

**Purchase Order Terms and Conditions, Technology Vendor Addendum**

The terms and conditions of this Addendum are incorporated into the contract between MCW and the vendor/supplier attached hereto. To the extent there is any conflict between the terms of this Addendum and the contract to which it is attached and incorporated into, the terms of this Addendum will govern.

- 1. Security Incident Notice.** Supplier shall notify MCW, without undue delay and in no event later than seventy-two (72) hours after discovery, of any security incident that has materially affected, or is reasonably likely to materially affect, the confidentiality, integrity, availability, authenticity, or provenance of any products or services supplied under this Agreement. Such notice shall set forth the material facts then known, the affected products or services, the nature and scope of the impact, and the mitigation or corrective actions being undertaken, and Supplier shall provide supplemental notice as additional material information becomes available.
- 2. Bill of Materials.** With respect to any delivered product, Supplier shall provide a current bill of materials reasonably sufficient to identify the material components of such product, including a software bill of materials to the extent applicable and reasonably available, upon delivery and following any material update or major release. Any such bill of materials may be provided subject to reasonable confidentiality restrictions.
- 3. Assessment of Rights and Remediation.** Upon not less than forty-five (45) days' prior written notice, and not more than once during any twelve (12)-month period except following a security incident, a material change, or where MCW has a reasonable basis for concern, MCW may request information reasonably necessary to assess Supplier's cybersecurity posture as it relates to the products or services, including current independent assurance materials (e.g., SOC 2 Type II reports, HiTrust, FedRAMP authorization materials, or comparable third-party assessment reports). If such materials are unavailable or insufficient for the foregoing purpose, Supplier shall reasonably cooperate with written requests for information, security questionnaires, and focused remote assessment activities limited to the relevant products or services and related controls. Supplier may redact information not relevant to the products or services or reasonably necessary to protect confidential information, provided that such redactions do not materially impair the assessment. If material deficiencies are identified, Supplier shall use commercially reasonable efforts to remediate or mitigate such deficiencies pursuant to a written remediation plan and mutually agreed remediation timelines, considering risk severity, technical feasibility, and operational impact.