Information Security and Business Continuity Planning for Archer SaaS, Archer Engage, and Archer Insight

Any capitalized terms used but not defined herein shall have the meaning set forth in the agreement between Archer and Client that references this document. Archer may review and update its security obligations in this addendum, provided that such updates do not materially diminish the protections herein.

Organizational Security Measures

(see below for security measures specific to the Archer SaaS Applications)

1. Measures to ensure security of processing.

1.1. Entrance Control. Where appropriate, Archer uses the following measures designed to prevent unauthorized persons from gaining access to data processing systems:

- Where visitors are permitted at data centers used to process Client-provided data, visitors must register the following information: full name of visitor; date and time of arrival; and purpose of visit.
- Archer grants data center access 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).
- Archer's corporate facility is secured by an access control system where Archer grants access to the corporate facility with an activated entry card or other appropriate technological measures.
- Outside areas may be under video surveillance or under monitoring by a security service or under guard service.

1.2. Admission Control. Appropriate measures preventing unauthorized persons from using data processing systems.

- Archer grants access to Archer-controlled IT systems only to users 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.
- Outside network access requires a two-factor-authentication.

1.3. Access Control. Appropriate measures to ensure that data cannot be read, copied, modified, or removed without authorization while processing or use and after storage, are as follows:

- Archer issues access authorization regarding the specific work area to which Archer assigns the resource (work roles); and
- Policy requires regular verification of access authorizations.

1.4. Separation Control. Appropriate measures ensuring that Archer can process data collected for different purposes separately:

- processing data of different controllers separately; and
- employing functional separation between test and production systems.

2. Measures to ensure integrity of processing.

2.1. Transmission Control. Appropriate measures to ensure that data cannot be read, copied, modified, or removed without authorization during electronic transmission or transport are:

- 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, Archer disposes of data media in accordance with data protection policies by using 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.

- Remote support (screen sharing) requires an affirmative action from the recipient of the screen share request.

2.2. Input Control. Measures to ensure the identity and authorization associated with input, access, modification, and data removal regarding data processing systems are as follows:

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

3. Measures to ensure security, availability, and resilience of processing.

3.1. 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:

- Archer on-boards subcontractors using processes that entail risk assessment, and contractual terms entailing data protection, confidentiality, integrity, and availability obligations, as appropriate.
- Archer regularly reviews subcontractors for compliance.
- To the extent legally permissible, Archer conducts background checks on its employees at the onboarding stage.

3.2. Data protection measures. Measures to ensure that data is protected from accidental destruction or loss, are as follows:

- Where appropriate, Archer installs anti-malware software on applicable systems.
- Firewalls or equivalent technologies (e.g., AWS security groups) to protect Archer-controlled networks.
- Network segmentation where applicable and appropriate.
- Content filtration (e.g., proxies) for the Archer corporate network.
- Interruption-free power supply for all critical systems.
- Fire safety systems where required by law.
- Processes and mechanisms for handling emergencies and disasters and communicates them to personnel responsible for handling such.

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

3.4. 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.

3.5. Encryption at rest. Archer encrypts data at rest using current industry standard encryption techniques, ciphers, and strengths.

3.6. 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:

- The Chief Information Security Officer reviews and approves corporate security policies at least annually.

Information Security Protections for Archer SaaS Applications

1. Adherence To Standards of Protection. Archer will apply commercially reasonable efforts to carry out the following procedures to protect Client 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 Client 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 Client is procuring Archer Insight or Archer Engage, all terms of this Exhibit 2 apply to Archer Application(s), not to Incidental Software (as defined below) controlled by Client; Client acknowledges and agrees that it is responsible for all appropriate information security and business continuity concerns related to Client's use of Incidental Software.

2. Definitions.

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

2.2. "**Encryption**" is a process of using an algorithm to transform data into coded information to protect confidentiality.

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

2.4. "**Incidental Software**" means software that must be installed in Client's on-premises environment to enable Client to use the Archer Application(s). This section applies to Archer Engage and Archer Insight only. If Client is an on-premises Archer GRC Platform Software Client, Client acknowledges and agrees that Incidental Software must be downloaded, installed, managed, configured, and maintained by Client to use its on-premises installation of the Archer GRC Platform Software to enable Client to use the Archer Application(s). Client may use that software only (a) in connection with Client's use of the Archer Application(s), (b) for the Subscription Term, and (c) in accordance with the Agreement. If that software is subject to an accompanying license agreement, Client must comply with the terms of that license. If that software does not have an accompanying license agreement, then Archer's standard end user license agreement made generally available by Archer on its website applies.

2.5. "**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.

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

3. Breach Notification and Remediation.

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

3.2. Breach Notification. Archer shall, within seventy-two (72) hours after the Security Incident, notify Client 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.

3.3. Breach Remediation. Archer shall promptly implement reasonable measures necessary to address the security of Archer's systems and Client Content security. If such measures include temporarily restricting access to any information, network or systems comprising the Archer Applications to mitigate against further breaches, Archer shall promptly notify Client 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 Client to allow Client to verify Archer's compliance with its obligations under this clause.

