Cybersecurity Appendix

In the event that any Services or Products (defined below) supplied under the Agreement include any Software or associated development activities, the Supplier agrees to comply with the requirements set forth in this Appendix. In the event of any inconsistency or conflict between this Appendix and any other provision of the Agreement with respect to subjects covered by this Appendix, then the provision requiring the more stringent requirement shall prevail. The requirements in this Appendix are in addition to any cybersecurity-related obligations between the Buyer and the Supplier under the Agreement.

Part A: Definitions

"Agreement" means the agreement or purchase order in which this Appendix is referenced or to which this Appendix is attached.

"Copyleft License" means the GNU General Public Licenses version 2.0 (GPLv2) or version 3.0 (GPLv3), Affero General Public License version 3 (AGPLv3), or any other license that requires, as a condition of use, modification and/or distribution of or making available over a network any materials licensed under such a license to be: (a) licensed under its original license; (b) disclosed or distributed in source code form; (c) distributed at no charge; or (d) subject to restrictions on assertions of a licensor's or distributor's patents.

"**Cybersecurity Laws**" are all laws, regulations, codes, guidance (from regulatory and advisory bodies), international and national standards, and sanctions, relating to security of networks, information systems, security breaches including data breaches and incident reporting requirements, including without limitation any privacy or data protection laws, the Cybersecurity Directive ((EU) 2016/1148), Commission Implementing Regulation ((EU) 2018/151), the Network and Information Systems Regulations 2018 (SI 506/2018), all as amended or updated from time to time.

"Cybersecurity Vulnerability (ies)" means any bug, software defect, virus, design flaw, harmful code, security incident or other vulnerability (whether known, latent or otherwise) with Software associated with a Product that could adversely impact: (a) the Buyer (b) any network, software or information system or (c) the confidentiality, security, integrity or availability of information or processes associated with the Product.

"Cybersecurity Vulnerability Management Plan" is a plan, created by the Supplier and submitted to the Buyer for approval, which lays out the Supplier's secure code practices, SDLC, proactive measures to be taken to identify Cybersecurity Vulnerabilities and incident response plan.

"Data Hosting Services" means the provision of hardware, systems, Software and infrastructure required to store and manage access to data, including any disaster recovery or business continuity related processes.

"Deliverables" means the goods, Products, Equipment, IT Hardware, Third-Party Services and the like that are incidental to and the "minor" accompaniment to the Software procurement.

"Device" means the computer system or server that hosts the Product(s) or a portion thereof.

"Good Industry Practices" means the standards, practices, methods and procedures conforming to all applicable Laws and the degree of skill, diligence, foresight and operating practice which would reasonably be expected from a skilled and experienced Supplier engaged in the same or similar type of undertaking under the same or similar circumstances to the Agreement.

"Law(s)" means all applicable laws, legislation, rules, regulations, codes and standards of governmental agencies or authorities having jurisdiction over the activities relating to this Policy, the Agreement and any SOW or PO under it or where the Deliverables will be used, including all applicable export control laws.

"Open Source Software" or "OSS" means any material that is distributed as "open source software" or "freeware" or is otherwise distributed publicly or made generally available in source code form under terms that permit modification and redistribution of the material on one or more of the following conditions: (a) that if the material, whether or not modified, is redistributed, that it shall be: (i) disclosed or distributed in source code form; (ii) licensed for the purpose of making derivative works; and/or (iii) distributed at no charge; (b) that redistribution must be licensed or distributed under any Copyleft License, or any of the following license agreements or distribution models: (1) GNU's General Public License (GPL), Lesser/Library GPL (LGPL), or Affero General Public License (AGPL), (2) the Artistic License (e.g., PERL), (3) the Mozilla Public License, (4) Common Public License, (5) the Sun Community Source License (SCSL), (6) the BSD License, (7) the Apache License and/or (8) other Open Source Software licenses; and/or (c) which is subject to any restrictions on assertions of patents.

"Product(s)" mean any goods, products, Software, Deliverables and associated Services supplied under the Agreement.

"Services" means any and all services provided by Supplier to Buyer pursuant to the terms of the Agreement referred to with more particularity in related Statement(s) of Work ("**SOWs**") and POs.

"Software" means all operating systems, applications, and portions of code used or created by the Supplier to carry out and deliver the agreed work. This includes both software hosted by the Supplier (SaaS or PaaS) and software that is provided to Buyer to host. Plug-ins, drivers, scripts, mobile apps, desktop apps, operating systems, web apps, macros, databases, formulas, flow charts, and any other code are all included in this category.

