SUPPLIER ACCEPTABLE USE POLICY

1. Purpose

This Supplier Acceptable Use Policy (the "**Policy**") regulates and manages Supplier compliance with Buyer's Systems security programs and Supplier's use of Buyer's Electronic Information Resources to ensure that they are used in a manner that:

(i) serves the intended purpose of Buyer's Purchase Orders;
(ii) complies with other Buyer policies, code(s) of conduct and applicable Laws;
(iii) maintains the Buyer's good reputation;
(iv) protects Buyer Confidential Information and Buyer Property; and
(v) limits the possibility of damage to, unauthorized access to and use of Buyer Systems, Buyer Property and data.

2. Definitions

Capitalized terms used and not otherwise defined in this Policy shall have the meaning assigned to such terms in the Parties' underlying contract Terms and Conditions (together **"the Agreement"**).

"Buyer Confidential Information" shall, whether furnished before or after the date of the Agreement and irrespective of the form of communication, mean: (i) the terms of the Agreement; (ii) all information and material disclosed or provided by Buter to Supplier, including Buyer Property and Confidential Information; (iii) all information derived from Buyer's Property; and (iv) all of Buyer's IP Rights.

"Buyer's IP Rights" means Buyer shall own exclusively all rights in ideas, know-how, inventions, works of authorship, documentation, strategies, plans, data and databases created in or resulting from Supplier's performance as agreed by the Parties under the Agreement, including all patent rights, copyrights, moral rights, rights in proprietary information, data rights, database rights, trademark rights and other intellectual property rights.

"Buyer Property" means all tangible and intangible property, including information or data compilation of any description, tools, materials, plans, drawings, software, knowhow, documents, intellectual property, equipment or material: (a) furnished or licensed to Supplier by Buyer; (b) specifically paid for by Buyer; or (c) created with Buyer IP Rights and shall remain Buyer's personal property.

"Cybersecurity Vulnerability Management Plan" is a plan, created by Supplier, submitted to 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.

"**Electronic Information Resources**" includes but is not limited to Buyer's network, servers, personal computers, workstations, Software, hardware, internet/intranet, electronic messaging systems ("E-mail"), fax machines, network and mobile telephony devices, pagers, and the like.

"**Industry Practices**" means the best 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 skilled and experienced Supplier Personnel engaged in the same or similar type of undertaking under the same or similar circumstances to the Services and Deliverables.

"Laws" mean all applicable laws, legislation, rules, regulations, codes and standards of governmental agencies or authorities having jurisdiction over the activities relating to this Policy and the Agreement and any related SOW or Purchase Order under it, including all applicable export control laws.

"Software" means all operating systems, applications, and portions of code used or created by a Supplier to carry out and deliver the agreed work. This includes both software hosted by Suppliers (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.

"Supplier Personnel" means all persons and entities providing any Services and/or Deliverables under this Policy and the Agreement, including Supplier's parents, subsidiaries, affiliated companies, employees, agents, contractors, subcontractors and suppliers of any tier, as well as anyone directly or indirectly employed or retained by any of them or acting on behalf of any of the foregoing.

"System(s)" (either Buyer's or Supplier's) means property not limited to technology assets owned by Buyer or Supplier and/or third-party applications used by the Parties under license.

3. Scope

This Policy applies to all Buyer legal entities and their 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, "**Buyer Personnel**") and Supplier Personnel.

All Supplier Personnel are responsible for adhering to best Industry Practices of Supplier's industry and shall have the requisite skill, experience and qualifications to represent the Supplier in respect of this Policy.

4. Right to Access/Privacy

Buyer's Electronic Information Resources and all data residing therein is owned exclusively by Buyer and as such may be viewed or accessed at any time by Buyer without the consent or knowledge of Supplier Personnel.

Buyer has the right but not the obligation to monitor, access and review any aspects of its Electronic Information Resources including, but not limited to, monitoring internet use, reviewing E-mail sent and received by Supplier Personnel, sniffing network traffic and reviewing files stored on any communication Systems.

The Parties agree that Supplier Personnel have no privacy expectations in any Buyer Electronic Information Resources, or related data.

Irrespective of any wording to the contrary in this or any other agreement, Buyer's data shall always remain the property of the Buyer and shall never be mined by the Supplier or used by Supplier except to carry out the Services that the Buyer is purchasing.

