**DATA PROCESSING ADDENDUM**

This Data Processing Addendum ("DPA" or "Addendum") forms part of the Agreement (defined below) between the party identified in the Agreement or the applicable Archer quotation ("Customer") and RSA Security LLC, its direct and indirect subsidiaries and Affiliates ("Archer") and applies to the extent that (i) Archer Processes Personal Data, as a Processor, on behalf of Customer, as Controller, in providing Services, or (ii) the Agreement expressly incorporates this DPA by reference. All capitalized terms not defined in this DPA will have the meanings set forth in the Agreement.

1. **Definitions**.

"Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with another entity. For purposes of this definition, "control" means direct or indirect ownership or control of more than 50% of the voting interests of the entity.

"Agreement" means the written or electronic agreement identified and located at https://www.archerirm.com/company/standard-form-agreements between Customer and Archer pursuant to which Archer provides Services to Customer.

"Data Breach" means a material breach by Archer of the security obligations under this Addendum leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, the Personal Data Processed.

"Controller" means an entity which, alone or jointly with others, determines the purposes and means of the Processing of the Personal Data.

" Processor" means an entity that Processes Personal Data on behalf of a Controller.

"Data Protection Laws" means any data protection and/or privacy related laws, statutes, directives, or regulations (and any amendments or successors thereto) to which a party to this Addendum is subject and which are applicable to the Services provided under the Agreement.

"GDPR" means General Data Protection Regulation 2016/679 on the protection of natural persons in the Processing of Personal Data and on the free movement of such data, as may be amended or superseded from time to time.

"Personal Data" means any information relating to an identified or identifiable natural person ("Data Subject") which is Processed by Archer, acting as a Processor on behalf of the Customer, in connection with the provision of and subject to the limitations of the Services (as set forth in the Agreement), and which is subject to Data Protection Laws. For the avoidance of doubt, in cases where data is anonymized or pseudonymized such that the Data Subject cannot be identified by Archer, such data shall not be deemed nor construed as 'Personal Data'.

"Processing", "Processed", or "Process" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection,

recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction, subject to the parameters and limitations as set forth in the Agreement between Archer and Customer.

"Services" means any Archer cloud-based license or service, or customer support service provided by Archer to Customer pursuant to the Agreement.

“EU Standard Contractual Clauses” are the clauses as approved by the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 and located at https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.

"Subprocessor" means a third party engaged by Archer that Processes Personal Data pursuant to the Agreement.

“UK Standard Contractual Clauses” are the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the Commissioner under S119A(1) Data Protection Act 2018.

2. **Processing**.

2.1 As between Archer and Customer, Archer will Process Personal Data under the Agreement as a Processor acting on behalf of the Customer. Customer agrees that it will not require Archer to undertake or engage in any activity that would require, or result in, Archer acting in the capacity of a Controller.

2.2 Customer authorizes Archer to Process the Personal Data to provide the Services in accordance with Archer’s rights and obligations under the Agreement and in any subsequent statements of work or service orders.

2.3 This Addendum, the Agreement, and any subsequent statements of work or service orders, and any configurations by Customer or its authorized users, comprise Customer’s complete instructions to Archer regarding the Processing of Personal Data. Any additional or alternate instructions must be agreed upon by the parties in writing, including the costs (if any) associated with complying with such instructions.

2.4 Archer is not responsible for determining if Customer’s instructions are compliant with applicable law. However, if Archer is of the opinion that a Customer instruction infringes applicable Data Protection Laws, Archer shall notify Customer as soon as reasonably practicable and shall not be required to comply with such infringing instruction.

2.5 Customer will, in its use of the Services, comply with its obligations under Data Protection Laws when Processing Personal Data and when issuing Processing instructions to Archer. Customer represents that it has all rights and authorizations necessary for Archer to lawfully process Personal Data pursuant to the Agreement, as described in applicable Data Protection Laws.

2.6 Archer may only disclose Personal Data to its Subprocessors, Affiliates, and subsidiaries for the purpose of: (a) complying with Customer’s reasonable and lawful instructions; (b) as required in connection with the Services and as permitted by this Addendum; and/or (c) as required to comply with Data Protection Laws, or an order of any court, tribunal, regulator, or government agency with competent jurisdiction to which Archer is subject. With regard to (c) above, Archer will (to the extent permitted by

law) inform the Customer in advance of making any disclosure of Personal Data and will reasonably cooperate with Customer to limit the scope, proportionality, and duration of such requested disclosure to what is strictly necessary or legally required.

2.7 Archer shall maintain the confidentiality of Personal Data in accordance with Data Protection Laws applicable to Processors and shall ensure those authorized to Process the Personal Data (including its Subprocessors) are committed to obligations of confidentiality.

3. **Subprocessing**.

