Auditoria Data Processing Addendum

This Data Processing Addendum (including all Schedules attached hereto, the "**DPA**") is incorporated into, and is subject to the terms and conditions of, the Auditoria Master Subscription Agreement or other written or electronic agreement ("**Agreement**") between Auditoria.AI, Inc. ("**Auditoria**") and the entity identified as "Customer" in the Agreement ("**Customer**"). This DPA applies to the extent Auditoria's Processing of Customer Personal Data is subject to the Data Protection Laws. This DPA shall be effective for the term of the Agreement.

1. Definitions

1.1. For this DPA:

1.1.1. "**CCPA**" means the California Consumer Privacy Act, the and their implementing regulations;

1.1.2. "**Controller**" means the entity which determines the purposes and means of the Processing of Personal Data;

1.1.3. "**Customer Personal Data**" means the Personal Data described under Schedule 1 to this DPA;

1.1.4. "**Data Protection Laws**" means all laws relating to data protection and privacy applicable to Auditoria's Processing of Customer Personal Data, including without limitation, the CCPA, the GDPR and member state laws implementing the GDPR, the United Kingdom's Data Protection Act 2018, and applicable privacy and data protection laws of any other jurisdiction, each as amended, repealed, consolidated or replaced from time to time;

1.1.5. "**Data Subjects**" means the individuals identified in Schedule 1;

1.1.6. "**EU SCCs**" means the Standard Contractual Clauses approved with Commission Implementing Decision (EU) 2021/914 of June 4, 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, as amended, supplemented, updated or replaced from time to time;

1.1.7. "**GDPR**" means the General Data Protection Regulation (EU) 2016/679 together with any national implementing laws in any member state of the EEA ("**EU GDPR**") and the EU GDPR as incorporated into the laws of the United Kingdom ("**UK GDPR**");

1.1.8. "**Personal Data**", "**Personal Data Breach**" and "**Processing**" will each have the meaning given to them in the Data Protection Laws. The term "Personal Data" includes "personal information," "personally identifiable information," and equivalent terms as such terms may be defined by the Data Protection Laws. The term "Personal Data Breach" includes equivalent terms as defined by the Data Protection Laws;

1.1.9. "**Processor**" means the entity which Processes Personal Data on behalf of the Controller;

1.1.10. "**Sell**" has the meaning given in the Data Protection Laws; and

1.1.11. "**UK SCCs**" means the Standard Contractual Clauses for controller to processor transfers set forth in the European Commission's decision (C(2010)593) of 5 February 2010.

1.2. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement.

2. Processing of Customer Personal Data

2.1. The parties acknowledge and agree that Customer is the Controller or Processor of Customer Personal Data and Auditoria is a Processor of Customer Personal Data. Auditoria will only Process Customer Personal Data as a Processor on behalf of and in accordance with Customer's prior written instructions, including any instructions provided through Customer's use of the Auditoria Solution. Auditoria is hereby instructed to Process Customer Personal Data to the extent necessary

to provide the Auditoria Solution as set forth in the Agreement and this DPA. Auditoria shall not (1) retain, use, or disclose Customer Personal Data other than as provided for in the Agreement, as needed to provide the Auditoria Solution, or as otherwise permitted by Data Protection Laws; or (2) Sell Customer Personal Data. Auditoria certifies that it understands and will comply with the restrictions contained in this Section 2.1.

2.2. Auditoria will immediately inform Customer if, in its opinion, an instruction from Customer infringes the Data Protection Laws.

2.3. The details of Auditoria's Processing of Customer Personal Data are described in Schedule 1.

2.4. If applicable laws preclude Auditoria from complying with Customer's instructions, Auditoria will inform Customer of its inability to comply with the instructions, to the extent permitted by law.

2.5. Each of Customer and Auditoria will comply with their respective obligations under the Data Protection Laws.

3. Cross-Border Transfers of Personal Data

3.1. With respect to Customer Personal Data originating from the European Economic Area ("**EEA**") or Switzerland that is transferred from Customer to Auditoria in the United States, the parties agree to comply with the general clauses and with "Module Two" (Controller to Processor) of the EU SCCs, which are incorporated herein by reference, with Customer as the "data exporter" and Auditoria as the "data importer."