5. Appropriate Use of Buyer's Electronic Information Resources

Supplier represents and warrants that Supplier Personnel shall comply with the following when accessing the Buyer's Electronic Information Resources. That Supplier Personnel shall:

(i) exercise the same degree of care in accordance with best Industry Practices and adopt the same degree of professionalism when communicating by phone or E-mail, or writing a letter or memo on behalf of the Supplier;

(ii) maintain Buyer Property, Confidential Information and data stored on any information storage or processing devices or systems in accordance with this Policy;

(iii) immediately report any actual or possible theft or unauthorized access to or use of any passwords, Buyer data, or assigned Buyer Property to the Buyer's Representative in accordance with the Agreement;

(iv) only use Buyer's Confidential Information, Property and data & Electronic Information Resources for the purposes of fulfilling its obligations under the Agreement; and shall use the same degree of care as with its own assets and confidential information, which shall be at least in accordance with the best Industry Practices of Supplier's industry. Supplier Personnel shall prevent any disclosures of the same, except to authorized Personnel and solely to the extent necessary to permit them to assist the Supplier in performing its obligations under this Agreement and pursuant to applicable

Law;

(v) ensure passwords to Buyer's Systems are protected against loss, theft, damage, compromise, or misuse;

(vi) only download or use pre-approved licensed Software authorized by Buyer's IT Department on Buyer's Systems;

(vii) use Software purchased by Buyer only for its intended purpose applicable to the Agreement, always consistent with Buyer's IT department policies for Software installation;

(viii) ensure that Buyer's Electronic Information Resources must be password protected with an active automatic screen lock feature that activates after fifteen (15) minutes or less of inactivity. Users must lock Buyer's Electronic Information Resources when unattended and never leave a resource unattended in a public place;

(ix) take measures to prevent the spread of viruses, worms, phishing email messages, and malicious software by not installing unauthorized software, being careful when clicking on any links contained in e-mails, and not opening links or attachments from unexpected senders. Users must immediately report any actual or possible impacts to the Buyer's Representative (particularly in respect of malware or unauthorized access to Buyer's Systems) in accordance with the Agreement;

(x) not allow a third-party to access, view, store or process Buyer's unencrypted Confidential Information, other than personal information specified elsewhere in this Policy or in the Agreement, without the express written permission of the Buyer. If a third-party has access to encrypted information, but also has access to the encryption key, that qualifies as having unencrypted access under this sub-section;

(xi) not allow Supplier Personnel to use Buyer's Electronic Information Resources to make any public announcements, take or release any photographs or make any statements on social media in about the Supplier's engagement with Buyer in the Agreement;

(xii) only provide Deliverables and Services that do not constitute an infringement or violation of any rights of third-parties, including intellectual property rights; and

(xiii) only provide Services and Deliverables that conform in all material respects with all requirements of the Agreement, all specifications and documentation and in any applicable SOW or PO.

6. Prohibitions on Usage of Buyer Electronic Information Resources

Supplier Personnel shall not use Buyer's Electronic Information Resources in any of the following circumstances, which are strictly prohibited by this Policy. Usage:

(i) in a manner that jeopardizes the confidentiality, integrity, or availability or safety of the Buyer's Electronic Information Resources;

(ii) in violation of applicable Laws, regulations or compliance requirements, including ant-harassment Laws;

(iii) to access, display, send, receive, store, create, or transmit images or communications that mock, degrade, or disrespect a protected class or an individual's legally protected characteristics;

(iv) to access, display, send, receive, store, create, or transmit pornography or sexually explicit images or communications;

(v) for any personal reasons;

(vi) that involves sending or forwarding general business (i.e. non-personal) emails from an authorized Buyer's E-mail account to a personal or non-Buyer account without prior authorization by the Buyer;

(vii) for unauthorized solicitation purposes or promotions;

(viii) purposes outside of scope for the agreed Services and/or Deliverables;

(ix) of Buyer email account to state or imply that Supplier Personnel is authorized to speak on behalf of Buyer, unless expressly authorized to do so by the Buyer;

(x) of another user's account or attempting to capture or guess other users' passwords or other credentials; by sharing individual user account passwords or other credentials with others or allowing someone else to use a password;

(xi) via unauthorized access directly to Buyer's IT networks over and above approved Buyer Systems access;

(xii) Involving tampering with Buyer's Systems, installing unauthorized Software, disabling, or otherwise interfering with security controls on a Buyer's Systems;

(xiii) via unauthorized access, transmission, or distribution of third-party copyrighted materials without an active license that may constitute an infringement or violation of any rights of third-parties, including intellectual property rights;

(xiv) of Buyer Electronic Information Resources in conjunction with the execution of programs, Software, or processes that are intended to disrupt (or that could reasonably be expected to disrupt) other Buyer computers or network users, or damage or degrade performance, Software, or hardware components of a Buyer Electronic Information Resources;

(xv) by knowingly establishing, or causing to be established, communications to Buyer's Systems that could allow unauthorized access to Buyer Electronic Information Resources; and

(xvi) of Buyer Electronic Information Resources other than for their intended and authorized purpose(s), including but not limited to; mining cryptocurrency and operating or assisting in the operation of a non-Buyer business.

