

Privacy & Security Addendum to Standard Purchase Order Terms and Conditions

1. **General** This addendum outlines Privacy and Security terms and conditions that are required in addition to Oshawa PUC Networks Inc ("OPUC") standard purchase order terms and conditions for all goods and services related to operational and information technology (*hardware, software and data*) including communication networks, information systems, industrial controls and all programmable electronic devices.

2. **Acceptance of Purchase Order** The Supplier by the Acceptance of this Purchase Order (the "Order") accepts all the terms and conditions of this Addendum, in addition to OPUC standard purchase order terms and conditions. These terms and conditions supersede and take precedence over any and all previous verbal or written arrangements in connection with this Order. Any deletions, modifications, alterations of, or additions to the terms and conditions of the Order to be binding shall be in writing and specified by OPUC in the Order and shall be attached to this Purchase Order.

Privacy

3. **Definitions**

(a) **Authorized Personnel** means all employees, representatives, agents, contractors, subcontractors and vendors of the Supplier who require access to Personal Information for the purpose of providing the goods and services in this Order.

(b) **MFIPPA** means the Ontario Municipal Freedom of Information and Protection of Privacy Act which OPUC is subject to.

(c) **PIPEDA** means the Personal Information Protection and Electronic Documents Act of Canada which applies to private-sector organizations across Canada that collect, use or disclose personal information in the course of a commercial activity, and which Suppliers may be subject to.

(d) **Personal Information** means information about an identifiable individual including without limitation: name, address, birth date, gender, marital status, telephone number, electricity consumption, and account numbers. Authorized Personnel may be given access to Personal Information by OPUC for the purposes of this Order.

(e) **Privacy Law** means MFIPPA, PIPEDA and any other applicable law created to protect the privacy of personal information.

(f) **Privacy Requirements** means collectively, Privacy Law and the terms and conditions in this addendum.

4. **Personal Information Access Acknowledgement** Supplier acknowledges and agrees that it may be necessary in the course of providing the goods and services in this Order, for Supplier to access, compile and use Personal Information on behalf of OPUC.

5. **Ownership of Personal Information** Nothing in this Order provides Supplier with any rights to Personal Information disclosed by or originating from OPUC, other than the limited right to access,

compile and use Personal Information as set out in this Order. Supplier acknowledges and agrees that Personal Information shall remain under the control of OPUC, including without limitation, when Supplier is using and storing Personal Information for the purpose of providing the goods and services in this Order.

6. **Personal Information Restrictions** Supplier shall only access, compile and use Personal Information to the extent required for the purpose of providing the goods and services of this Order and shall not access, compile or use Personal Information on its own behalf or for its own purposes or those of a third party other than OPUC. Without limiting the generality of the preceding, Supplier shall not aggregate or otherwise modify Personal Information for any purpose other than the purposes of this Order, and shall not disclose Personal Information to anyone other than Authorized Personnel. Supplier acknowledges and agrees to comply fully with the Privacy Requirements.

7. **Obligation to Notify OPUC** Supplier shall immediately notify OPUC in writing upon any of the following:

- (a) Supplier receives a complaint or allegation, or independently concludes that any of its practices or procedures in providing the goods and services in this Order contravene Privacy Law;
- (b) Supplier becomes aware of loss, theft, unauthorized access, disclosure, copying, use or modification of any Personal Information or breach of Privacy Requirements
- (c) Supplier becomes aware of any vulnerability or breach of its privacy controls and safeguards, whether by Authorized Personnel or others, which may adversely impact the security and integrity of Personal Information
- (d) Supplier receives any privacy-related requests or complaints in relation to the goods and services of this Order;
- (e) Supplier receives a production or disclosure order, in any form, regardless of the issuing authority, purporting to apply to Personal Information.

8. **Assistance with Privacy Compliance and Continuous Improvement** Upon request, Supplier agrees to cooperate and assist OPUC in privacy compliance audits, reviews and investigations to:

- (a) Provide information about Supplier's access, compilation and use of Personal Information, including response to any inquiry (in the context of an investigation or otherwise), for a regulatory authority, or to address any complaint or concerns regarding Personal Information;
- (b) Participate in any regulatory or legal proceedings related to Personal Information; and
- (c) Provide information required by OPUC for privacy impact assessments.