4. Independent Control Attestation and Testing. Archer shall employ independent third-party oversight as follows:

4.1. Attestation. At least annually and at its own expense, Archer shall ensure that an audit of data center facilities where Archer stores, processes, or transmits Client Content 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 Client 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 Archer Applications is available to Client. Archer shall make such Audit Report available under a separate non-disclosure agreement mutually agreed upon by them.

4.2. 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 Archer Applications and upon Client's reasonable request, Archer shall provide a copy of the most recent executive summary regarding such testing.

4.3. Follow-up Inquiries. For clarification and the avoidance of doubt, to the extent such information has not otherwise been made available to Client, Client has the right to request clarifying information related to: Audit Reports; Archer's good faith answers to previously-answered industry standard questionnaires; executive summaries of third-party penetration testing reports related to the Archer Applications; vulnerabilities of which the public is generally aware (such as zero-day vulnerabilities); and questions posed by regulators in accordance with applicable law which are not addressed by the foregoing ("**Follow-Up Inquiries**"). Follow-up Inquiries must be made in writing by Client, and Archer will use commercially reasonable efforts to respond to Follow-up Inquiries in a timely manner given the nature and scope of such Follow-up Inquiries. Notwithstanding the foregoing, in no event shall Archer be obligated to disclose information Archer reasonably deems: Archer proprietary information; information beyond the scope of the Archer Applications as it relates to Client; or information related to an ongoing (i.e., not yet remediated) security concern where the disclosure of such information has the potential to lead to a Security Incident.

5. Data Security. Archer shall use commercially reasonable efforts to carry out the following procedures to manage Client Content as follows:

5.1. Information Classification and Logical Separation. If Client discloses Client Content to Archer or if Archer accesses Client Content as permitted by the Agreement, Archer shall classify Client Content as Confidential and handle it in accordance with the terms hereof. Archer will have no visibility at upload into the types of information stored on the Archer Applications by Client. Client Content shall be logically separated such that there is no co-mingling of Client Content with that of any other Archer Clients.

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

5.3. 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 Archer protects Client Content against unauthorized access or destruction. If Archer uses public key infrastructure (PKI), Archer shall protect it by 'hardening' the underlying operating system(s) and restricting access to certification authorities.

5.4. Data Access; **Transmission**. Archer shall make Archer-controlled applications and systems used to process or store Client 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, Archer shall protect Client Content using appropriate cryptography.

5.5. Event Logging.[1] For systems directly providing the Archer Applications to Client, Archer shall maintain logs of key events that may affect the confidentiality, integrity, and/or availability of the Archer Applications to Client and that may assist in the identification or investigation of material incidents and/or security breaches occurring in relation to Archer systems. Archer shall retain the logs for at least 90 days and protect them against unauthorized changes (including, amending or deleting a log). Archer will monitor and log all system access to the Archer Applications to produce a forensic trail that includes, but is not limited to, web server logs, application logs, system logs, and network event logs, as applicable to the Archer Application(s). Such logs are Archer confidential information, but Archer will disclose them as necessary to comply with applicable law.

5.6. Disposition of Client Content. In the event of termination of the Archer Application(s), Archer shall use industry standard techniques (such as those detailed by NIST 800-88) designed to prevent unauthorized individuals from accessing Client Content as part of the decommissioning process.

6. Computer & Network Security. Archer shall use commercially reasonable efforts to carry out the following procedures to protect Client Content:

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

6.2. Internal Network Segment Security. Data entering the Archer Application's network from external sources shall pass through Firewalls to enforce secure connections between internal and external systems.

6.3. External Network Segment Security. The Archer Application's connections to the Internet shall (a) have appropriate security measures and controls applied, and (b) the Archer SaaS, Archer Engage, and Archer Insight applications 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.

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

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

- **User IDs.** Archer shall assign each user of a system containing Client Content a unique identification code ("**User ID**").
- **Passwords**. Each user of a system containing Client Content shall use a unique password whose length, complexity, and age should be governed in accordance with industry best practices.
- **Two-Factor Authentication for Remote Access**. Remote access to systems containing Client Content shall require the use of two-factor authentication.

[1] For Engage for Vendors, Engage for Business Users, and Archer Insight, where Client utilizes Incidental Software (if any) in connection with the Archer Application(s), Client is responsible for monitoring and logging the use of the Incidental Software that is under Client's control.

- **Deactivation**. Archer shall automatically deactivate User IDs after a technologically enforced number of unsuccessful log-in attempts. Archer shall restrict or time out interactive sessions after a technologically enforced period of inactivity. Archer shall promptly deactivate User IDs for Archer Personnel with access to Client Content upon changes in job responsibilities that render such access unnecessary and during termination of employment.

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

6.7. Malware Protection. Archer will install and run industry standard malware protection on all systems underlying Archer Applications. Archer shall regularly update anti-malware definition files in accordance with industry standards. For the avoidance of doubt, Client remains responsible for protecting its own systems by installing, updating, and maintaining industry standard malware protection. For Engage for Vendors, Engage for Business Users, and Archer Insight, Client is responsible for malware protection on all systems underlying the Incidental Software (if any) that is under Client's control.