3.2. For the EU SCCs the parties agree that:

3.2.1. In Clause 7, the optional docking clause will not apply;

3.2.2. In Clause 9, Option 2 will apply and the time period for prior notice of Sub-Processor changes will be as set forth in Section 5.1 of this DPA;

3.2.3. In Clause 11, the optional language will not apply;

3.2.4. In Clause 17, the EU SCCs shall be governed by the laws of Ireland;

3.2.5. In Clause 18(b), the parties agree to submit to the jurisdiction of the courts of Ireland;

3.2.6. In Annex I, Section A (List of Parties), (i) the data exporter's and the data importer's identity and contact details and, where applicable, information about their respective data protection officer and/or representative in the EEA are those set forth in the Agreement or as otherwise communicated by each party to the other party; (ii) Customer is a Controller and Auditoria is a Processor; (iii) the activities relevant to the data transferred under the EU SCCs relate to the provision of the Auditoria Solution pursuant to the Agreement; and (iv) entering into this DPA shall be treated as each party's signature of Annex I, Section A, as of the effective date of this DPA;

3.2.7. In Annex I, Section B (Description of Transfer): (i) Schedule 1 to this DPA describes Auditoria's Processing of Customer Personal Data; (ii) the frequency of the transfer is continuous (for as long as Customer uses the Auditoria Solution); (iii) Customer Personal Data will be retained in accordance with Clause 8.5 of the EU SCCs and this DPA; (iv) Auditoria uses the Sub-Processors identified at Schedule 3 hereto to support the provision of the Auditoria Solution.

3.2.8. In Annex I, Section C (Competent Supervisory Authority), the competent supervisory authority identified in accordance with Clause 13 of the EU SCCs is the competent supervisory authority communicated by Customer to Auditoria. Unless and until Customer communicates a competent supervisory authority to Auditoria, the competent supervisory authority shall be the Irish Data Protection Commission.

3.2.9. In Annex II, Auditoria has implemented and will maintain appropriate technical and organizational measures to protect the security, confidentiality and integrity of Customer Personal Data as described in Schedule 2.

3.3. If the transfer of Customer Personal Data is subject to the Swiss Federal Act on Data Protection, the parties agree to rely on the EU SCCs with the following modifications: (i) references to the 'GDPR' in the EU SCCs will be understood as references to the Swiss Federal Act on Data Protection insofar as the transfer of Customer Personal Data is subject to the Swiss Federal Act on Data Protection; (ii) the Federal Data Protection and Information Commissioner (FDPIC) will be the competent supervisory authority under Clause 13 of the EU SCCs; (iii) the parties agree to abide by the GDPR standard in relation to all Processing of Customer Personal Data that is governed by the Swiss Federal Act on Data Protection; and (iv) the term 'Member State' in the EU SCCs will not be interpreted in such a way as to exclude Data Subjects who habitually reside in Switzerland from initiating legal proceedings in Switzerland in accordance with Clause 18(c) of the EU SCCs.

3.4. With respect to transfers from Customer to Auditoria of Customer Personal Data originating from the United Kingdom, the parties agree to comply with the UK SCCs, which are incorporated herein by reference. The parties agree that, for the UK SCCs: (i) Customer is the "data exporter", and Auditoria is the "data importer"; (ii) all references to the "Directive 95/46/EC" and its provisions shall be deemed to refer to the relevant provisions of the UK GDPR and the Data Protection Act 2018 of the United Kingdom; (iii) all references to the "Commission" shall be deemed to refer to the Information Commissioner; (iv) all references to the "European Economic Area" or the "European Union" shall be deemed to refer to the United Kingdom; (v) for Appendix 1 to the UK SCCs, information about the exporter and importer, the categories of Data Subjects, types of Personal Data and type of Processing operations are as set out in Schedule 1 to this DPA; and (vi) for Appendix 2 to the UK SCCs, the security measures are as described in Schedule 2. The parties acknowledge that the Information Commissioner's Office has not yet approved new standard contractual clauses under the UK GDPR. The UK SCCs will apply only until the Information Commissioner's Office issues new standard contractual clauses under the UK GDPR. If the Information Commissioner's Office approves the EU SCCs for transfers from the UK, the parties agree that the EU SCCS as implemented by this DPA will be the mechanism to legitimize such transfers. Where necessary, the parties shall work together, in good faith, to enter into an updated version of the UK SCCs or negotiate an alternative solution to enable transfers of Customer Personal Data in compliance with Data Protection Laws.