3.1 Customer agrees that Archer may appoint and use Subprocessors to Process Personal Data in connection with the Services PROVIDED that: (a) Archer complies with the requirements of clause 3.2 below in relation to any changes it makes to its Subprocessors (b) Archer puts in place a written contract with each Subprocessor that imposes obligations that are (i) relevant to the Services to be provided by the Subprocessors, and (ii) materially similar to the rights and/or obligations granted or imposed on Archer under this Addendum; and (c) where a Subprocessor fails to fulfill its data protection obligations as specified above, Archer shall be liable to the Customer for the performance of the Subprocessor's obligations.

3.2 The current list of Subprocessors is located at https://www.archerirm.com/company/standard-form-agreements ("Sub processors List"). If Archer engages a new Subprocessor to Process Personal Data in connection with the Services, provided Customer subscribes to receive notifications from https://www.archerirm.community/, Archer shall send an e-mail notification to Customer, and where Customer has subscribed, inform Customer, via such e-mail notification, of the engagement at least 30 days in advance of such appointment by maintaining an up to date Sub processors List and the Customer may object to the engagement of such Subprocessor by notifying Archer within ten (10) days of Archer's notification, provided that such objection shall be on reasonable, substantial grounds directly related to such Subprocessor's ability to comply with substantially similar obligations to those set out in this Addendum. If the Customer does not so object, the engagement of such Subprocessor shall be deemed accepted by the Customer. If the Customer does so object, Archer shall use commercially reasonable endeavours to recommend a reasonable change to the Customer's configuration of the Services to avoid processing of Personal Data by the objected-to new Subprocessor without unreasonably burdening the Customer. If Archer is unable to make available such change within a reasonable period of time, which shall not exceed 30 days, the Customer may terminate this Agreement with respect only to those Services which cannot be provided by Archer without the use of the objected-to new Subprocessor by providing written notice to Archer. Such termination shall not entitle Customer to any refund on a committed Subscription Term and Customer shall remain liable for all fees otherwise due. For the avoidance of doubt, Customer shall be liable to pay any outstanding fees on a committed Order.

4. **Security Measures**.

4.1 Taking into account industry standards, the costs of implementation, the nature, scope, context, and purposes of the Processing, and any other relevant circumstances relating to the Processing of the Personal Data on Archer systems, Archer shall implement appropriate technical and organisational measures to ensure security, confidentiality, integrity, availability, and resilience of processing systems and services involved in the Processing of the Personal Data are commensurate with the risk in respect of such Personal Data. The Parties agree that the technical and organisational security measures described in the applicable option in Annex 2 provide an appropriate level of security for the protection of Personal Data to meet the requirements of this clause. Archer will periodically (i) test and monitor the effectiveness of its safeguards, controls, systems, and procedures, and (ii) identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of the Personal Data, and ensure these risks are

addressed. Archer shall implement and document appropriate business continuity and disaster recovery plans, in accordance with the applicable option in Annex 2, to enable it to continue or resume providing Services (including restoring access to the Personal Data where applicable) in a timely manner after a disruptive event.

4.2 Customer is responsible for using and configuring the Services in a manner that enables Customer to comply with Data Protection Laws. Such measures shall provide an appropriate level of security for the protection of Personal Data to meet the requirements of this clause.

4.3 Archer restricts its personnel from Processing Personal Data without authorization (unless required by applicable law) and will ensure that any personnel authorized by Archer to process Personal Data is subject to an obligation of confidentiality.

5. **Data Breach.**

5.1 Archer will notify Customer without undue delay after becoming aware of a Data Breach in relation to the Services provided by Archer under the Agreement, and shall:

(a) to the extent such information is known or available to Archer at the time, provide Customer with details of the Data Breach, a point of contact, and the measures taken or to be taken to address the Data Breach; and

(b) reasonably cooperate and assist Customer with any investigation into, and/or remediation of, the Data Breach (including, without limitation and where required by Data Protection Laws, the provision of notices to regulators and affected individuals); and

(c) not inform any unaffiliated third party (other than, in each case as necessary, another customer affected by the same Data Breach, a Subprocessor potentially possessing relevant information, or experts or consultants utilized by Archer) of any Data Breach relating to the Personal Data without first obtaining Customer's prior written consent, except as otherwise required by applicable law.

5.2 In the event Customer intends to issue a notification regarding the Data Breach to a data protection supervisory authority, other regulator, or law enforcement agency, Customer shall (unless prohibited by law) allow Archer to review the notification and Customer shall consider any reasonable comments or amendments proposed by Archer.

6. **Demonstrate Compliance.**

Archer shall, upon reasonable prior written request from Customer (not to be made more than once in any twelve-month period), provide Customer such information as may be reasonably necessary under applicable law and in accordance with Archer's security practices, to demonstrate Archer's compliance with its obligations under this Addendum.

7. **International Data Transfers.**

7.1 Archer may, in connection with the provision of the Services, or in the normal course of business, make international transfers of Personal Data to its Affiliates, subsidiaries, and/or Subprocessors. When making such transfers, Archer shall ensure appropriate protection is in place to safeguard the Personal Data transferred under or in connection with this Addendum.

