Data Privacy and Security Addendum

This Data Privacy and Security Addendum ("DPSA") governs the processing, protection, and security of AltaGas Data in connection with the services provided under the applicable Agreement entered into by you (hereinafter referred to as "Service Provider") and an AltaGas Related Party ("AltaGas"). "AltaGas Related Party" means AltaGas and its affiliates, and each of their respective directors, officers, employees, contractors (other than Service Provider and its subsidiaries, affiliates, subcontractors, licensors, consultants, advisors, insurers, agents and representatives. Such subsidiaries, affiliates, subcontractors, suppliers, vendors, licensors, consultants, advisors, insurers, agents and representatives are, collectively, the "Service Provider Related Parties."

1. Purpose. This DPSA articulates the accountability of Service Provider and the Service Provider Related Parties for data protection and information security for AltaGas Data that is transmitted, accessed, processed, stored, hosted, or is otherwise accessible by Service Provider and/or Service Provider Related Parties, as well as for the use of, and access to, AltaGas Information Technology Systems, whereby "Information Technology Systems" are defined as systems including but not limited to hardware, software, applications, computers, mobile devices, networks, access points, servers, and databases. The obligations set out in this DPSA are in addition to, and shall not limit, any of Service Provider's obligations contained in the Agreement. Capitalized terms not defined in this DPSA shall have the meaning set forth in the body of the Agreement. In the event of any conflict between the terms of the Agreement and those of this DPSA, the terms of this DPSA shall control.

   For the purposes of this DPSA, "AltaGas Data" means: (1) all AltaGas personal information, as that term is generally defined in Applicable Privacy Laws (defined as all privacy and data protection laws and regulations in the countries, states, and/or territories where any AltaGas personnel are employed and/or resident"); (2) any and all information relating to AltaGas or its business or operations (including, for the avoidance of doubt, Critical Energy Infrastructure Information (as such term is defined in 18 C.F.R. § 388.113 (which may be amended or recodified)), AltaGas affiliate entities, customers, end users, AltaGas personnel, or AltaGas service providers or suppliers; (3) all data that are disclosed by or on behalf of AltaGas, its affiliates, customers, end users, AltaGas personnel, AltaGas service providers, or AltaGas suppliers, and which is accessed, processed, or hosted by Service Provider and/or Service Provider Related Parties; and (4) all data that are created by Service Provider-provided deliverables or services that: (a) were provided, collected or generated as part of the use or operation of the deliverables or the provision or receipt of the services or in order to comply with any applicable law; or (b) otherwise became known to either party (or, in the case of Service Provider Service Provider Related Parties) as a result of any actions under or in respect of the Agreement.

2. Standards. Service Provider uses reasonable and appropriate methods and safeguards to protect the confidentiality, availability and integrity of AltaGas Data in accordance with Service Provider's document security policies and procedures. Service Provider will provide to AltaGas its information security policies and procedures upon written request.

   Service Provider's information security practices have been designed to leverage best practices for securing AltaGas Data and meet the requirements identified in the ISO 27001 and ISO 27017 standards, the NIST CSF standards or such other data security standards as AltaGas may reasonably request.

3. Access to AltaGas Information Technology Systems. In addition to any requirements set forth herein, Service Provider responsibilities with respect to access to AltaGas systems include, but are not limited to:

   3.1. If AltaGas provides a computer or other device, including, but not limited to smart-phones, tablets, tough-books, and desktop/laptop computers to the Service Provider, Service Provider will use such equipment provided and any AltaGas network connections solely for purposes of providing services under the Agreement, including connection to AltaGas's computer system for delivering and receiving information

related to work under the Agreement. Service Provider is responsible for providing its own internet access.

3.2. Any or all uses of AltaGas's computer system and all files on AltaGas's computer system may be monitored, recorded, copied, audited, inspected, and disclosed to authorized AltaGas personnel, law enforcement personnel, as well as authorized officials of other agencies, both domestic and foreign. By using any AltaGas system, Service Provider and its employees' consent to such monitoring, recording, copying, auditing, inspection, and disclosure at the discretion of authorized AltaGas personnel. Users of AltaGas's computer system understand that they have no explicit or implicit expectation of privacy.

4. Information Security Infrastructure.

4.1. Access Controls for Service Provider Personnel.

(a) Access Policy. Service Provider has in place, complies with, and enforces an access control policy (physical, technical and administrative) based on least privileges principles.

(i) Service Provider restricts access to AltaGas Data solely to Service Provider personnel (including, as may be applicable, Service Provider Related Parties' personnel) who have a need to access the AltaGas Data in connection with the Services or as otherwise required by applicable law.

(b) Access to AltaGas Data will be restricted as required by applicable law for AltaGas or the AltaGas Related Party that has entered into the Agreement.

4.2. Authentication. Service Provider uses industry standard practices, including multi-factor authentication (MFA), to identify and authenticate all Service Provider Personnel who attempt to access Service Provider network or information systems.

