Data Protection Attachment

The Parties agree to the following provisions in connection with any Company Data stored or hosted by or on behalf of Contractor in connection with the Contract between Company and Contractor to which this Attachment is attached or incorporated by reference. Unless otherwise indicated herein, capitalized terms used in this Attachment without definition shall have the respective meanings specified in the Contract. To the extent there is a conflict between the terms of this Attachment and the terms of the Contract, this Attachment shall control. The obligations set forth herein form an integral part of the Contract.

I. Definitions

a. "Company Data" shall mean all data supplied by or on behalf of Company in connection with the Contract, excluding any confidential information of Contractor.

b. "Data Breach" shall mean the unauthorized access by an unauthorized person that results in the use, disclosure or theft of Company Data.

c. "Non-Public Data" shall mean Company Data, other than Personal Data, that is non-public, proprietary or confidential. Non-Public Data includes any data deemed confidential pursuant to the Contract, otherwise identified by Company as Non-Public Data, or that a reasonable person would deem confidential.

d. "Personal Data" shall mean Company Data that (1) relates to an individual person; and (2) identifies or can be used to identify, locate, or contact that individual alone or when combined with other personal or identifying information that is or can be associated with that specific individual;

e. "Security Incident" shall mean the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with the hosted environment used to perform the services.

II. Company Data

a. Company will be responsible for the accuracy and completeness of all Company Data provided to Contractor by Company. Company shall retain exclusive ownership of all Company Data. Contractor shall restrict access to Company Data to their employees with a need to know (and advise such employees of the confidentiality and non-disclosure obligations assumed herein).

b. Upon reasonable notice, Company shall have reasonable access to Company Data in the possession of Contractor. At no time shall such files be withheld from Company or otherwise disguised or encoded in a manner inconsistent with the purpose and intent of providing full and complete Company access. After termination of the Contract, Company Data in the possession of Contractor shall, (1) at Company's request within ten (10) business days of termination, be returned to Company in a reasonable format as mutually agreed to between the parties within ten (10) business days of receiving such request, and (2) be destroyed within thirty (30) days by Contractor, and Contractor shall provide Company with written certification signed by an authorized representation of such return or destruction.

c. Contractor shall promptly notify the Company upon receipt of any requests from unauthorized third parties which in any way might reasonably require access to Company

Data or Company's use of the hosted environment. Contractor shall notify the Company by the fastest means available and also in writing pursuant to Contract notice provisions and the notice provision herein. Except to the extent required by law, Contractor shall not respond to subpoenas, service or process, and other legal request related to Company without first notifying the Company and obtaining the Company's prior approval, which shall not be unreasonably withheld, of Contractor's proposed responses. Contractor agrees to provide its completed responses to the Company with adequate time for Company review, revision and approval.

III. Data Security

a. Contractor will use commercially reasonable efforts, consistent with industry standards, to provide security for the hosted environment and Company Data and to protect against unauthorized access to the hosting environment. Contractor shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of Personal Data and Non-Public Data. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the Contractor applies to its own personal data and non-public data of similar kind.

b. Contractor shall implement and maintain a written information security program including appropriate policies, procedures, and risk assessments that are reviewed at least annually. At a minimum, Contractor's safeguards for the protection of Company Data shall include: (i) limiting access of Company Data to authorized persons; (ii) securing business facilities, data centers, paper files, servers, backup systems, and computing equipment, including, but not limited to, all mobile devices and other equipment with information storage capability; (iii) implementing network, application, database, and platform security; (iv) securing information transmission, storage, and disposal; (v) implementing authentication and access controls within media, applications, operating systems, and equipment, including the use of multifactor authentication for access to any Company Data; (vi) encrypting Company Data stored on any media; (vii) encrypting Company Data when transmitted; (viii) strictly segregating Company Data from information of Contractor or its other Companies so that Company Data is not commingled with any other types of information; (ix) conducting risk assessments, penetration testing, and vulnerability scans and promptly implementing, at Contractor's sole cost and expense, a corrective action plan to correct any issues that are reported as a result of the testing; (x) implementing appropriate personnel security and integrity procedures and practices, including, but not limited to, conducting background checks consistent with applicable law; and (xi) providing appropriate privacy and information security training to Contractor's employees.