7.2 Where the provision of Services involves the transfer of Personal Data from the United Kingdom to countries outside the EEA (which are not subject to an adequacy decision under Data Protection Laws) (each an "ex-UK Transfer") such transfer shall be subject to the following requirements: (a) Archer has in

place intra-group agreements that incorporate UK Standard Contractual Clauses with any Affiliates or subsidiaries which may have access to the Personal Data; and (b) Archer has in place agreements with its Subprocessors that incorporate the UK Standard Contractual Clauses, as appropriate.

7.3 Where the provision of Services involves the transfer of Personal Data from the EEA to countries outside the EEA (which are not subject to an adequacy decision under Data Protection Laws) (each an "**ex-EEA Transfer**") such transfer shall be subject to the following requirements: (a) Archer has in place intra-group agreements that incorporate EU Standard Contractual Clauses with any Affiliates or subsidiaries which may have access to the Personal Data; and (b) Archer has in place agreements with its Subprocessors that incorporate the EU Standard Contractual Clauses, as appropriate.

7.4 Archer and Customer agree that, where the transfer of Personal Data from Customer to Archer in connection with the Services constitutes an ex-EEA Transfer, Archer and Customer shall comply with the EU Standard Contractual Clauses in relation to such ex-EEA Transfer (which for these purposes are hereby incorporated into this Agreement and executed by the parties) with the amendments set out below applied to the EU Standard Contractual Clauses:

a) When Customer (as data exporter) acts as the Controller and Archer (as data importer) acts as a Processor, then Module Two applies, and the other Modules shall be disregarded.
   i. The appropriate designation is set forth in Annex I attached hereto.
   ii. Option 2 for Clause 9(a) applies. Archer shall inform the Customer of any intended changes to sub-processors at least 30 days in advance.
   iii. Option 2 for Clause 17 applies. As described in Clause 17, Parties agree that the law of the relevant Member State shall be the governing law.
   iv. For Clause 18, disputes shall be resolved in the courts of Data Exporter Member State
   v. Liability arising under the EU Standard Contractual Clauses in respect of a party shall form part of the liability of such party under the Agreement.
   vi. Annex II and III shall be as set out below.

7.5 Archer and Customer agree that, where the transfer of Personal Data from Customer to Archer in connection with the Services constitutes an ex-UK Transfer, Archer and Customer shall comply with the UK Standard Contractual Clauses in relation to such ex-UK Transfer (which for these purposes are hereby incorporated into this Agreement and executed by the parties) with the designations and amendments set out in Annex 2 to this DPA.

7.6 If there is any conflict or ambiguity between the terms of this Addendum and the terms of the EU Standard Contractual Clauses, the term contained in the EU Standard Contractual Clauses shall have priority (but only to the extent and in respect of the transfer, and not in respect of any other processing activity).

8. **Deletion of Data.**

Upon termination of the Services (for any reason) and if requested by Customer in writing, Archer shall, as soon as reasonably practicable and in accordance with applicable law, delete the Personal Data on Archer systems, PROVIDED that Archer may: (a) retain one copy of the Personal Data as necessary to comply with any legal, regulatory, judicial, audit, or internal compliance requirements; and (b) defer the deletion of the Personal Data to the extent and for the duration that any Personal Data or copies thereof

cannot reasonably and practically be expunged from Archer's systems. The parties hereby expressly acknowledge that Customer instructs Archer to maintain back-up files of all Customer data (which may include Personal Data), for the duration established in the Agreement. For such retention or deferral periods as set forth above, the provisions of this Addendum shall continue to apply to such Personal Data. Archer reserves the right to charge Customer for any reasonable costs and expenses incurred by Archer in deleting the Personal Data pursuant to this clause. A certificate of destruction will be provided upon request.

9. **Cooperation.**

9.1 If Archer receives any request from Data Subjects, or applicable data protection authorities relating to the Processing of Personal Data under the Agreement, including requests from Data Subjects seeking to exercise their rights under Data Protection Laws, Archer will promptly redirect the request to the Customer. Archer will not respond to such communication directly without Customer's prior authorization, unless legally compelled to do so. If Archer is required to respond to such a request, Archer will promptly notify Customer and provide Customer with a copy of the request, unless legally prohibited from doing so.

9.2 Archer shall provide reasonable cooperation and assistance to Customer, to the extent applicable in relation to Archer's processing of the Personal Data, in connection with any data protection impact assessment(s) which the Customer may carry out in relation to the processing of Personal Data to be undertaken by Archer, including any required prior consultation(s) with supervisory authorities. Archer reserves the right to charge Customer a reasonable fee for the provision of such cooperation and assistance.

9.3 To the extent required by Data Protection Laws, Archer will, upon reasonable notice and at Customer's expense, provide reasonably requested information regarding the Services to enable Customer to carry out data protection impact assessments ("DPIAs") and/or prior consultations with data protection authorities.