4.3. Encryption. Service Provider encrypts AltaGas Data at rest within the Services using ciphers at least as strong as 256-bit AES or any higher standard which is an industry best practice for the Services. AltaGas Data in transit to and from the Services is transferred to/from the Services across encrypted network connections and/or protocols (*i.e.*, HTTPS and/or VPN). If backups are permitted under the Agreement, backups of AltaGas Data are encrypted and stored in a secondary data center or hosted location. Service Provider will ensure that encryption keys used to protect AltaGas Data and communications related to AltaGas are securely protected against unauthorized access, separation of duties exists, and the keys are recoverable. Key backup and recoverability must be established and tested to ensure continued access to data keys.

4.4. Data Minimization. Service Provider shall ensure that the collection, use, and retention of AltaGas Data is limited to what is necessary for the purposes identified in the Agreement. Service Provider will collect only the necessary data, use it solely for agreed purposes, retain it only as long as needed or legally required, and then securely delete or anonymize it as per the direction of AltaGas. Service Provider shall provide written confirmation of such deletion or anonymization to AltaGas upon request.

4.5. Asset Inventory. Service Provider maintains and tracks inventories and locations of all computing equipment and media used in connection with the processing and handling of AltaGas Data. Access to such inventories is restricted to authorized Service Provider Personnel. All destruction of assets is completed in accordance with best practices for data removal and destruction.

4.6. Network and Host Security.

(a) Network Security. Service Provider uses a security information and event management (SIEM) system and maintains firewalls and other control measures (e.g., security appliances, network segmentation) to cause access from and to its networks to be appropriately controlled. Logs from hosts that process

or access AltaGas information are centrally collected and monitored through the Service Provider's SIEM.

(b) Security Updates and Endpoint Protection. The Service Provider Systems and applications that are associated with or that process or handle AltaGas Data are patched and otherwise secured to mitigate the likelihood and impact of security vulnerabilities in accordance with Service Provider patch management processes and within a reasonable time after Service Provider has actual or constructive knowledge of any critical or high-risk security vulnerabilities. Service Provider shall deploy and maintain endpoint detection and response (EDR) or extended detection and response (XDR) capabilities on endpoints that access, process, or store AltaGas Data, configured to detect, investigate, and respond to malicious activity.

(c) Malicious Software. Service Provider will ensure that detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures are implemented. Where the use of mobile code is authorized, the configuration must ensure that the authorized mobile code operates according to a clearly defined security policy, and unauthorized mobile code is prevented from executing and adversely affecting the confidentiality, integrity or availability of AltaGas Data and Services.

4.7. Physical Security. If Service Provider will be hosting AltaGas Data:

(a) Service Provider restricts the geographic location of any facility hosting, or computer equipment accessing, AltaGas Data as required by applicable law for AltaGas or the AltaGas Related Party that has entered into the Agreement.

(b) Service Provider maintains physical security safeguards at any facilities where Service Provider hosts AltaGas Data. Physical access to such facilities is only granted following a formal authorization procedure and access rights are reviewed periodically.

(b) Such facilities are rated as Tier 3 data centers or greater, and access to such facilities must be limited to identified and authorized individuals. Such facilities use a variety of industry standard systems to protect against loss of data due to power supply failure, fire and other natural hazards.

(c) Service Provider will ensure that security perimeters (barriers such as walls, card-controlled entry gates or staffed reception desks) are used to protect areas that contain AltaGas Data, Information and information processing facilities.

4.8. Backups. If Service Provider will be hosting AltaGas Data, Service Provider provides 24/7/365 managed backup services that include AltaGas Data stored in the primary site backed up on at least a daily basis to a secondary site (the geographic location of the secondary or other back-up site is restricted as required by applicable law for AltaGas or the AltaGas Related Party that has entered into the Agreement). Service Provider provides backup services for all components of the solution included in the Services. Backups are maintained for a period of ninety (90) days in the primary data center, and ninety (90) days in the secondary data center.

4.9. Data Management. Service Provider maintains reasonable controls for information governance and data management in connection with the Services. Service Provider destroys, deletes, or otherwise makes irrecoverable AltaGas Data upon the disposal or repurposing of storage media. If Service Provider is hosting AltaGas Data, Service Provider will ensure that the AltaGas Data and the Service Provider Information Technology Systems on which AltaGas Data is stored are at all times physically and logically separated from data hosted for other customers of Service Provider.

5. Independent Assessments. On an annual basis and further subject to the other requirements set out in the Agreement, Service Provider will cause an independent third-party organization conduct a SOC2 Type 2 or equivalent independent assessment of the standards set forth in this DPSA, and will provide a copy of the

assessment to AltaGas within thirty (30) days of receipt. Any such assessment must be provided with an unqualified opinion. Additionally, Service Provider undergoes penetration testing, conducted by an independent third-party organization, on an annual basis. Service Provider will provide documentation on performed internal assessments and penetration to AltaGas upon request.

