**Security Addendum**

This Security Addendum and the terms herein supplement and are made a part of each agreement between CCC Intelligent Solutions Inc. or its Affiliate (as applicable "CCC") and its customer which incorporates this Security Addendum by reference (the "Agreement"). Terms used herein shall have the meaning set forth in the Glossary attached hereto (regardless of how those terms may be defined in the Agreement). All terms not defined in this Security Addendum take their definitions from the Agreement.

**1. Information Security Program**.

**a**. CCC will, at all times and in accordance with the provisions herein, have and maintain a written information security program based on a current Risk Assessment, which CCC will conduct at least annually, or otherwise as needed. As part of the information security program, CCC will provide and maintain technical, administrative, and physical environments having appropriate security controls effectively designed to protect from internal and external threats; unauthorized disclosure; and data loss/corruption. CCC will regularly update the information security program at least annually or when material changes to infrastructure, data, or threats occur. In furtherance of this goal, CCC will designate a single individual in charge of, and responsible for, said information security program.

**b.** CCC represents and warrants that the administrative, physical, and technical safeguards of its information security program are defined and maintained in accordance with an industry-standard risk management framework such as the National Institute for Standards and Technology (NIST) Cyber Security Framework v2.0.

**c.** CCC agrees to designate an individual/team within its company, or employ a consultant, tasked with reviewing and communicating to decision makers such laws and regulations, as well as applicable guidance documents.

**d.** CCC will involve its board of directors in information security decisions by delivering, at least annually, a report on CCC's information security program holding senior management accountable for implementing CCC's cyber risk management program.

**e.** CCC will provide each member of the CCC Workforce with recurring security awareness training appropriate to the individual's job function.

**f.** Except as set forth in the Agreement, if CCC discards or otherwise discontinues its use of media used at any time for Customer Data, such information shall be destroyed from the informational assets of CCC as follows: (i) when CCC intends to re-purpose the machine for re-use within its company, CCC will minimally use the Clear sanitization method defined in NIST 800-88 revision or (ii) when CCC intends to re-purpose the machine for use outside of CCC's ownership CCC will minimally use Purge sanitization method defined in the then current NIST revision.

**g.** If physical media is transported outside of CCC's control, such media must be encrypted using Strong Encryption, and CCC will utilize authorized couriers, transport the media in locked containers, have signatures reflecting authorization to transport, and have receipts for delivery of the physical media.

**h.** Customer recognizes that in the ordinary course of use of the Services in commerce by or on behalf of Customer, Customer Data will be shared with third parties involved in (i) the processing of Customer insurance claims or (ii) performing motor vehicle repairs in connection with a claim handled by Customer ("Intended Recipients"), and CCC shall not be in breach of the Agreement or this Security Addendum for such communication or be liable for the acts or omissions of those Intended Recipients with their receipt of, access to, or use of such Customer Data. Customer acknowledges that the provision of the Services to Intended Recipients includes making Customer Data accessible to others via the Collision Industry Electronic Commerce Association Estimate Management System ("EMS") extract and that provision of access to EMS for such purposes shall not constitute a breach of the Agreement or this Security Addendum.

**2. CCC Environment**.

**a.** Penetration Testing. At least once per year and upon a substantive change in CCC infrastructure, CCC will conduct an internal and external infrastructure penetration test and, for any software provided to Customer by CCC under the

Agreement, an application penetration test. Upon Customer's request an executive summary report will be made available to Customer. Penetration tests will be performed by an independent third-party. Upon CCC's determination, any "very high", "high", or "medium" vulnerabilities according to the Common Vulnerability Scoring System, or ratings higher than 4.0, will be promptly remediated and retested at CCC's expense.

**b.** Processing and Cross-Border Transfers. Customer Data may be Processed by CCC or its subprocessors in compliance with Applicable Laws.

**c.** Business Continuity & Disaster Recovery. CCC maintains a documented business continuity ("BCP") and disaster recovery ("DR") plan, which at a minimum:

i. Governs and defines objectives and actions required during the BCP/DR event;
ii. Provides for secure offsite copies of appropriate BC/DR documentation for retrieval following a disaster event;
iii. Defines and documents DR procedures to enable CCC to recover Protected Data;
iv. Prioritizes recovery activity based upon a documented process; and
v. Defines and documents a formal communicated plan if a BCP/DR event occurs.

**3. Information Security Policies.**

**a.** Formal Security Policies. CCC will implement and maintain written information security policies that are approved by CCC's senior management and are communicated to the CCC Workforce. The information security policies will be based on CCC's Risk Assessment and will address, at least, the areas set out in an industry standard, such as the National Institute for Standards and Technology (NIST) Cyber Security Framework v2.0.

**b.** Security Policy Review. To ensure continued suitability, adequacy, and effectiveness, CCC will review its information security policies at planned intervals (but in no event less frequent than annually) or when material changes to infrastructure, data, or threats occur.

**4. Incident Response**.

**a.** Incident Response Plan. CCC will maintain a current, and tested, written incident response plan having specific procedures for dealing with, and responding to, cyber incidents. To the extent CCC stores or has access to Customer Data, and if requested by Customer CCC will make available for inspection said incident response plan but will not be required to provide any copies during an audit conducted by the Customer, as set forth in Section 7 below.

**b.** Incident Response Program. CCC will maintain an incident response program effectively designed to intake and route cyber incidents to decision makers. CCC will form, train, and test an incident response team tasked with carrying out the cyber crisis management plan and responding to cyber incidents in an efficient and expedited manner.