9. **Requests for Access and Correction** Supplier shall direct all requests for access to or correction of Personal Information to OPUC.

10. **Inspection and Audit** OPUC reserves the right to audit and verify, both physically and electronically, Supplier's compliance with the Privacy Requirements. This includes examination of

Supplier's equipment and records and/or interviews with Supplier's personnel, subcontractors and vendors. Supplier shall permit and provide reasonable assistance with such inspections and audits, and shall maintain appropriate data and systems to facilitate such.

11. **Change in Privacy Requirements** Supplier acknowledges that Privacy Law and other privacy requirements to which OPUC is subject to may change at any time. To the extent there are changes that affect the goods and services provided in this Order, Supplier shall accept all reasonable and regulatory imposed amendments to the Privacy Requirements in order for OPUC to maintain compliance.

12. **Security and Location of Personal Information held by Supplier** Unless otherwise agreed to in writing by OPUC, Supplier shall:

(a) Hold Personal Information in a secure physical and electronic environment in the province of Ontario, which meets or exceeds industry standards and best practice related to the protection of Personal Information.

(b) Not permit Personal Information to be accessed by Authorized Personnel outside of Ontario.

(c) Segregate Personal Information from other data held by Supplier.

(d) Ensure all contractors, subcontractors and vendors that are Authorized Personnel, are bound by the same Privacy Requirements as the Supplier.

(e) Keep detailed log records of Supplier's access, compilation and use of Personal Information, including the date and identity of Authorized Personnel. Within twenty-four (24) hours of a request, Supplier shall provide a copy of log records to OPUC for review.

(f) Not withhold any Personal Information from OPUC for any reason whatsoever, including those connected to any dispute with OPUC, or attempts by Supplier to enforce an alleged payment obligation or specific terms of this Order.

13. **Limitation of Access and Use of Personal Information** Supplier shall:

(a) Ensure only persons who require access to Personal Information for the purpose of providing the goods and services in this Order, shall be Authorized Personnel.

(b) Limit the access and use of Personal Information to only that which is required for Authorized Personnel to provide the goods and services of this Order.

(c) Ensure Authorized Personnel are familiar with, and bound by the same Privacy Requirements as the Supplier.

(d) Take reasonable steps, including training, the execution of applicable agreements, implementation of appropriate controls, monitoring and enforcement measures, to ensure Authorized Personnel comply with the Privacy Requirements.

(e) Remove access rights and prohibit Authorized Personnel from accessing Personal Information upon Order completion, work reassignment, or termination of employment or contract with Supplier. Supplier shall ensure the return of all Personal Information in such cases and remind all parties of surviving obligations with respect to the Privacy Requirements.

14. **Return of Personal Information** Upon termination or expiry of this Order, or upon written notice from OPUC, Supplier shall return to OPUC, forthwith and as directed by OPUC, all Personal Information held or stored by Supplier (including any copies thereof) or, at OPUC's sole discretion, Supplier shall destroy all such Personal Information as directed by OPUC (including any copies thereof), and provide OPUC with an officer's certificate attesting to such.

15. **Privacy Requirements Indemnification** Supplier shall indemnify and hold harmless OPUC, its Affiliates, and their representatives (including their officers, employees and agents) from and against any and all claims, demands, suits, losses, damages, fines or judgments (including related expenses and legal fees) that it may incur related to or arising from any non-compliance by Supplier with the Privacy Requirements.

16. **Survival** All rights, obligations and duties hereunder shall survive the expiration or termination of this Order.

Security

17. **Security Control Acknowledgement** Supplier acknowledges the fundamental importance of establishing logical and physical controls in order to maintain the security, integrity and availability of the goods and services provided, and limit unauthorized access, destruction, loss or alteration to, and disclosure of, OPUC's Confidential Information and Personal Information, in all formats including but not limited to electronic and paper formats, in accordance with this Order.

18. **Information Security Policy and Procedures** Supplier shall establish and maintain formal information security policies and procedures that put into effect controls around OPUC's Confidential Information and Personal Information, and the systems that process them, in accordance with Privacy Requirements, industry standards, best practice and any additional requirements specified by OPUC.