6. Business Continuity and Disaster Recovery. Service Provider will maintain, test, and comply with documented business continuity and disaster recovery ("BCDR") plans that will be provided to AltaGas upon request. The BCDR plans should specify how often the plans are reviewed and tested and how testing is conducted (informal vs. formal/tabletop vs. full exercise). BCDR plans must outline the jurisdiction(s) in which Service Provider maintains BCDR facilities and where AltaGas Data may be stored during a BCDR situation. Service Provider will: (i) provide notice of BCDR testing that may impact the Services or AltaGas Data in advance; (ii) provide summary results of any BCDR testing including any corrective action plans to address any deficiencies; and (iii) correct any deficiencies uncovered during such testing within a reasonable timeframe commensurate with the materiality of the deficiency.

7. Remote Work / Work from Home. Service Provider will comply with industry standard controls and AltaGas policies with respect to any work-from-home or provision of Services from a location other than Service Provider's or AltaGas's facilities.

8. Security Incident Management.

   8.1. Notice. Service Provider will notify AltaGas of any potential breach of security of or relating to Service Provider Information Technology Systems that may lead to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to AltaGas Data (a "Security Incident") without undue delay after becoming aware of the Security Incident [and, in any event, within 24 hours of becoming aware of such Security Incident.] Service Provider will provide such notice (including a brief description of the Security Incident and its potential impact on AltaGas Data) to the following contacts:

   (a) Via email to cyber-report@altagas.ca and cyber-report@washgas.com

   (b) Via phone to the AltaGas IT service desk at 1-855-362-8317 - **DO NOT simply leave voicemail or send email - please ensure you reach an employee, because it is CRITICAL that AltaGas begins response procedures immediately**.

   8.2. Communication. Notwithstanding Section 8.1, Service Provider shall notify AltaGas of any Security Incident prior to issuing or filing any public communication, notice, press release or report (collectively, "Security Incident Communications") and shall, to the extent reasonably practicable in the circumstances, consult with AltaGas on the content of such Security Incident Communications; *provided, however,* that if Service Provider is required by law to issue such Security Incident Communications pursuant to applicable law ("Mandated Communications"), Service Provider shall only be required to make such good faith efforts to notify and consult with AltaGas on the content of such Mandated Communications as are reasonable in the circumstances.

   8.3. Updates and Cooperation. Service Provider will cooperate with AltaGas's reasonable requests for information regarding any such Security Incident, and Service Provider will provide regular updates on the Security Incident and the investigative action and corrective action taken. Service Provider's obligation to report or respond to a Security Incident is not an acknowledgement by Service Provider of any fault or liability with respect to the Security Incident. Service Provider acknowledges that Security Incidents affecting other Customers in a virtualized environment may affect AltaGas, and Service Provider shall inform AltaGas of other security events while respecting other Customers' privacy.

8.4. Remediation. In the event of a Security Incident, Service Provider will, at its own expense: (i) investigate the Security Incident; (ii) provide AltaGas with a remediation plan to address the Security Incident and to mitigate the incident and reasonably prevent any further incidents; (iii) remediate the effects of the Security Incident in accordance with such remediation plan and take other steps as required to mitigate the effects of the Security Incident; (iv) reasonably cooperate with AltaGas and provide commercially reasonable assistance to help AltaGas comply with such applicable law, including by providing AltaGas with notice and other information (including, but not limited to, sharing Security Incident investigation related information and audit logs), as available, related to the Security Incident as may be required by applicable law; and (v) cooperate with any law enforcement or regulatory official investigating such Security Incident.

8.5. Indemnity. Notwithstanding anything to the contrary in the Agreement, including any other indemnity provisions or limitation of liability provisions, and regardless of any conflict hierarchy contained in the Agreement, all of which the parties agree shall be subordinate to this Section 8.5, Service Provider will indemnify, defend, and hold AltaGas, its subsidiaries, affiliates, and their respective officers, directors, employees, agents, successors and permitted assigns (the "AltaGas Indemnitees") harmless from the following, all of which shall be deemed direct damages: all losses, damages, liabilities, deficiencies, actions, judgments, interest, awards, penalties, fines, costs or expenses of whatever kind, including reasonable attorneys' fees, the cost of enforcing any right to indemnification hereunder and the cost of pursuing any insurance providers, arising out of or resulting from any third party claim against any AltaGas Indemnitee arising out of or resulting from Service Provider's failure to comply with any of its obligations under this DPSA, including but not limited to AltaGas's documented internal and external costs associated with investigating, addressing and responding to the Security Incident, including:

(a) preparation and mailing or other transmission of notifications or other communications to consumers, employees or others as AltaGas deems reasonably appropriate;
(b) establishment of a call center or other communications procedures in response to such Security Incident (e.g., AltaGas service FAQs, talking points and training);
(c) public relations and other similar crisis management services;
(d) legal, consulting and accounting fees and expenses associated with AltaGas's investigation of and response to such Security Incident;
(e) any government fines or penalties; and
(f) costs for commercially reasonable credit reporting and monitoring services that are associated with legally required notifications or are advisable under the circumstances.

9. Liability. Any limitations of liability or damages contained in the Agreement will not apply to any Security Incident or breach of this DPSA, nor to Service Provider's indemnification obligations contained in this DPSA.