"Third-Party Materials" means materials which are incorporated by Supplier in any Products provided to Buyer, the proprietary rights to which are owned by one or more third-party individuals or entities.

Part B: Secure Software Development

1. Supplier shall ensure all Products have been developed in accordance with principles of secure software development consistent with software development Good Industry Practices, including security design review, secure coding practices, risk-based testing and remediation requirements. Supplier must use Good

Industry Practices and measures to secure the Software development environment of the Products from unauthorized access.

2. Supplier shall include cybersecurity guidance in the Product documentation provided to Buyer. This documentation shall include guidance on how to configure the Products and/or the surrounding environment to best ensure security. It shall also include guidance on which logical or physical ports are required for the Product(s) to function. If authentication is used to protect access to any service or capability of the Product(s), regardless of the intended user of that service/capability, Supplier shall ensure that:

    (i) the Product(s) shall not provide access to that service or capability using a default account/password;
    (ii) the Product(s) shall not provide access to that service or capability using a "Backdoor" account or password;
    (iii) the Product(s) associated authentication and password change processes shall be implemented with an appropriately secure cryptographic level; and
    (iv) Buyer shall be able to change any passwords supported by the Product(s).

3. Services or capabilities that are not required to implement the Product's functionality shall by default be disabled or shall require authentication to protect access to the service or capability.

4. In the event that any wireless technology is incorporated in any Product(s), Supplier shall document that the wireless technology complies with standard operational and security requirements specified in applicable wireless standard(s) or specification(s) (e.g., applicable IEEE standards, such as 802.11) and by Law.

5. In the event that any cryptographic systems are contained in the Product(s), Supplier shall only use cryptographic methods that are "Approved" as defined in the Federal Information Processing Standard (FIPS) Security Requirements for Cryptographic Modules (FIPS 140-2) or local equivalent standard and Supplier shall provide an automated remote key-establishment (update) method that protects the confidentiality and integrity of the cryptographic keys.

6. All data transfer handled by the Product(s), whether over private or public networks, will be sent using a Buyer approved encryption mechanism such as SSH version 2 or higher, or TLS version 1.2 or higher. No unencrypted data transfers will be allowed.

7. If the Product(s) is installed on a Supplier provided Device, or if there is Software hosted by the Supplier that forms part of the Product(s) (such as a SaaS model), then the Device must: (i) incorporate a host-based firewall to block any unsolicited inbound requests, while documenting any exceptions required; (ii) incorporate approved anti-virus software which must be active and up to date on the Device; (iii) all critical and recommended software updates and patches must be installed for the Device operating system and all software running on the Device; (iv) disk encryption must be enabled on all internal operating system and data drives and the cipher set to AES-128 encryption or better on the Device

Part C: Cybersecurity Vulnerabilities, Assessment and Reporting

1. Supplier must develop and maintain an up-to-date Cybersecurity Vulnerability Management Plan designed to promptly identify, prevent, investigate and mitigate any Cybersecurity Vulnerabilities and perform any required recovery actions to remedy the impact.

2. Supplier shall notify Buyer's Representative at the agreed Address for Service within a reasonable period, in no event not to exceed five (5) Business Days after discovery, or shorter if required by applicable Law, of any potential Cybersecurity Vulnerability. Supplier shall report any Cybersecurity Vulnerability to Buyer's Representative referred to in the applicable Agreement or SOW. Within a reasonable time thereafter, Supplier shall provide Buyer, free of charge, with any upgrades, updates, releases, maintenance releases and error or bug fixes necessary to remediate any Cybersecurity Vulnerability. Supplier shall cooperate with Buyer in its investigation of a Cybersecurity Vulnerability, whether discovered by Supplier, Buyer, or a third-party, which shall include providing Buyer a detailed description of the Cybersecurity Vulnerability, the remediation plan and any other information Buyer reasonably may request concerning the Cybersecurity Vulnerability, as soon as such information can be collected or otherwise becomes available. Buyer shall have the right to conduct a cybersecurity audit assessment of the applicable Product(s) which may involve penetration tests or other security testing as required, and audit of the Product development lifecycle. Supplier shall designate an individual responsible for the management of the Cybersecurity Vulnerability and shall identify such individual to Buyer promptly.

3. Other than when required by Law, Supplier may not make or permit any public statements concerning Buyer's involvement with any such Cybersecurity Vulnerability to any third-party without the explicit written authorization of Buyer's Legal Department.