4. Confidentiality and Security

4.1. Auditoria will require Auditoria's personnel who access Customer Personal Data to commit to protect the confidentiality of Customer Personal Data.

4.2. Auditoria will implement commercially reasonable technical and organisational measures, as further described Schedule 2, that are designed to protect against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data.

4.3. To the extent required by Data Protection Laws, Auditoria will provide Customer with reasonable assistance as necessary for the fulfilment of Customer's obligations under Data Protection Laws to maintain the security of Customer Personal Data.

5. Sub-Processing

5.1. Customer agrees that Auditoria may engage Sub-Processors to Process Customer Personal Data on Customer's behalf. Auditoria will inform Customer of any intended changes concerning the addition or replacement of Sub-Processors and Customer will have an opportunity to object to such changes on reasonable grounds within seven days after being notified. If the parties are unable to resolve such objection, either party may terminate the Agreement by providing written notice to the other party.

5.2. Auditoria will impose on its Sub-Processors substantially the same obligations that apply to Auditoria under this DPA. Auditoria will be liable to Customer for breaches of its Sub-Processors' obligations as it would be for its own.

5.3. The parties agree that the copies of the Authorized Sub-Processor agreements that must be provided by Auditoria to Customer pursuant to Clause 9(c) of the EU SCCs and Clause 5 of the UK

SCCs, if applicable, may have commercial information or clauses unrelated to the EU or UK SCCs removed by Auditoria beforehand; and, that such copies will be provided by Auditoria, in a manner to be determined in its discretion, only upon Customer's written request.

6. Data Subject Rights

Customer is responsible for responding to any Data Subject requests relating to Customer Personal Data ("Requests"). If Auditoria receives any Requests during the term, Auditoria will advise the Data Subject to submit the request directly to Customer or the appropriate Controller. Auditoria will provide Customer with self-service functionality or other reasonable assistance to permit Customer to respond to Requests.

7. Personal Data Breaches

Upon becoming aware of a Personal Data Breach affecting Customer Personal Data, Auditoria will (i) promptly take measures designed to remediate the Personal Data Breach and (ii) notify Customer without undue delay. Customer is solely responsible for complying with Personal Data Breach notification requirements applicable to Customer. At Customer's request, Auditoria will reasonably assist Customer's efforts to notify Personal Data Breaches to the competent data protection authorities and/or affected Data Subjects, if Customer is required to do so under the Data Protection Laws. Auditoria's notice of or response to a Personal Data Breach under this Section 7 will not be an acknowledgement or admission by Auditoria of any fault or liability with respect to the Personal Data Breach.

8. Data Protection Impact Assessment; Prior Consultation

Taking into account the nature of the Processing and the information available to Auditoria, Auditoria will reasonably assist Customer in conducting data protection impact assessments and consultation with data protection authorities if Customer is required to engage in such activities under applicable Data Protection Laws and such assistance is necessary and relates to the Processing by Auditoria of Customer Personal Data.

9. Deletion of Customer Personal Data

Customer instructs Auditoria to delete Customer Personal Data within 30 days of the termination of the Agreement and delete existing copies unless applicable law requires otherwise. The parties agree that the certification of deletion described in Clause 8.5 of the EU SCCs and Clause 12 of the UK SCCs, if applicable, shall be provided only upon Customer's written request. Notwithstanding the foregoing, Auditoria may retain Customer Personal Data to the extent and for the period required by applicable laws provided that Auditoria maintains the confidentiality of all such Customer Personal Data and Processes such Customer Personal Data only as necessary for the purpose(s) specified in the applicable laws requiring its storage.