9.4 Neither Archer nor any Subprocessor shall be liable for any claim brought by Customer or any third party arising from any action or omission by Archer and/or Subprocessors to the extent such action or omission resulted from compliance with Customer's instructions, security practices, policies, and/or procedures.

10. **General.**

10.1 Any claims brought under this Addendum will be subject to the terms and conditions of the Agreement, including the exclusions and limitations set forth in the Agreement.

10.2 In the event of any conflict between this Addendum and the Agreement, the terms of this Addendum will prevail with respect to its subject matter.

10.3 Archer may modify the terms of this Addendum as provided in the Agreement (i) if required to do so by a supervisory authority or other government or regulatory entity, (ii) if necessary, to comply with Data Protection Laws, or (iii) to implement or adhere to applicable Standard Contractual Clauses,

approved codes of conduct or certifications, binding corporate rules, or other compliance mechanisms, which may be permitted under Data Protection Laws. Supplemental terms may be added as an Annex or Appendix to this Addendum where such terms only apply to the Processing of Personal Data under the Data Protection Laws of specific countries or jurisdictions. Archer will provide notice of such changes to Customer, and the modified Addendum will become effective, in accordance with the terms of the Agreement or as otherwise provided on Archer's website if not specified in the Agreement.

# Annex 1

## Annex I to the Standard Contractual Clauses

A. LIST OF PARTIES

Module Selection

| Select applicable Module(s) | |
|---|---|
| | Module One: Controller to Controller |
| **X** | Module Two: Controller to Processor |
| | Module Three: Processor to Processor |
| | Module Four: Processor to Controller |

**Data exporter(s):**

**Name:** The entity identified as "Customer" in the Addendum.

**Address:** The address for Customer associated with its account or as otherwise specified in the Addendum or the Agreement.

**Contact person's name, position and contact details:** The contact details associated with Customer's account, or as otherwise specified in the Addendum or the Agreement.

**Activities relevant to the data transferred under these Clauses**: The activities are specified in Section 2 of the Addendum.

**Signature and date**: In accordance with the Agreement signature and Effective Date.

**Role (controller/processor)**: Controller.

**Data importer(s):**

**Name**: "Archer" as identified in the Addendum, or the applicable Archer Security LLC Affiliate.

**Address**: The address for Archer is specified in the Agreement.

**Contact person's name, position and contact details**: The contact details for Archer are specified in the Addendum or the Agreement.

**Activities relevant to the data transferred under these Clauses**: The activities are specified in Section 2 of the Addendum.

**Signature and date**: By transferring Personal Data to Third Countries on Customer's instructions, the data importer will be deemed to have signed this Annex I.

**Role (controller/processor**): Processor

B. DESCRIPTION OF TRANSFER

***Categories of data subjects whose personal data is transferred**:*

*The data subjects are Customer's end users, employees, contractors, suppliers and other third parties relevant to the Services.*

***Categories of personal data transferred**:*

- *Contact details: which may include name, address, email address, telephone, fax, other contact details, emergency contact details, associated local time zone information.*

- *Customer details: which may include Contact details, invoicing, and credit related data.*

- *IT systems and operational information: which may user ID and password details, computer name, email address, domain name, user names, passwords, IP address, permission data (according to job roles), account and delegate information for communication services, individual mailboxes and directories, chat communication data, software and hardware inventory, tracking information regarding patterns of software and internet usage (e.g. cookies), and information recorded for operational and/or training purposes.*

- *Customer support: which may include personal identifiers, voice, video and data recordings.*

- *Other: Any other Personal Data contained within Customer Content*

***Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures**:*

*Archer does not intend to process any special categories of Personal Data on behalf of the Customer. Customer agrees not to provide, transfer, or disclose any special categories of Personal Data at any time to any of Archer's service offerings.*

***The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):***

*Personal data is transferred in accordance with Customer's instructions as described in Section 2.*

***Nature of the processing:***

*The nature of the processing is described in Section 2 of the Addendum.*

***Purpose(s) of the data transfer and further processing**:*

*To provide the Services.*

***The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period****:*

The data exporter determines the duration of processing in accordance with the terms of the Addendum

***For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing****:*

*The subject matter, nature, and duration of the processing are described in Section 2 of the Addendum.*

C. COMPETENT SUPERVISORY AUTHORITY

***Identify the competent supervisory authority/ies in accordance with Clause 13:***

*The data exporter's competent supervisory authority will be determined in accordance with the GDPR.*

# Annex II

## Annex II to the Standard Contractual Clauses. Technical and Organizational Measures Including Technical and Organizational Measures to Ensure the Security of the Data.