19. **Information Security Organization** Supplier shall define roles and responsibilities for the ongoing review of information security safeguards to reasonably ensure its continuing suitability, adequacy and effectiveness, in accordance with Privacy Requirements, industry standards, best practice, any additional requirements specified by OPUC, and changing threats to security.

20. **Asset Management** Supplier shall inventory all data centres, facilities and systems that create, store, process and disseminate OPUC's Confidential Information and Personal Information, and establish ownership and responsibility for the successful operation of security controls for each of those environments. Supplier shall maintain up-to-date network diagrams, process flow charts and interface maps for such, including the identification of any external dependencies, and shall provide copies to OPUC upon request.

21. **Human Resources** Supplier shall establish and maintain controls to ensure that employees, contractors and third party staff are suitably screened and educated on security practices prior to being

given access to OPUC's data and the systems that process that data. Supplier shall ensure all individual access to OPUC's Confidential Information and Personal Information is promptly removed upon work reassignment, termination of employment or termination of contract. At the request of OPUC, Supplier shall provide a list of individuals that have access to any OPUC operational and information technology (*hardware, software and data*) including communication networks, information systems, industrial controls and all programmable electronic devices.

22. **Physical and Environmental Security** Supplier shall establish a security perimeter around the physical work environment and sensitive data processing facilities, and establish physical entry controls to reasonably ensure that only authorized individuals gain access to the environment, and environmental controls to protect against damage from fire, flood, and other forms of man-made or natural disasters affecting the Supplier's facility.

23. **Communication and Operations Management** Supplier shall establish controls and procedures for the secure operation of systems and networks facilitating access to OPUC's Confidential Information and Personal Information in order to reasonably prevent accidental or deliberate misuse and disclosure. Such controls shall include, but are not limited to, capacity planning, change management, least privileges granted, segregation of duties, separation of production environment from development/test environments, backups, network security, the encryption of data in transit, and restricting the use of removable media.

24. **Access Controls** Supplier shall establish controls and procedures for the authorization, regular review and revocation of access at all levels of the system environment including physical access, network access, operating systems, applications and database access. Supplier shall maintain suitable authentication controls to reasonably ensure that an individual's access rights to OPUC's Confidential Information and Personal Information is appropriate for the individual's role, regardless of how that individual is attempting to access the information or the location from which access is being attempted.

25. **Information Systems Acquisition, Development and Maintenance** Supplier shall maintain an application development and maintenance framework that protects the integrity of the production application and associated source code from unauthorized and untested modifications. Such a framework shall establish control over OPUC's Confidential Information and Personal Information, across all environments within the development lifecycle of systems.

26. **Incident Management** Supplier shall establish policies and procedures for the timely communication and investigation of suspected breaches in the security of OPUC's Confidential Information and Personal Information. At a minimum, communication, and authorization to disclose such incidents to OPUC must take place prior to any discussion and disclosure with regulators, clients, outside law enforcement agencies or representatives of the media. Incident investigations and associated information handling shall be performed in accordance with all applicable law.

27. **Business Continuity and Disaster Recovery Management** Supplier shall establish appropriate policies, procedures, systems and contingencies to ensure continued provision of goods and services in accordance with this Order. Backups of OPUC Confidential Information and Personal Information shall be conducted, maintained, and tested periodically.

28. **Security Compliance** Supplier shall establish policies and procedures to ensure that the design, operation and management of systems processing OPUC's Confidential Information and Personal

Information comply with the Privacy Requirements, industry standards, best practice, any additional requirements specified by OPUC, changing threats to security, and all other applicable laws.

29. **Data Destruction and Disposal** Supplier shall implement processes and controls to ensure that any storage media or data is disposed or destroyed securely in accordance with the Privacy Requirements, industry standards, best practice, and any additional requirements specified by OPUC. OPUC shall reserve the right to obtain destruction certificates from Supplier upon request.

30. **Systems Monitoring and Auditing** Supplier shall maintain wherever possible monitoring and auditing capabilities of systems such that an audit trail of activities by staff or automated processes can be reviewed. Supplier shall make available upon OPUC's request, any reports related to such within twenty-four (24) hours.