4. To the extent any applicable Law (including any privacy or data processing Laws) requires the Supplier to notify or report any security incident, including any Cybersecurity Vulnerability, to a regulator or national authority or any other organization, Suppler shall comply with the applicable Law within the required time periods to provide such notification or report. If applicable, Suppler shall (at its own cost) co-operate promptly with Buyer so that it may comply with its obligations under applicable Law.

Part D: Additional Representations and Warranties

1. **Open-Source Software and Third-Party Materials Warranty.** Supplier represents, warrants and covenants that (i) it has disclosed all Copyleft Licenses, Open Source Software and Third-Party Materials utilized with the Product(s) and no Open Source Software or Third-Party Materials have been or will be provided to Buyer or used as a component of or in relation to any Product(s) provided under the Agreement, except with the prior written authorization of Buyer; and (ii) all Open Source Software contained within the Product(s) are and shall be in material compliance with the terms and conditions of the applicable licenses governing their use, and the Product(s) or the use thereof by Buyer shall not cause Buyer or Buyer's Software or intellectual property rights to be subject to the terms or conditions of a Copyleft License, or require Buyer to fulfil any open source license obligations for any Open Source Software contained within the Product(s).

2. **Code Integrity Warranty.** Supplier represents, warrants and covenants that the Product(s) (including any Open Source Software and Third-Party Materials utilized with the Products): (a) do not contain any restrictive devices such as any key, node lock, time-out, time bomb, or other function, whether implemented by electronic, mechanical or other means, which may restrict or otherwise impair the operation or use of the Product(s) or any material embodying or comprising the Product(s); and (b) shall be free of viruses, malware, Cybersecurity Vulnerability and other harmful code (including, without limitation, time-out features) which may interfere with the use of the Product(s) regardless of whether Supplier or its personnel purposefully placed such code in the Product(s). In addition to exercising any of Buyer's other rights and remedies under this Appendix and the Agreement or otherwise at Law or in equity, Supplier shall provide Buyer, free of charge, with any and all new versions, upgrades, updates, releases, maintenance releases, and error or bug fixes of the Product(s) (collectively, "**Revised Code**") which prevents a breach of any of the warranties provided under this Appendix or corrects a breach of such warranties. Revised Code contained in the Product(s) constitutes Products for purposes of this Appendix.

3. **Good Industry Practices**. The Supplier represents, warrants and covenants that it:
   (a) shall use best efforts to ensure continuity of the Services and Data Hosting Services at all times;
   (b) shall use best efforts to ensure the continuity of any services, works or manufacturing process provided by Buyer that rely on the Product(s); and
   (b) shall at all times in accordance with Good Industry Practices implement, operate, maintain and adhere to its Cybersecurity Vulnerability Management Plan as required in Part C, Clause 1 of this Appendix, and shall provide copies of such Management Plan to Buyer promptly on its request.

4. **Supplier Indemnity.** The Supplier shall defend, indemnify release and hold the Buyer, its Affiliates and its and their customers, and each of its and their directors, officers, managers, employees, agents, representatives, distributors, resellers, sublicensees, contractors, successors and assigns (collectively, "**Indemnitees**") harmless from any and all claims, legal actions, demands, settlements, losses, judgments, fines, penalties, damages, liabilities, costs and expenses of any nature, resulting from, arising out of, or relating to any breach by the Supplier of its obligations under this Appendix or relating to applicable Cybersecurity Laws.

Part E: Additional Insurance

Supplier shall, at its own cost and expense, obtain and maintain in full force and effect insurance consistent with the requirements set forth in the Buyer's Insurance Appendix, to include Cyber Event Coverage, covering all Products including failure of IT security (including any liability arising from or related to any Cybersecurity Vulnerability), data privacy breach, third-party property and intellectual property rights infringement.

Part F: Audit & Assessment

The Supplier agrees to participate in an annual vendor security assessment directed by the Buyer. This assessment will include:

i. Providing a current SOC 2 Type 2 report or ISO 27001 certificate (or both), or another third-party attestation.
ii. Providing a current third-party penetration test for Buyer's review.
iii. Providing updated copies of company policies, or reviewing those policies with Buyer, as appropriate.
iv. Providing an updated network architecture diagram, if applicable.
v. Continuous updates: Supplier agrees to notify Buyer within a reasonable time frame of any changes to their answers to its security questions, rather than waiting for the next annual review to take place.
vi. Right to audit: Supplier agrees to cooperate in audits of the answers that they provide during their annual reviews, at Buyer's request.

<<<End of Document>>>