**c.** Notification. Within forty-eight (48) hours of any Data Breach, CCC will notify Customer. Such notice will contain the following:

i. the nature, source and scope of the Data Breach, the data impacted, the dates of occurrence and discovery;
ii. information regarding containment, including containment measures taken and identification of any continuing exposure; and
iii. contact information for a senior level person responsible for communicating with Customer regarding the Data Breach.

**d.** Cooperation and Control. In the event of a Data Breach, CCC will reasonably cooperate with Customer (provided that Customer will not require anything of CCC that would prejudice CCC), provide regular and detailed updates, promptly conduct an investigation to determine the cause and extent of the breach, and will provide Customer with a summary report. CCC may make public statements or notifications as required by Applicable Law.

**e.** Cooperation with CUSTOMER Inquiries. In the event the Customer becomes aware of a cyber-related issue that might adversely affect CCC's security program, a notice may be communicated to CCC for its awareness. The notice will

request that CCC provide a response back to Customer detailing any impact such cyber-related issue may have on CCC's information security program and its ability to protect Customer Data.

**f.** Documentation. CCC maintains documentation on Data Breaches for at least five (5) years from the date of a breach event.

**5. Portable Device Management**.

**a.** Employee-owned Devices. With the exception of Business Contact Information, no Customer Data will be stored on, or accessed by, a non-CCC managed device.

**b.** Mobile Computing. With the exception of Business Contact Information, no Customer Data will be stored on a Portable Device and even then, only if the following are true:

i. The Portable Device employs Strong Encryption;
ii. CCC installs and maintains on the device software with the ability to remotely wipe, or permanently disable access to, the Customer Data;
iii. CCC maintains a log recording each such device and what Customer Data resides on, or is accessed by, that device; and
iv. The Portable Device uses Multi-Factor Authentication.

**6. Third-Party Vendor Management**.

**a.** Due Diligence. Prior to entering contracts or relationships with a Third-Party Provider, CCC will conduct a review of the third party's information security program and its ability meet security requirements appropriate to the level of access it will have to Customer Data and CCC's Information Processing Systems.

**b.** Third Party Oversight. CCC will contractually impose security obligations on the Third-Party Provider that are appropriate to the Services to protect Customer Data. For Cloud Providers employed by CCC, CCC will, at a minimum, review the Cloud Providers' SOC 2, Type II report and any other security-related documentation made available by the Cloud Provider. Such reviews will be conducted on an annual basis.

**7. Audit**.

Customer may request CCC's standard privacy and security questionnaires (SIG), third party reports (SOC2 Type II), and documentation to demonstrate compliance with this Security Addendum through the CCC Trust Center (https://trust.cccis.com/CCCIS). Customer requests will be reasonable and appropriate and submitted to CUSTOMER account manager.

**Glossary**

**“Applicable Laws”** has the meaning set forth in the Agreement.

**“Aggregate Data,” “De-Identified Data,” “Personal Data,” “Process,” “Processor,”** and **“Sub-Processor”** have the meanings set forth in the Data Processing Addendum incorporated into the Agreement.

**"Business Contact Information"** means information used to communicate between the parties to the Agreement such as name, job title, department name, company name, business telephone number, business fax number, and business email address.

**"Cloud Provider"** is defined as third parties contracted by CCC to provide any or all of the following: Software as a Service (SaaS); Platform as a Service (PaaS); or Infrastructure as a Service (IaaS), as such terms are defined by the National Institute of Standards and Technology ("NIST") Special Publication 800-145.

**“Customer Data”** has the meaning set forth in the Agreement.

**"Data Breach"** is defined as (a) unauthorized access to CCC's environment, or an environment controlled by CCC or its contractor(s) or vendor(s)s, where Customer Personal Data is stored or accessed, (b) unauthorized viewing, acquisition, exfiltration, or retrieval of Customer Personal Data under the care of CCC or its contractor(s) or vendor(s), or (c) the unauthorized destruction, loss, alteration or disclosure of, or access to Customer Personal Data transmitted, stored, or otherwise Processed.

**"Information Processing System(s)"** is defined as the individual and collective electronic, mechanical, and software components (including associated media types) of CCC's operations (including any Third-Party Provider operations) that store, access, process or protect Customer Data.

**"Multi-Factor Authentication"** or **"MFA"** is defined as authentication through verification of at least two of the following types of authentication factors: (a) Knowledge factors (e.g., password); (b) Possession factors (e.g., token); or (c) Inherence factors (e.g., biometric characteristic).

**"Portable Device"** means a non-CCC managed device that is capable of being easily transported, generally designed to be held and used in the hands or on the lap. It includes, but is not limited to, laptops, smartphones, PDAs, MP3 devices, USB devices, and virtual reality devices.

**"Risk Assessment"** is defined as the process of identifying inherent security risks and providing measures, processes and controls to reduce the impact of the identified risks to business operations.

**"Strong Encryption"** is defined as industry recognized encryption algorithms that employ at a minimum 256-bit AES or an equivalent strength protocol for symmetric encryption and at a minimum 2048-bit RSA or an equivalent strength protocol for asymmetric encryption.

**"CCC Workforce"** is defined as the CCC employees, contractors, or third-party workforce augmentees with access to Customer Data or CCC Information Processing System(s).

**"Third-Party Provider"** is defined as a third-party contractor, vendor, or other provider of CCC having access to Customer Data or access to networks or systems that contain Customer Data.