31. **Supply Chain Management** Supplier in consultation with OPUC, shall identify, prioritize and assess the critical information systems, components, and services required for the purpose of providing the goods and services in this Order.

32. **Integrity Controls** Supplier shall establish controls, procedures, and designs to ensure network integrity is protected, incorporating network segregation where appropriate.

33. **Security Testing and Reviews** Supplier shall conduct at a minimum, annual reviews of its security systems and controls, including where applicable, penetration testing, intrusion detection and malware alerts. The results of such reviews shall be shared with OPUC upon request.

34. **Verification and Audit of Security Compliance** Supplier represents and warrants that it maintains adequate internal audit functions to assess internal controls in its environment, and to protect the security and confidentiality of OPUC's Confidential Information and Personal Information which it may access, compile or use to provide the goods and services in this Order. Supplier shall make available upon OPUC's request, any reports related to such within twenty-four (24) hours.

Furthermore, Supplier shall permit OPUC and its contractors or agents to perform, at OPUC's expense, periodic external vulnerability audits and testing, including penetration testing and payment vulnerability scans of the goods and services provided in this Order. OPUC shall provide Supplier a minimum of five (5) days notice prior to commencing any such audits or testing. OPUC shall limit such audits or testing to no more than once per quarter, unless there is a material change in the goods and services provided in this Order. OPUC shall notify Supplier if a security vulnerability is uncovered during such audit and testing, and upon receipt of notification, Supplier shall prepare an action plan to appropriately address the vulnerability forthwith, and inform OPUC of such plan.

35. **Security Warranty** Supplier represents and warrants that goods and services including any software, related documentation, updates furnished hereunder and the media it is delivered on, or any "Software as a Service" or "Cloud" service, have been scanned for viruses and other malicious code and have been found to be free from viruses and malicious code; and that the goods and services do not (a) grant access to servers, systems or programs of OPUC, its Affiliates or Representatives by person(s) other than OPUC, its Affiliates or Representatives or (b) contain any program, routine, code, device or other undisclosed feature including but not limited to a time bomb, virus, software lock, Trojan horse, worm or trap door ("Disabling Feature") that is designed to delete, disable or interfere with the goods and services, and if any Disabling Feature is discovered or reasonably suspected to be present,

Supplier shall immediately notify OPUC and, at its sole expense, delete such Disabling Feature and carry out the recovery necessary to remedy its impact.

36. Technical Support Requirements for software, firmware and chipsets For goods provided in this Order that involve software, firmware or chipsets, Supplier shall:

(a) Implement appropriate standards, processes and methods to prevent, identify, evaluate and repair any vulnerabilities, malicious code, and security incidents in such goods which shall be consistent with industry standards and best practice

(b) Continue to support and provide services to repair, update, upgrade and maintain such goods including the provision of patches to OPUC remedying vulnerabilities for the reasonable lifetime of such goods

(c) Supplier shall provide to OPUC a bill of materials identifying all third-party software components contained in such goods. Third-party software shall be up-to-date at the time of delivery to OPUC

(d) Supplier shall grant to OPUC the right, but OPUC shall not be obliged, to test or have tested such goods for malicious code and vulnerabilities at any time, and shall adequately support OPUCN

(e) Supplier shall provide OPUC a contact for all information security related issues, to be available during normal business hours. Contact must respond to OPUC inquiries within twenty-four (24) hours.

37. Minimum Service Level Requirements Unless otherwise agreed to in writing by OPUC, Supplier shall ensure all goods and services considered critical to OPUC business functions, and for which OPUC requires on-going support from Supplier, shall be supported in accordance with the following minimum service level requirements:

Severity of Issue	Definition	Minimum Response Time
Level 1 – Critical	Complete failure of a platform or system, including but not limited to complete inability to access or use such.	1 hour
Level 2 – High	Essential functionalities are disrupted	2 hours
Level 3 – Medium	Partial or limited loss of functionality	4 hours
Level 4 – Low	Inconvenience but not impacting performance	24 hours

Furthermore, Supplier shall ensure that service level response times are sufficient to maintain a monthly service availability of 99.9% for all such goods and services provided.