**Option 1: Where Personal Data is processed in connection with use of Archer on premise Software, Maintenance Support, or Professional Services**

Technical and organizational security measures in Archer's compliance programs include the following:

A. **Measures to ensure security of processing**

1. **Entrance Control**

Where appropriate, the following measures designed to prevent unauthorized persons from gaining access to data processing systems are used:

- Where visitors are permitted at data centers used to process customer-provided data, visitors must register the following information: full name of visitor; date and time of arrival; and purpose of visit;
- Data center access is granted on a least-privilege, and need-to-know basis;
- CCTV covers appropriate areas (e.g., entrances to data centers and other sensitive data center areas);
- The Archer corporate facility is secured by an access control system where access to the corporate facility is granted with an activated entry card or other appropriate technological measures; and
- Outside areas may be under video surveillance or under monitoring by a security service or under guard service.

2. **Admission Control**

Appropriate measures preventing unauthorized persons from using data processing systems.

- Access to Archer-controlled IT systems is granted only to users when registered under authorized usernames;
- Internal password policy aligns to NIST SP 800-63B guidelines, or its successor;
- Archer corporate policy includes automatic computer lock after a short, technologically enforced period, with renewed access to the PC only after new registration with a valid username and password; and
- Outside network access requires a two-factor-authentication.

3. **Access Control**

Appropriate measures to ensure that data cannot be read, copied, modified, or removed without authorization in the course of processing or use and after storage, are as follows:

- Access authorization is issued in respect of the specific area of work to which the resource is assigned (work roles); and
- Policy requires regular verification of access authorizations.

4. **Separation Control**

Appropriate measures ensuring that data collected for different purposes can be processed separately:

- Data of different controllers shall be processed separately; and
- Functional separation between test and production systems is employed.

B. **Measures to ensure integrity of processing**

1. **Transmission Control**

Appropriate measures to ensure that data cannot be read, copied, modified, or removed without authorization during electronic transmission or transport are as follows:

- Encrypted data transfer when handling data and when accessing the company network;
- Monitoring of data transfer for suspicious traffic;
- Restrictive usage of Wireless LAN;
- Wireless networking is not leveraged in the provision of Archer cloud-based services;
- Restrictive remote access to Archer corporate network and systems (using two-factor-authentication);
- Where applicable, data media is disposed of in accordance with data protection policies by use of one or more of the following, as appropriate: safety containers and document shredders; physical destruction; erasure using industry standard processes; crypto shredding; or other approved disposition procedures; and
- Remote support (screen sharing) requires an affirmative action from the recipient of the screen share request.

2. **Input Control**

Measures to ensure the identity and authorization associated with input, access, modification, and removal of data with respect to data processing systems are as follows:

- When using relevant applications, access is automatically recorded; and
- Remote support (screen sharing) permits the recipient of the screen share request to terminate the support activity at any time.

C. **Measures to ensure security, availability, and resilience of processing**

1. **Subcontractors and background checks**

No Processing according to Art. 28 GDPR shall take place without Controller's instructions, clear contract drafting, formalized assignment management, strict vetting processes, and checks. In addition:

- Subcontractors are on-boarded using processes that entail risk assessment, and implementation of contractual terms entailing data protection, confidentiality, integrity, and availability obligations, as appropriate;
- Subcontractors are regularly reviewed for compliance; and
- To the extent legally permissible, Archer ensures that background checks are conducted on its employees and subcontractors at the onboarding stage.

2. **Data protection measures**

Measures to ensure that data is protected from accidental destruction or loss, are as follows:

- Where appropriate, anti-malware software is installed on applicable systems;
- Firewalls or equivalent technologies (e.g., AWS security groups) are used to protect Archer-controlled networks;
- Network segmentation is used where applicable and appropriate;
- Content filtration (e.g., proxies) are implemented for the Archer corporate network;

- Interruption-free power supply is required for all critical systems;
- Fire safety systems are in place where required by law; and
- Processes or mechanisms for handling emergencies and disasters are in place and communicated to personnel responsible for handling such.

3. **Resiliency**

Where appropriate, punctual peak demands or long-term high demands are reflected in the design of systems and services (e.g., memory, access, and throughput capacities, etc.) to ensure resilience and consistency of processing.

4. **Incident Response**

Corporate response capabilities related to cybersecurity incidents are in place to address incident scope, identification, assessment, response, and remediation, including notifications to regulators, controllers, and/or data subjects, as may be required.

5. **Encryption at rest**

Data is encrypted at rest using current industry standard encryption techniques, ciphers, and strengths.

6. **Testing**

Processes for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of data processing are as follows:

- Corporate security policies are reviewed at least annually, with final review/approval provided by the Chief Information Security Officer.

**Option 2: Where Personal Data is processed in connection with use of Archer SaaS and / or Archer Engage**

**INFORMATION SECURITY AND BUSINESS CONTINUITY PLANNING FOR ARCHER SAAS OFFERING**

## 1. ADHERENCE TO STANDARDS OF PROTECTION.

Archer will apply commercially reasonable efforts to carry out the following procedures to protect Customer Content. In fulfilling its obligations under this Exhibit, Archer may, from time to time, utilize methods or procedures ("Processes") similar to and substantially conforming to certain terms herein. Archer shall ensure that any such Processes are no less rigorous in their protection to Customer than the standards reflected in this Exhibit's terms set forth below and shall provide safeguards no less protective than those of the original terms of this Exhibit in all material respects.

