CAE Information Security Terms for Suppliers

These CAE Information Security Terms for Suppliers ("**ISTS**") form part of and apply to the CAE Purchasing General Terms and Conditions ("**GTC**") that form part of a binding contract ("**Contract**") between CAE Inc. or the entity affiliated to CAE Inc. identified in the PO ("**CAE**") and the addressee ("**Supplier**") and apply to each Purchase Order ("**PO**") referring thereto that an authorized procurement or global strategic sourcing representative ("**Representative**") of CAE may issue to Supplier. Each PO shall contain a description of any required services ("**Services**"), goods, materials or items ("**Goods**") requested by CAE.

The obligations under the ISTS apply at any time Supplier, during the performance of the Contract, processes, stores or hosts Confidential Information and to all locations from which Supplier conducts business, whether under Supplier's direct control or under the control of Supplier's third party provider.

a. Information Security Program

1) Supplier must define, implement and maintain a comprehensive information security program which is defined as a set of policies, standards, procedures and controls aimed at protecting the confidentiality, integrity and availability requirements related to Confidential Information (as defined in the GTC) received for or during the performance of the Contract.

2) Supplier's security program must identify and assign roles and responsibilities pertaining to information security. It must establish coordination mechanisms among organizational entities and be approved by a senior officer of Supplier responsible and accountable for information security risk. Supplier must review its security program at least annually and update it to reflect any organizational changes or problems identified each year.

3) As part of Supplier's security program, Supplier must develop, disseminate and periodically review an audit and accountability policy that addresses all the elements covered by the scope of its information security program.

4) Supplier must provide prior written notice to CAE in the event Supplier intends to change the location where the Confidential Information is processed, stored or hosted.

5) Subject to Supplier's notification to CAE pursuant to subsection c.6), Supplier must notify CAE within 48 hours of any inability to meet its obligations set forth in the ISTS.

b. Assessment of Security Controls Performance

1) Supplier must, upon CAE's request, grant CAE or a third party mandated by CAE, permission to perform a review, assessment or audit of Supplier's compliance with the ISTS. Supplier must cooperate and provide access to relevant documentation, premises or personnel as reasonably requested by CAE or the third-party mandated by CAE, in the course of the review, assessment or audit. Additionally, Supplier must promptly provide CAE with the results of any assessments made by or for Supplier related to its cyber security program.

2) Supplier must define a security assessment and testing plan which defines the scope of the assessment of the implementation and effectiveness of security controls, possible enhancements of these controls within the scope of the organization and its environment. A report must be produced as a result of the assessment and a copy shall promptly be provided to CAE.

3) Supplier must develop a plan of action and milestones to address the vulnerabilities and weaknesses noted during the assessment. Existing plan of action and milestones must be updated regularly based on the findings from security assessments, business impact analysis and security monitoring activities.

4) Supplier must notify in writing CAE thirty (30) days before effecting any changes in the content of its security controls and/or cyber security program that could result in reduced protection, security and safeguarding of CAE's Confidential Information.

c. Risk Event Management

1) As soon as practicable, but in any event before the commencement of performance of any Services or delivery of Goods, Supplier must disclose in writing to CAE any and all security incidents, breaches or claims resulting from an information security incident that have occurred in the twelve months preceding the date of the PO. An information security incident also includes situations where Supplier suspects that the confidentiality, integrity and availability requirements associated with Supplier's network or systems have been violated.

2) Supplier must develop and implement an incident response program including a set of policies, processes, workflows, procedures that address purpose, scope, coordination, roles and responsibilities and capabilities that include preparation, detection, analysis, containment, eradication and recovery. The program must include an incident response plan containing a roadmap for the implementation of the incident response capability, description of the organizational structure dedicated to incident response, high-level approach to incident response, definition of reportable incidents, metrics for the assessment of the incident response capabilities and should incorporate lessons learned from previous incidents handling capabilities into its incident response procedures, training and testing. These documents must be communicated to all personnel involved in the incident response process, reviewed and updated at least annually.

3) Supplier must provide incident response training to its personnel consistent with assigned roles and responsibilities.

4) Supplier must track and document information security incidents.

5) Supplier must test at least annually its incident response capabilities to assess their effectiveness and document the results.

6) Supplier must inform CAE within 24 hours of a security/breach incident that may affect the security of Confidential Information, as further described in Section 22 of the GTC.

d. Business Continuity / Disaster Recovery

1) Supplier must identify, plan, document, test and implement business continuity and disaster recovery procedures that will allow for a timely recovery of critical business functions and processes in the event of a disruption of the business.

e. Third Parties

1) Without limiting the generality of Section 31 of the GTC, Supplier may not subcontract with any third party to perform any of its obligations under the ISTS without prior written consent of CAE.

2) Once any third party has been approved by CAE, Supplier must (i) require that such provider of external information system services complies with the current ISTS and with applicable laws and regulations; and (ii) monitor security control compliance by such external service provider on an ongoing basis.

3) Supplier must conduct an organizational assessment prior to outsourcing any service related to information security and a copy shall promptly be provided to CAE.

f. Software

1) Supplier agrees that the software that processes, stores or hosts CAE's Confidential Information (i) has been designed and developed according to the best industry practices, and (ii) does not contain any vulnerability not disclosed in writing to CAE.

2) Supplier agrees to actively and periodically monitor vulnerabilities in the software that processes, stores or hosts CAE's Confidential Information and remediate such vulnerabilities promptly, starting with addressing the highest priority threats as efficiently as possible.