**ICW GROUP INFORMATION SECURITY REQUIREMENTS ADDENDUM TO AGREEMENT**

1. **Information Security Practices**: Service Provider will use documented commercially reasonable, industry standard information security practices and comply with all applicable laws, rules, regulations (e.g., 23 NYCCR 500 et seq., California Civil Code § 1798.80 et seq.) and reasonable policies and procedures of ICW to protect ICW data in Service Provider's possession, control or custody and the systems and servers used to collect, store, access, use, process, transmit or maintain such data in Service Provider's possession, control or custody from unauthorized access, destruction, use, modification, or disclosure. Such practices will include, but not be limited to, (a) current industry standard enterprise virus protection for servers and systems which collect, store, access, use, process, transmit or maintain any ICW data disclosed under the Agreement, (b) intrusion detection and countermeasures to detect and terminate unauthorized access and/or activity to such servers and systems, (c) firewalls to regulate the transmission of data entering the servers and systems from any external source and to enforce secure connections with other systems, and (d) monitoring and maintenance of access logs for such servers and systems. Service Provider will provide adequate physical security of all premises in which ICW data disclosed to it will be processed or stored, including reasonable surveillance monitoring and recording, limited access controls, and fire suppression and environmental control systems. Service Provider will correct any critical, high risk, or significant issues identified by ICW in Service Provider's information security practices within 5 business days. Service Provider will correct all other material issues identified by ICW within 10 business days.
2. **Due Diligence and Ongoing Assessment Process**: Service Provider will cooperate with ICW in its reasonable and appropriate due diligence and ongoing assessment processes used to evaluate the adequacy of Service Provider's information security practices and Service Provider's compliance with this Addendum. This includes, at least once every 12 months, providing Service Provider's incident response plan, policies and procedures, audit reports (e.g. SSAE 18, PCI-DSS), internal or third-party security assessments (e.g., penetration testing, vulnerability scans), and information and documentation related to Service Provider's information security practices in response to ICW's questionnaires within 5 business days of request. ICW may also perform reasonable annual video conference, or with approval from Service Provider annual onsite reviews of Service Provider to evaluate the continued adequacy of Service Provider's information security practices. Reviews will be subject to the reasonable supervision of Service Provider, will aim to minimize impact on Service Provider's business operations, and will be performed at mutually agreed upon times.
3. **Multi-Factor Authentication**: Service Provider will use effective access controls, which may include multi-factor authentication or risk based authentication, to protect against the unauthorized access to ICW data and the servers and systems used to collect, store, access, use, process, transmit or maintain such data in Service Provider's possession, control or custody. Multi-factor authentication must be used for any individual accessing ICW's internal network from an external network, unless ICW's Director of Information Security or designee has approved in writing the use of reasonably equivalent or more secure access controls.
4. **Encryption**: Service Provider will implement and maintain controls, including encryption with a minimum standard of 256-bit encryption, to protect ICW data both in transit over external networks and at rest. Service Provider may use effective alternative compensating controls for encryption only if reviewed and approved in writing by ICW's Director of Information Security or designee.
5. **Incident Response**: Service Provider will provide written notice to ICW's General Counsel, which must be received within 24 hours of any information security event directly impacting ICW's data in Service Provider's possession, control or custody or the servers and systems used to collect, store, access, use, process, transmit or maintain such data in Service Provider's possession, control or custody (by email to legal@icwgroup.com and overnight mail to Insurance Company of the West, Attn: General Counsel, 15025 Innovation Drive, San Diego, CA 92128). Information security event means any actual unauthorized access to, disclosure or use of ICW data in Service Provider's possession, control or custody or the servers or systems used to collect, store, access, use, process, transmit or maintain such data in Service Provider's possession, control or custody, or as otherwise defined by applicable law, rule, or regulation. Service Provider will cooperate with ICW, and at Service Provider's own expense, take all immediate and reasonable actions necessary to secure ICW data and such servers and systems in the event of an information security event. Unless otherwise required by law, Service Provider shall not notify any third parties of the involvement of ICW's data in the information security event without ICW's prior permission. In the event that Service Provider is required to report an information security event to any governmental or regulatory agency, whether under any federal, state or local law, including, but not limited to, any applicable privacy laws, Service Provider agrees to report the information security event to ICW concurrently with Service Provider's reporting of the information security event to the appropriate governmental or regulatory agency. Upon written request, Service Provider shall provide ICW with a written summary report of its investigation and remediation activities. Such report shall include: (i) the steps taken to investigate and mitigate the effects of the information security event, (ii) the nature of the information security event, and (iii) a description of the data accessed, used or disclosed. Any investigation and remediation activities undertaken by Service Provider associated with an information security event