For the avoidance of doubt, where Customer is purchasing an Engage Service Offering, all terms of this Exhibit 2 apply to the Service Offering(s), not to Incidental Software controlled by Customer; Customer acknowledges and agrees that it is responsible for all appropriate information security and business continuity concerns related to Customer's use of Incidental Software.

**A. Definitions**.

(i) "Firewall" is an integrated collection of security measures used to prevent unauthorized electronic access to a networked computer system.

(ii) "Encryption" is a process of using an algorithm to transform data into coded information in order to protect confidentiality.

(iii) "Intrusion Detection Process" (or "IDP") is a method of reviewing system events and Processes in near real time and, without unreasonable delay, alerting management to known patterns of behavior that indicate an intrusion is occurring or is likely to take place soon.

(iv) "Security Incident" means any loss of, or unauthorized or unlawful access to, acquisition of, use of, or disclosure of, Customer Content within the possession (*e.g.,* the physical or IT environment) of Archer or any Authorized Person.

(v) "Authorized Persons" means Archer's employees, contractors, or other agents who need to access Customer Content to enable Archer to perform its obligations under the Agreement, and who are bound by confidentiality and other obligations sufficient to protect Customer Content in accordance with the terms and conditions of the Agreement.

**B. Breach Notification and Remediation**.

In the event Archer becomes aware of a Security Incident, Archer shall, in the most expedient time possible under the circumstances, notify Customer of the Security Incident and shall, subject to applicable laws, regulations, or a governmental request, provide Customer with details to the extent available about the Security Incident, including how it occurred and how Archer will address the Security Incident. In the event of a Security Incident, Archer and Customer shall cooperate in good faith to resolve any privacy or data security issues involving Customer Content, and to make any legally required notifications to individuals affected by the Security Incident. In the event of an actual Security Incident involving Archer's systems or network, Archer shall:

(i) Breach Notification. Within seventy-two (72) hours after the Security Incident notify Customer of the approximate date and time of the Security Incident and a summary of known, relevant facts and actions taken to rectify the Processes and address the Security Incident's effects.

(ii) Breach Remediation. Promptly implement reasonable measures necessary to address the security of Archer's systems and the security of Customer Content. If such measures include temporarily restricting access to any information, network or systems comprising the Service Offering in order to mitigate against further breaches, Archer shall promptly notify Customer of the restricted access, in advance of such restriction when possible but in all cases as soon as possible under the circumstances. Archer shall cooperate in good faith with Customer to allow Customer to verify Archer's compliance with its obligations under this clause.

**C. Independent Control Attestation and Testing**.

Archer shall employ independent third party oversight as follows:

(i) Attestation. At least annually and at its own expense, Archer shall ensure that an audit of data center facilities where Customer Content is stored, processed, or transmitted by Archer is conducted according to appropriate industry security standards by an independent third party auditor and that such audit will result in the generation of an industry standard audit report (for example, SSAE-18 SOC 2, Type II, ISO 27001, or similar) ("Audit Report"). Upon Customer request and no more than once annually, Archer shall: (i) make good faith answers to an industry standard security questionnaire; and (ii) ensure that a copy of the most recent Audit Report pertaining to the Service Offering is available to customer. The availability of such Audit Report shall be made under a separate non-disclosure agreement mutually agreed upon by the parties.

(ii) Penetration Testing. At least annually and at its own expense, Archer shall engage a third party testing service provider for network penetration testing of the infrastructure and systems used to provide the Service Offering and upon reasonable Customer request, Archer will provide a copy of the most recent executive summary pertaining to said testing.

**D. Data Security**.

Archer shall use commercially reasonable efforts to carry out the following procedures to manage Customer Content as follows:

(i) Information Classification. If Customer discloses Customer's Content to Service Provider or if Service Provider accesses Customer's content as permitted by the

Agreement, Customer Content shall be classified as Confidential and handled in accordance with the terms hereof.

(ii) Encryption of Information. Industry-standard encryption techniques (for example, public encryption algorithms such as, RC5, IDEA, Archer and AES) shall be used at cipher strengths no less than 256-bit or equivalent for Customer Content. Archer shall use industry standard authentication practices to authenticate parties and secure messages and/or communications involving Customer Content, where applicable.

(iii) Cryptographic Key Management. Archer shall ensure that cryptographic keys are managed securely in accordance with control requirements and procedures which are consistent with industry best practices, and shall ensure that Customer Content is protected against unauthorized access or destruction. Archer shall ensure that if public key infrastructure (PKI) is used, it shall be protected by 'hardening' the underlying operating system(s) and restricting access to certification authorities.

(iv) Data Access; Transmission. Archer shall make Archer-controlled applications and systems used to process or store Customer Content accessible only by those whose job responsibilities require such access. If transferred across the Internet, wireless network (e.g., cellular, 802.11x, or similar technology), or other public or shared networks, Customer Content shall be protected using appropriate cryptography.

