Section P: Cybersecurity Risk Management
Revised: December 3, 2020

Cybersecurity Risk Management

1. The following provisions are applicable whenever the Supplier will store or process any information from Oshkosh Corporation or any if its subsidiaries and are in addition to any other information security requirements and safeguards applicable to Supplier.

2. "Cyber Incident" is defined as - An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

3. Supplier will use reasonable commercial efforts in accordance with industry standards that comply with the Oshkosh Supplier Cybersecurity Program or the Cybersecurity Maturity Model Certification (CMMC), whichever is applicable. Both programs are designed to:

    a) Provide confidentiality, integrity, and security of the information, supplier network, systems, and operations that the Buyer may interact with or store in their environment.

    b) Detect, prevent, and notify of any issues that may compromise the trust or information that was in trusted with Supplier.

    c) Satisfy contractual requirements for certification under all applicable regulations or standards.

4. Supplier further agrees to:

    a. Only collect, access, use, transfer or share Buyer information to authorized third parties, in performance of its obligations under the agreement and/or order, in conformance with this agreement, or to comply with legal obligations. Supplier will not make any secondary or other use (e.g. for the purpose of data mining) of Buyer information except as (a) expressly authorized in writing by Buyer in connection with Buyer's purchase of goods and/or services hereunder, or (b) as required by law.

    b. When asked, be able to provide a summary of its policies sufficient to evidence of reasonable satisfaction that each requirement is addressed in a manner consistent with the required Oshkosh Supplier Cybersecurity Program, or the appropriate contract requirements. Supplier shall provide Oshkosh Corporation with an updated index or summary upon request if changes are made within the supplier policy.

    c. Allow Oshkosh Corporation or its designee to conduct a security audit at Supplier's facilities with reasonable notice and allow a network audit at Oshkosh Corporation expense.

    d. Assure that all Oshkosh Corporation information and applicable software is appropriately backed up and recoverable in the event of a disaster or emergency, or information breach.

e. Provide Oshkosh Corporation with a termination plan that addresses how information will be returned to Oshkosh Corporation at the end of this agreement and/or order, including backup and archival information, and how the information will be permanently removed from Supplier's equipment and facilities. This plan shall include supplying the data to Oshkosh Corporation in an industry recognized, not proprietary database or format, and if not, a license to use the proprietary database software to access the data.

f. Supplier will not provide Oshkosh Corporation information to any other entity without the prior written approval of an Oshkosh Corporation representative.

g. Provide to Oshkosh Corporation written notice within 24 hours for breaches, or suspicion of breach of data that is (i) proprietary, (ii) highly classified, (iii) restricted, or breach of a system connected to Oshkosh Corporation systems. Such a notice will summarize in reasonable detail, the impact on Buyer or any individuals affected by such Cyber Incident and the corrective action and remediation efforts taken or proposed to be taken by the Supplier. Immediately following any Cyber Incident or any other failure to meeting information security standards, whether identified by Supplier or Oshkosh Corporation, the Supplier will take steps to mitigate risks posed. Failure to remedy the risk of a Cyber Incident or failure within the time frame and manner specified by Oshkosh Corporation is deemed a material breach of this agreement.

5. In the event a cyber security incident occurs Oshkosh Corporation has created a mechanism for suppliers to report Cyber Security Incidents through the OSN, Oshkosh Supplier Network at https://osn.oshkoshcorp.com/. All incidents will be systematically routed to the Oshkosh Global Information Security Office for review and disposition.

ANY PRINTED COPIES OF THESE TERMS AND CONDITIONS ARE UNCONTROLLED COPIES AND MAY BE OUTDATED. IT IS THE RESPONSIBILITY OF SUPPLIER TO VERIFY THAT IT IS IN COMPLIANCE WITH THE LATEST REVISION OF THESE TERMS AND CONDITIONS AS POSTED ON THE OSHKOSH PROCUREMENT WEBSITE OSN.OSHKOSHCORP.COM