7. System Development.

7.1. Development Methodology and Installation Process.

- **Documented Development Methodology**. Archer shall ensure that development activities for Archer-developed software used to provide the Archer Applications are carried out in accordance with a documented system development methodology.
- **Documented Deployment Process**. Archer shall ensure that new systems and changes to existing systems used in the provision of the Archer Applications are deployed in accordance with a documented process.

7.2. 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 Archer promotes applicable system changes to the production environment.

7.3. Client Content in Test Environments. Archer shall ensure that Client Content is not used within Archer test environments without Client's prior written approval.

7.4. Secure Coding Practices. Archer shall have secure development practices for itself and require the same of its coding vendors, if any, including the definition, testing, deployment, and review of security requirements.

8. General Security.

8.1. Point of Contact. Archer shall designate an account manager with whom Client may coordinate as an escalation point beyond typical Archer Applications Client support avenues available to Client.

8.2. Data Center Facilities. Archer Applications 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. Archer will supply and maintain adequate heating/cooling; electrical power; server hardware; network infrastructure and bandwidth; physical security and access controls; and professional fire detection/suppression capability necessary to provide the Archer Applications. Additional requirements specific to the data center facilities are:

- **Two-Factor Authentication**. Archer shall require two-factor authentication for entry on access points designed to restrict entry and limit access to certain highly sensitive areas.
- **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 Archer Applications.
- **CCTV Systems**. Archer shall use closed circuit television (CCTV) systems and CCTV recording systems to monitor and record access to controlled areas.

- **ID Badges**. Archer shall always issue and require identification badges showing the bearer's name, photographic likeness, and organization to which they belong at data center facilities.
- **Visitor Procedures**. Archer shall implement and follow procedures for validating visitor identity and authorization to enter the premises, 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.

8.3. 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 Archer Applications are tested, reviewed, approved, and applied by Archer using an industry standard change management process that accounts for risks to Archer, its Clients, and other such factors as Archer deems relevant. During the Subscription Term, Archer reserves the right to make modifications, including upgrades, patches, revisions or additions to the Archer Applications.

8.4. Archer Personnel.

- **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 Archer Applications under this Agreement, to the extent permitted by applicable law.
- **Training**. Archer Personnel involved in the provision of the Archer Applications 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 Archer Applications or prior to Archer Personnel being given access to Client Content.
- **Subcontractors**. Where applicable, Archer shall require subcontractors engaged in the provision of the Archer Application(s) (other than auxiliary services that facilitate the Archer Application(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.

9. Business Continuity Planning.

9.1. Archer shall ensure that the Archer Applications 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.

9.2. BCP Requirements. The BCP shall:

- Address the relocation of affected Archer Personnel to contingency locations and the reallocation of work;
- Require a remote contingency site with adequate security and capacity to provide the Archer Applications in accordance with the obligations of this Agreement;
- Require Processes designed to ensure that Archer automatically copies Client Content and other data necessary for the performance of the Archer Applications to a remote contingency site;
- Include a description of the recovery process Archer will implement following the occurrence of a disaster;
- Detail key resources and actions necessary to ensure that business continuity is maintained;
- Include a forty-eight (48) hour recovery time objective ("**RTO**") in which Archer shall recover the Archer Applications following the occurrence of a disaster; and
- Allow for the recovery of Client Content at the remote contingency site in accordance with a twenty-four (24) hour recovery point objective ("**RPO**").

9.3. BCP Testing. At least annually and at its own expense, Archer will conduct a test of the BCP. 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.

9.4. Backups. During the Term, Archer shall perform regular backups of Client Content to assist Archer in recovery of the Archer Application(s) in the event of a force majeure event affecting the Archer Application(s). For Engage for Vendors, Engage for Business Users, and Archer Insight where Client utilizes Incidental Software

(if any) in connection with the Archer Application(s), Client is responsible for backups of the Incidental Software that is under Client's control. The retention period for such backups shall be in accordance with Service Provider's backup retention policies, and Client remains responsible for reinstating backups to the extent loss of Client Content is not caused by Service Provider. All data back-ups will be encrypted and stored off-site. Archer SaaS and Archer Insight will retain daily data backups which will be stored/retained for a maximum period of 365 days. Engage for Vendors and Engage for Business Users will retain daily backups for thirty days.

9.5. BCP Activation.

- **Notification**. If Archer reasonably believes a force majeure event will adversely impact the Archer Applications or Archer's obligations under this Agreement, Archer shall, to the extent possible, promptly notify Client of such Force Majeure Event. Such notification shall, as soon as such details are known, contain:
  - A description of the force majeure event in question.
  - The impact the force majeure event is likely to have on the Archer Applications and Archer's obligations under this Agreement.
  - The operating strategy and the timetable for the utilization of the contingency site.
  - The timeframe in which Archer expects to return to business as usual.
  - Crisis management escalations affecting Client Content.

- **Contact Points**. Archer Client Support and/or Client's Archer account manager shall coordinate with Client'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. Client shall make sure that its representative is always known to Archer Client Support.