Waupaca Foundry, Inc.

Security Supplemental Terms and Conditions

The terms and conditions set forth herein ("**Supplement**") together with the Waupaca Foundry, Inc.'s General Terms and Conditions ("**GTCs**"), as may be amended from time to time, are incorporated into and shall be and become a part of any other applicable agreements, Purchase Orders, Written Orders or similar documents whereby Waupaca Foundry, Inc. ("Buyer") purchases Services, Goods or Supplies from a party selling such Services, Goods or Supplies ("Seller") and the aforementioned documents shall constitute the agreement between the parties (the "**Agreement**"). Capitalized terms used herein shall have the meaning set out in the Agreement unless otherwise defined in this Supplement.

1. Security Program a. Prior to providing Services, or Goods, or Supplies and throughout the term of the Agreement, Seller (and any qualified subcontractors, if applicable) shall implement and maintain a security program that is based on ISO 27001/27002, or an equivalent industry standard security controls framework, that has administrative, technical and physical safeguards designed to: (i) protect the security, confidentiality and integrity of Buyer data, systems, infrastructure, and information; (ii) protect against any anticipated threats or hazards to the Buyer data systems, infrastructure, and information; (iii) protect against unauthorized access to or use of Buyer data, systems, infrastructure, and information; (iv) be created and implemented in accordance with all local, state and federal laws and regulations applicable to Information Security, and (v) protect against interruption in the delivery of Services or Goods or Supplies provided to Buyer ("Seller Security Program"); and

b. Seller shall provide documentation to demonstrate that such Seller Security Program has been implemented. If the Parties agree additional security requirements are applicable based on the nature of the Services, or Goods, or Supplies to be provided by Seller under the Agreement, Seller shall provide documentation to demonstrate such additional security requirements (e.g., PCI DSS, GDPR, in-vehicle cyber security requirements).

c. In accordance with any requirements agreed under any relevant sections of the Agreement, Buyer will not unreasonably withhold consent to the use of security subcontractors by Seller if such subcontractor is under terms at least as stringent as agreed between Buyer and Seller, and Seller remains responsible for the acts of the subcontractor.

d. Buyer and Seller agree to treat documentation provided under this Supplement in accordance with the confidentiality sections of the Agreement.

2. Periodic Testing and Assessments a. During the term of the Agreement, Seller shall at least annually, upon request, provide documentation and control test evidence of Seller's (or, as applicable, its subcontractors) continued maintenance of the Seller Security Program. In the event that Buyer reasonably identifies controls gaps, and reserving Buyer's rights as set forth in Section 5 below, Seller agrees to work in good faith with Buyer to update associated controls in line with industry-recommended solutions.

b. Seller agrees to, as applicable to delivery of the Services, or Goods, or Supplies, (i) cooperate with Buyer to verify and test (for example, if applicable, application security testing and penetration testing) the end-to-end security controls of the applications, infrastructures, and

processes supporting the Services, or Goods, or Supplies, (ii) conduct threat modeling in order to identify risks, and (iii) assist Buyer in completing its various security assessments.

3. Failure to Maintain and Security Incidents

a. (i) If at any time during the term of the Agreement, Seller (or, as applicable, its subcontractors) fails to maintain the Seller Security Program, Seller will promptly take the following corrective actions ("**Corrective Actions**"): (a) investigate and perform a root-cause analysis to identify the cause of the failure; (b) correct the problem in a commercially reasonable time period; (c) take appropriate preventive measures to reduce the probability of a recurrence; and (d) take appropriate actions to mitigate any adverse effects prior to correction;

(ii) Seller shall promptly provide the Buyer with a report of any failure, and provide updates on Corrective Actions, including root cause of the problem, implementation plan, and status.

b. If at any time during the term of the Agreement, Seller (or, as applicable, its subcontractors) becomes aware of a security incident or reasonably suspected security incident, Seller (or, as applicable, its subcontractors) shall promptly notify the Buyer at Security@waupacafoundry.com. If no response is received within sixty (60) minutes, call U.S. (715) 258-1727. Seller shall implement a remediation plan agreed by the parties.

4. Buyer Right to Audit

Seller shall permit Buyer and its authorized representatives to audit Seller's compliance with this Supplement at any time during Seller's normal business hours upon advance written notice to Seller. Seller shall also obtain for Buyer the right at any time during normal business hours to audit any facilities or entities used to fulfill Seller's obligations under the Agreement. Seller shall cooperate in all respects with any such audits.

5. Remedy for Failure to Comply

In addition to any other remedies available to Buyer, in the event that Seller (or, as applicable, its subcontractors) does not maintain the Seller Security Program, Buyer may immediately suspend any or all of Seller's (or, as applicable, its subcontractor's) access to Buyer data, systems, infrastructure, and information or Seller's delivery or implementation of Services, or Goods, or Supplies, as applicable. Buyer will have no payment obligations to Seller for Services, or Goods, or Supplies that are not delivered as a result of the suspension.