7. Confidential Information Security

Buyer Confidential Information or Buyer Property must not be transmitted over external networks, including the internet, without using an appropriate encryption mechanism approved by the Buyer's Representative.

All Buyer Confidential Information and Buyer Property is the property of the Buyer and can only be used, transferred, stored or processed in ways that are consistent with the Policy, the Agreement and pursuant to applicable Law and that is permitted for use by the Buyer.

If Supplier is requested or required by interrogatories, subpoena, Court Order or similar legal process, to disclose any E-Mails, Buyer Confidential Information or Buyer Property, it agrees to provide Buyer with prompt written notice (no later than two (2) Calendar Days following receipt of such request) of each such request/requirement, to the extent practicable, so that Buyer may seek an appropriate protective order and/or waive compliance by Supplier with the provisions of this Policy, as appropriate. Failure to disclose or produce such Buyer Confidential Information or Property or the alteration or deletion of the same that are identified for disclosure may subject the Buyer and Supplier Personnel responsible for such failure to formal sanctions.

8. Compliance with Laws & Violations of this Policy

All Services & Deliverables shall be carried out and delivered in full compliance with all applicable Laws. Any Supplier Personnel that observes or is made aware of a suspicious, questionable or unauthorized event must report it to Buyer's Representative without delay. Security incidents or threats include, but are not limited to:

(i) any violation of this Policy;

(ii) intrusions of Buyer's Electronic Information Resources;

(iii) attempts (either failed or successful) to gain unauthorized access to Buyer's Electronic Information Resources Buyer system or database;

(iv) misuse of Buyer's Electronic Information Resources by Supplier Personnel or any third-party authorized by Supplier to have access to the same;

(v) unauthorized access to Buyer's Electronic Information Resources;

(vi) virus attacks

(vii) unwanted disruption or denial of service to Buyer's Electronic Information Resources; and

(viii) changes to Buyer's Electronic Information Resources without Buyer's knowledge, instruction, or consent.

9. Baseline Hardening & Minimum Standards Applicable to Systems Access & Buyer's Electronic Information Resources

Any Supplier Personnel or third-party who has been authorized to use a Supplier System that is not owned and controlled by the Buyer to connect to Buyer's Electronic Information Resources, must ensure that such System meets the following hardening standards:

(i) System utilizes a host-based firewall to block any unsolicited inbound requests, while documenting any exceptions required;
(ii) approved anti-virus software is active and up to date on the System;
(iii) all critical and recommended patches must be installed for the operating system and all software running on the System, in accordance with the Supplier's patch management policy;
(iv) endpoints should have web filtering enabled with security threat categories blocked (at a minimum);
(v) access to Buyer Electronic Information Resources shall be routed through Buyer's approved remote access software. Buyer will provide documentation and requirements;
(vi) full disk encryption must be enabled on all Systems and data drives and the cipher set to AES-128 encryption or better;
(vii) removable media shall not be used for storing or transferring Buyer data;
(viii) data that is classified as Confidential or Restricted cannot be stored on non-Buyer Systems and devices. This data should be stored in approved Buyer Systems and be worked on live; and
(ix) if the System is owned by a Supplier or third-party authorized by Buyer, then a: (a) Cybersecurity Vulnerability Management Plan; (b) risk management plan; (c) a warranty signed by the Supplier's CISO (or equivalent position) that the Supplier and its Personnel shall comply with this Policy shall be submitted to the Buyer's Representative prior to commencement of Services/Deliverables impacted by this Policy in accordance with the Agreement and provided an annual basis thereafter. This can be during annual Supplier audits

10. Signatures

Supplier warrants that all Supplier Personnel and authorized third-party personnel granted access to the Buyer's Electronic Information Resources shall be provided a written copy of this Policy and has signed the following statement before access is granted to Buyer Electronic Information Resources:

"I have received a written copy of this Suppler Acceptable Use Policy.

I have read and fully understand the terms of this Policy and agree to abide by it.

I acknowledge that:

(i) security software may record the internet address of any site that I visit and keep a record of any network activity in which I transmit or receive any kind of file, including E-mail messages

(ii) any message I send or receive will be recorded and stored in an archive file for the Parties

(iii) any violation of this Policy may lead to revocation of my use privileges or even legal sanction. "

11. Escalations & Enquires on this Policy

For queries or clarifications on this Policy please contact Buyer's Representative.

<< END OF DOCUMENT >>