(v) Event Logging. For systems directly providing the Service Offering to Customer, Archer shall maintain logs of key events that may affect the confidentiality, integrity, and/or availability of the Service Offering to Customer and that may assist in the identification or investigation of material incidents and/or security breaches occurring in relation to Archer systems. The logs shall be retained for at least 90 days and protected against unauthorized changes (including, amending or deleting a log).

(vi) Removable Media. "Removable Media" means portable or removable magnetic and/or optical media, including but not limited to hard disks, floppy disks, USB memory drives, zip disks, optical disks, CDs, DVDs, digital film, memory cards, magnetic tape, and other removable data storage media whether owned by Customer or Archer. The use of Removable Media is prohibited unless authorized by Customer in writing.

(vii) Disposition of Customer Content. In the event of termination of the Service Offering(s), Archer shall use industry standard techniques (such as those detailed by NIST 800-88) designed to prevent Customer Content from being exposed to unauthorized individuals as part of the decommissioning process.

**E. Computer & Network Security.**

Archer shall use commercially reasonable efforts to carry out the following procedures to protect Customer Content:

(i) Server Security. Computer systems comprising the Service Offering shall be dedicated solely to the provision of the Service Offering and not used by Archer for development and/or testing unless required to fulfill obligations within this Agreement.

(ii) Internal Network Segment Security. Data entering the Service Offering's network from external sources shall pass through Firewalls to enforce secure connections between internal and external systems.

(iii) External Network Segment Security. The Service Offering's connections to the Internet shall (a) have appropriate security measures and controls applied, and (b) include an IDP that monitors data within the external network segment and information coming to Firewalls. Archer's IDP shall be designed to detect and report unauthorized activity prior to entering the Firewalls. Archer shall disable unnecessary network access points.

(iv) Network and Systems Monitoring. Archer shall actively monitor its networks and systems used to provide the Service Offering to detect deviation from access control policies and actual or attempted intrusions or other unauthorized acts.

(v) User Authentication. Archer shall implement Processes designed to authenticate the identity of its system users through the following means:

i. User IDs. Each user of a system containing Customer Content shall be assigned a unique identification code ("User ID").

ii. Passwords. Each user of a system containing Customer Content shall use a unique password whose length, complexity, and age should be governed in accordance with industry best practices.

iii. Two-Factor Authentication for Remote Access. Remote access to systems containing Customer Content shall require the use of two-factor authentication.

iv. Deactivation. Archer User IDs shall be automatically deactivated after a technologically enforced number of unsuccessful log-in attempts. Interactive sessions shall be restricted or timed out after a technologically enforced period of inactivity. User IDs for Archer Personnel with access to Customer Content shall be deactivated promptly upon changes in job responsibilities that render such access unnecessary and during termination of employment.

(vi) Account Access. Archer shall provide account access to Archer Personnel on a least-privilege, need to know basis.

**F. System Development.**

(i) Development Methodology and Installation Process.

i. Documented Development Methodology. Archer shall ensure that development activities for Archer-developed software used in the provision of the Service Offering are carried out in accordance with a documented system development methodology.

ii. Documented Deployment Process. Archer shall ensure that new systems and changes to existing systems used in the provision of the Service Offering are deployed in accordance with a documented process.

(ii) Testing Process. Archer shall ensure that all reasonable elements of a system (i.e. application software packages, system software, hardware and services, etc.) shall be tested at all relevant stages of the systems development lifecycle before applicable system changes are promoted to the production environment.

(iii) Customer Content in Test Environments. Archer shall ensure that Customer Content is not used within Archer test environments without Customer's prior written approval.

(iv) Secure Coding Practices. Archer shall have secure development practices for itself and require the same of its subcontractors, including the definition, testing, deployment, and review of security requirements.

**G. General Security.**

(i) Point of Contact. Archer shall designate an account manager with whom Customer may coordinate as an escalation point beyond typical Service Offering customer support avenues available to Customer.

(ii) Data Center Facilities. The Service Offering shall be housed in secure areas and protected by perimeter security such as barrier access controls (e.g., the use of guards and entry badges) that provide a physical environment secure from unauthorized access, damage, and interference. Additional requirements specific to the data center facilities are:

i. Two-Factor Authentication. Two-factor authentication shall be required for entry on access points that are designed to restrict entry and limit access to certain highly sensitive areas.

ii. Limited Internet Access. Archer Personnel shall have access to external email and/or the Internet only to the extent required by job function in support of the Service Offering.

iii. CCTV Systems. Closed circuit television (CCTV) systems and CCTV recording systems shall be used to monitor and record access to controlled areas.

iv. ID Badges. Identification badges showing the bearer's name, photographic likeness and organization to which he or she belongs shall be issued and required at data center facilities at all times.

v. Visitor Procedures. Procedures for validating visitor identity and authorization to enter the premises shall be implemented and followed, including but not limited to an identification check, issuance of a clearly-marked Visitor identification badge, host identity, purpose of visit, and recorded entry and departure times.

