procedures for the transport, storage, and disposal of the backup copies of the data and, upon Maple Leaf Foods' request, provide such documented procedures.