shall be in accordance with applicable laws, regulations, industry standards and best practices. If under applicable laws or regulations it is necessary to inform any affected individual of an information security event involving their personal information, sensitive information or personally identifiable information (PII), Service Provider agrees to be responsible for the reasonable costs associated with such notification, including the provision of any required credit monitoring, to affected individuals. An "information security event" does not and shall not include 'pings', port scans, or similar exploratory contacts which do not result in unauthorized access to, disruption, disclosure, or use of personal information or the servers and systems under Service Provider's possession, custody or control.

6. **Data Management**: Except with the written consent of ICW's Director of Information Security or designee, Service Provider will not (a) host ICW data except in a single-tenant environment, (b) comingle ICW's data with data of other parties; or (c) host, store, transfer or use ICW data outside of the United States.
7. **Third Party Contractors:** ICW's data and the servers and systems used to collect, store, access, use, process, transmit or maintain such data in Service Provider's possession, control or custody may not be accessed or held by third party contractors (including, but not limited to subcontractors, and any software-as-a-service (SaaS) or cloud service providers) without the prior written consent of ICW's Director of Information Security or designee. Service Provider will be wholly responsible to ICW for any obligations or liabilities arising from the acts or omissions of its third party contractors. The requirements in this Addendum will apply to third party contractors as they apply to Service Provider. Service Provider will ensure that its third party contractors supply applicable assessment documentation (e.g. SSAE 18 SOC, PCI-DSS, ISO) at least once every 12 months, and will promptly provide to ICW documentation reasonably necessary to demonstrate such third party contractors' compliance with this Addendum upon request. Service Provider will ensure that all security-related obligations it owns as part of a shared security model with its third party contractors are clearly defined, complied with, and reviewed at least annually.
8. **CCPA**:
    a. Definitions. The following definitions and rules of interpretation apply in this Addendum:
        i. **Agreement** means the documentation, including but not limited to purchase order terms and conditions, governing the agreement between the Service Provider and ICW with respect to the Contracted Business Purpose. The Agreement includes this Addendum.
        ii. **CCPA** means collectively the California Consumer Privacy Act of 2018, as amended (Cal. Civ. Code §§ 1798.100 to 1798.199), and any related regulations or guidance provided by the California Attorney General, the California Privacy Protection Agency, or any other regulatory body with appropriate authority. Terms defined in the CCPA, including, but not limited to personal information, sale and collect, carry the same meaning in this Addendum.
        iii. **Contracted Business Purposes** means the purpose described in the Agreement related to specific goods and/or services for which Service Provider receives or accesses personal information from or on behalf of ICW.
        iv. **ICW** means collectively the applicable ICW Group entity that enters into the Agreement with Service Provider for the Contracted Business Purpose and such ICW Group entity's affiliated companies.
        v. **Service Provider** means the provider of goods and/or services to ICW that is identified in the Agreement.
    b. Service Provider's CCPA Obligations
        i. Service Provider and its contractor(s), if applicable, will only use, retain, or disclose personal information it Collects pursuant to the Agreement for the Contracted Business Purpose or as otherwise permitted by the CCPA.
        ii. Service Provider and its contractor(s), if applicable, will not use, retain, disclose, sell, or otherwise make available personal information it Collects pursuant to the Agreement for Service Provider's own commercial purposes or in a way that does not comply with the CCPA. If a law requires the Service Provider or its contractor to disclose personal information for a purpose unrelated to the Contracted Business Purpose or as otherwise permitted by the CCPA, the Service Provider must first inform ICW of the legal requirement and give ICW an opportunity to object or challenge the requirement, unless the law prohibits such notice.
        iii. Service Provider and its contractor(s), if applicable, will not retain, use, or disclose the personal information that it Collects pursuant to the Agreement outside the direct business relationship between the Service Provider and ICW, unless expressly permitted by the CCPA. For example, Service Provider and its contractor(s) are prohibited from combining or updating personal information that it Collected pursuant to the Agreement with personal information that it received from another source or Collected from its own interaction with the consumer, unless expressly permitted by the CCPA.
        iv. Service Provider and its contractor(s), if applicable, will limit personal information collection, use, retention, and disclosure to activities reasonably necessary and proportionate to achieve the Contracted Business Purposes or as otherwise permitted by the CCPA.