(iii) Change and Patch Management. Archer shall use commercially reasonable efforts to ensure that changes (including but not limited to emergency fixes, application patches, firmware updates, and similar) to its applications and infrastructure associated with the Service Offering are tested, reviewed, approved, and applied using an industry standard change management process that accounts for risks to Archer, its customers, and other such factors as Archer deems relevant.

(iv) Archer Personnel.

i. Background Screening. Archer shall perform background checks in accordance with Archer screening policies on all Archer employees and consultants who are or will be supporting the Service Offering under this Agreement, to the extent permitted by applicable law.

ii. Training. Archer Personnel involved in the provision of the Service Offering shall receive appropriate ongoing security awareness training. Such security awareness training shall be provided within one (1) month of Archer Personnel being engaged in the provision of the Service Offering or prior to Archer Personnel being given access to Customer Content.

iii. Subcontractors. Where applicable, Archer shall require subcontractors engaged in the provision of the Service Offering(s) (other than auxiliary services that facilitate the Service Offering(s) (e.g. guard service, media destruction, etc.)) to have in place and maintain a commercially reasonable business continuity program that complies with industry best practices.

**2. BUSINESS CONTINUITY PLANNING.**

Archer shall ensure that the Service Offering business continuity plan ("BCP") capabilities include, at a minimum, a secure contingency site containing the hardware, software, communications equipment, and current copies of data and files necessary to perform Archer's obligations under this Agreement.

**A.** BCP Requirements. The BCP shall:

(i) address the relocation of affected Archer Personnel to contingency locations and the reallocation of work;

(ii) require a remote contingency site with adequate security and capacity to provide the Service Offering in accordance with the obligations of this Agreement;

(iii) require Processes designed to ensure that Customer Content and other data necessary for the performance of the Service Offering are automatically copied to a remote contingency site;

(iv) include a description of the recovery process to be implemented following the occurrence of a disaster;

(v) detail key resources and actions necessary to ensure that business continuity is maintained;

(vi) include a forty-eight (48) hour recovery time objective ("RTO") in which the Service Offering shall be recovered following the occurrence of a disaster; and

(vii) allow for the recovery of Customer Content at the remote contingency site in accordance with a twenty-four (24) hour recovery point objective ("RPO").

**B.** BCP Testing. At least annually and at its own expense, Archer will conduct a test of the BCP Plan. Upon reasonable request, Archer will provide an overview consisting of the date(s), scope, and outcome (on a succeed or fail basis) of the last test.

**C.** BCP Activation.

(i) Notification. In case of a Force Majeure Event that Archer reasonably believes will impact the Service Offering or its ability to perform its obligations under this Agreement, Archer shall, to the extent possible, promptly notify Customer of such Force Majeure Event. Such notification shall, as soon as such details are known, contain:

i. a description of the Force Majeure Event in question;
ii. the impact the Force Majeure Event is likely to have on the Service Offering and Archer's obligations under this Agreement;
iii. the operating strategy and the timetable for the utilization of the contingency site;
iv. the timeframe in which Archer expects to return to business as usual; and
v. crisis management escalations affecting Customer Content.

(ii) Contact Points. Archer Archer Customer Support and/or Customer's Archer account manager shall coordinate with Customer's representative for the purpose of exchanging information and detailed, up-to-date status and on-going actions on and from the occurrence of a disaster. Customer shall make sure that its representative is at all times known to Archer Archer Customer Support.

# Annex III

## Annex III to the Standard Contractual Clauses. List of Sub-Processors.

As applicable, the controller authorizes the use of the sub-processors located at Archer Subprocessor List

## Annex 2 – UK Standard Contractual Clauses

The following designations and amendments shall apply to the UK Standard Contractual Clauses:

1. Part 1: Table 1: Parties of the UK Standard Contractual Clauses shall be in accordance with Annex I to the Standard Contractual Clauses at Annex 1.

2. Part 1: Table 2: Selected SCCs, Modules and Selected Clauses is as set out below:

    a. The relevant designations are in accordance with Section 7.4 of the DPA, unless such designations contradict the UK Standard Contractual Clauses, in which case the UK Standard Contractual Clauses shall prevail.

3. For the purpose of the relevant designations at Part 1: Table 3 Appendix Information, the following shall apply:
    a. Annex 1A and Annex 1B details are in accordance with Annex I to the Standard Contractual Clauses at Annex 1 to this DPA
    b. Annex II 'Technical and organisational measures including technical and organisational measures to ensure the security of the data' is in accordance with Annex II to the Standard Contractual Clauses at Annex 1 to this DPA.
    c. Annex III: List of Sub processors is in accordance with Annex III to the Standard Contractual Clauses at Annex 1 to this DPA.

4. For the purpose of Part 1: Table 4: Ending this Addendum when the Approved Addendum Changes, the following selections shall apply: 'Importer' and 'Exporter'.