c. Contractor represents and warrants to the Company that the hosting equipment and environment will be routinely checked with a commercially available, industry standard software application with up-to-date virus definitions. Contractor will regularly update the virus definitions to ensure that the definitions are as up-to-date as is commercially reasonable. Contractor will promptly purge all viruses discovered during virus checks. If there is a reasonable basis to believe that a virus may have been transmitted to Company by Contractor, Contractor will promptly notify Company of such possibility in a writing that states the nature of the virus, the date on which transmission may have occurred, and the means Contractor has used to remediate the virus.

d. Contractor shall provide its services to Company and its users solely from data centers in the U.S. Storage of Company Data at rest shall be located solely in data centers in the U.S.

Contractor shall not allow its personnel or contractors to store Company Data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. Contractor shall permit its personnel and contractors to access Company Data remotely only as required to fulfill Contractor's obligations under the Contract.

e. Contractor shall allow the Company to audit conformance to the Contract terms. The Company may perform this audit or contract with a third party at its discretion and at Company's expense.

f. Contractor shall perform an independent audit of its data centers at least annually at its expense, and provide a redacted version of the audit report upon request. Contractor may remove its proprietary information from the redacted version. A Service Organization Control (SOC) 2 audit report or approved equivalent sets the minimum level of a third-party audit.

g. Any remedies provided in this Attachment are not exclusive and are in addition to other rights and remedies available under the terms of the Contract, at law or in equity.

IV. Security Incident or Data Breach Notification: Contractor shall inform Company of any Security Incident or Data Breach.

a. Contractor may need to communicate with outside parties regarding a Security Incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the Contract. If a Security Incident involves Company Data, Contractor will coordinate with Company prior to any such communication.

b. Contractor shall report a Security Incident to the Company identified contact set forth in the Contract and herein within five (5) days of discovery of the Security Incident or within a shorter notice period required by applicable law or regulation.

c. Contractor shall: (I) maintain processes and procedures to identify, respond to and analyze Security Incidents; (ii) make summary information regarding such procedures available to Company at Company's request, (iii) mitigate, to the extent practicable, harmful effects of Security Incidents that are known to Contractor; and (iv) document all Security Incidents and their outcomes.

d. If Contractor has reasonable belief or actual knowledge of a Data Breach, Contractor shall (1) promptly notify the appropriate Company identified contact set forth herein within 48 hours or sooner, unless shorter time is required by applicable law, and (2) take commercially reasonable measures to address the Data Breach in a timely manner.

V. Breach Responsibilities: This section only applies when a Data Breach occurs with respect to Personal Data within the possession or control of Contractor.

a. Contractor, unless stipulated otherwise, shall promptly notify the Company identified contact within 24 hours or sooner, unless shorter time is required by applicable law, if it confirms that there is, or reasonably believes that there has been a Data Breach. Contractor shall (1) cooperate with Company as reasonably requested by Company to investigate and resolve the Data Breach, (2) promptly implement necessary remedial measures, if necessary, and (3) document responsive actions taken related to the Data

Breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.

b. Unless otherwise stipulated, if a Data Breach is a direct result of Contractor's breach of its obligation to encrypt Personal Data or otherwise prevent its release, Contractor shall bear the costs associated with (1) the investigation and resolution of the Data Breach; (2) notifications to individuals, regulators or others required by applicable law; (3) credit monitoring services required by applicable law; (4) a website or toll-free numbers and call center for affected individuals required by applicable law; and (5) complete all corrective actions as reasonably determined by Contractor based on root cause.

c. If a Data Breach is a direct result of Contractor's breach of its obligations to encrypt Personal Data and Non-Public Data or otherwise prevent its release, Contractor shall indemnify and hold harmless Company, including Company's directors, employees, officers, agents, affiliates and subsidiaries, against all penalties assessed to Indemnified Parties by governmental authorities in connection with the Data Breach.

VI. **Notice:** In addition to notice requirements under the terms of the Contract, notifications in connection with data protection should also be sent to: cybersecurity@williams.com.