v. Service Provider and its contractor(s), if applicable, must promptly comply with any ICW request or instruction requiring the Service Provider to provide, amend, transfer, or delete the personal information, or to stop, mitigate, or remedy any unauthorized processing.

vi. If the Contracted Business Purposes require the collection of personal information from individuals on ICW's behalf, Service Provider shall not sell or share such personal information it Collects pursuant to the Agreement and will always provide a CCPA-compliant notice addressing use and collection methods that ICW specifically pre-approves in writing. Service Provider will not modify or alter the notice in any way without ICW's prior written consent.

c. Assistance with ICW's CCPA Obligations

i. Service Provider will reasonably cooperate and assist ICW with meeting ICW's CCPA compliance obligations and responding to CCPA-related inquiries, including responding to verifiable consumer requests, taking into account the nature of the Service Provider's processing and the information available to the Service Provider.

ii. Service Provider must notify ICW immediately if it receives any complaint, notice, or communication that directly or indirectly relates either party's compliance with the CCPA. Specifically, the Service Provider must notify ICW within five working days if it receives a verifiable consumer request under the CCPA.

iii. Service Provider hereby grants ICW the right, upon notice, to take reasonable and appropriate steps to stop and remediate the Service Provider's or its contractor's unauthorized use or personal information, including but not limited to providing documentation upon request from ICW that verifies that Service Provider and its contractors no longer retain or use the personal information of consumers that have made a valid request to delete with ICW.

iv. Service Provider will promptly notify ICW in writing if Service Provider makes a determination that it can no longer meet its obligations under the CCPA.

d. Subcontracting

i. ICW's data and the servers and systems used to collect, store, access, use, process, transmit or maintain such data may not be accessed or retained by third party contractors without the prior written consent of ICW's Director of Information Security or designee. Any subcontractor used must qualify as a service provider under the CCPA, including having a written contract with Service Provider, and Service Provider cannot make any disclosures to the subcontractor that the CCPA would treat as selling or sharing. Service Provider is wholly responsible to ICW for any obligations or liabilities arising from the acts or omissions of its third party contractors.

ii. For each subcontractor used, Service Provider will give ICW an up-to-date list disclosing: the subcontractor's name, address, and contact information; the type of services provided by the subcontractor; and the personal information categories disclosed to the subcontractor in the preceding 12 months.

iii. Upon ICW's written request, Service Provider will audit a subcontractor's compliance with its personal information obligations and promptly provide ICW with the audit results.

e. Service Provider certifies that it understands this Agreement's and the CCPA's restrictions and prohibitions on selling and sharing personal information and retaining, using, or disclosing personal information outside of the parties' direct business relationship, and it will comply with them.

9. **Security Awareness Training**: Service Provider shall provide regular security awareness training to all of its authorized users of ICW data and the servers and systems under Service Provider's possession, custody or control used to collect, store, access, use, process, transmit or maintain such data. Such security awareness training shall be updated from time to time to reflect security risks identified through periodic assessments of such servers and systems or as may be required by changes to applicable data protection and privacy laws, rules or regulations.

10. **General**: Service Provider represents and warrants that it complies with its information security policies and procedures and that all information provided pursuant to this Addendum is accurate and complete. Each party will bear its own costs and expenses associated with its compliance with this Addendum. Breach of this Addendum will constitute a material breach of the Agreement, and Service Provider agrees to defend, indemnify and hold harmless ICW, its employees, officers, and directors from and against all third party claims, suits, demands, damages, losses and liabilities, including reasonable legal fees and expenses, relating to or arising from any breach of Service Provider's obligations under this Addendum. The obligations of this Addendum will survive any termination, cancellation or expiration of the Agreement for so long as Service Provider has possession, custody or control of personal information it Collected pursuant to the Agreement or as set forth in the Agreement, whichever is longer. The Parties agree to amend this Addendum as necessary to comply with new or amended applicable laws, rules, and regulations.