Cybersecurity Requirements

1. Supplier shall take appropriate organizational and technical measures to ensure the confidentiality, authenticity, integrity and availability of Supplier Operations as well as Deliverables. These measures shall be consistent with good industry practice and shall include an appropriate information security management system consistent with standards such as ISO/IEC 27001 or IEC 62443 (to the extent applicable).

2. Supplier Operations means all assets, processes and systems (including information systems), data (including Purchaser data), Personnel, and sites, used or processed by Supplier from time to time in the performance of this Contract.

3. Should Deliverables contain software, firmware, or chipsets:

    a. Supplier shall implement appropriate standards, processes and methods to prevent, identify, evaluate and repair any vulnerabilities, malicious code, and security incidents in Deliverables which shall be consistent with good industry practice and standards such as ISO/IEC 27001 or IEC 62443 (to the extent applicable);

    b. Supplier shall continue to support and provide Services to repair, update, upgrade and maintain Deliverables including the provision of patches to Purchaser remedying vulnerabilities for the reasonable lifetime of the Deliverables;

    c. Supplier shall provide to Purchaser a bill of materials identifying all third-party software components contained in the Deliverables. Third-party software shall be up-to-date at the time of delivery to Purchaser;

    d. Supplier shall grant to Purchaser the right, but Purchaser shall not be obliged, to test or have tested Deliverables for malicious code and vulnerabilities at any time, and shall adequately support Purchaser;

    e. Supplier shall provide Purchaser a contact for all information security related issues (available during business hours).

4. Supplier shall promptly report to Purchaser all relevant information security incidents occurred or suspected and vulnerabilities discovered in any Supplier Operations and Deliverables, if and to the extent Purchaser is or is likely to be materially affected.

5. Supplier shall take appropriate measures to achieve that its subcontractors and suppliers shall, within a reasonable time, be bound by obligations similar to the provisions of this section.

6. Upon Purchaser's request, Supplier shall provide written evidence of its compliance with this section including generally accepted audit reports (e.g., SSAE-18 SOC 2 Type II).

7. Supplier shall provide to Customer all related documentation and the current and readable source code and object code of software developed or converted for Customer.

Customer has the right to yearly audit or have audited the Supplier’s compliance with the provisions of this section at the Supplier’s relevant site(s) without cause and, in addition, if Customer has a justified suspicion that Supplier is not in full compliance with those provisions, in each case upon reasonable prior notice.