10. Audits

10.1. Customer may audit Auditoria's compliance with its obligations under this DPA up to once per year. In addition, Customer may perform more frequent audits (including inspections) in the event: (1) Auditoria suffers a Personal Data Breach affecting Customer Personal Data; (2) Customer has genuine, documented concerns regarding Auditoria's compliance with this DPA or the Data Protection Laws; or (3) where required by the Data Protection Laws, including where mandated by regulatory or governmental authorities with jurisdiction over Customer Personal Data. Auditoria will contribute to such audits by providing Customer or Customer's regulatory or governmental authority with the information and assistance reasonably necessary to conduct the audit, including any relevant records of Processing activities applicable to the Auditoria Solution, as described below.

10.2. To request an audit, Customer must submit a detailed proposed audit plan to privacy@Auditoria.ai at least one month in advance of the proposed audit start date. The proposed audit plan must describe the proposed scope, duration, start date of the audit, and the identity of any third party Customer intends to appoint to perform the audit. Auditoria will review the proposed audit plan and provide Customer with any concerns or questions (for example, Auditoria may object to the third party auditor as described in Section 10.3, provide an Audit Report as described in Section 10.4,

or identify any requests for information that could compromise Auditoria confidentiality obligations or security, privacy, employment or other relevant policies). The parties will negotiate in good faith to agree on a final audit plan at least two weeks in advance of the proposed audit start date.

10.3. Auditoria may object to third party auditors that are, in Auditoria's reasonable opinion, not suitably qualified or independent, a competitor of Auditoria, or otherwise manifestly unsuitable. Customer will appoint another auditor or conduct the audit itself if the parties cannot resolve the objection after negotiating in good faith.

10.4. If the requested audit scope is addressed in an SSAE 16/ISAE 3402 Type 2, ISO, NIST or similar audit report performed by a qualified third party auditor on Auditoria's systems that Process Customer Personal Data ("Audit Reports") within twelve (12) months of Customer's audit request and Auditoria confirms there are no known material changes in the controls audited, Customer agrees to accept the Audit Report in lieu of requesting an audit of the controls covered by the Audit Report.

10.5. The audit must be conducted at a mutually agreeable time during regular business hours at the applicable facility, subject to the agreed final audit plan and Auditoria's health and safety or other relevant policies and may not unreasonably interfere with Auditoria business activities and shall be subject to terms Auditoria may reasonably impose to protect its operations and the confidentiality of its information and the information of third parties to whom Auditoria owes an obligation of confidentiality.

10.6. Any audits are at Customer's expense. Customer will promptly disclose to Auditoria any perceived non-compliance or security concerns discovered during the audit, together with all relevant details.

10.7. The parties agree that the audits described in Clause 8.9 of the EU SCCs and Clause 5(f) of the UK SCCs, if applicable, shall be performed in accordance with this Section 10.

11. Liability

11.1. Each party's liability towards the other party under or in connection with this DPA will be limited in accordance with the provisions of the Agreement.

11.2. Customer acknowledges that Auditoria is reliant on Customer for direction as to the extent to which Auditoria is entitled to Process Customer Personal Data on behalf of Customer in performance of the Auditoria Solution. Consequently, Auditoria will not be liable under the Agreement for any claim brought by a Data Subject arising from (a) any action or omission by Auditoria in compliance with Customer's instructions or (b) from Customer's failure to comply with its obligations under the Data Protection Laws.

12. General Provisions

With regard to the subject matter of this DPA, in the event of inconsistencies between the provisions of this DPA and the Agreement, the provisions of this DPA shall prevail. In the event of inconsistencies between the DPA and the EU or UK SCCs, the EU OR UK SCCs will prevail.

CUSTOMER	**Auditoria**
By: Role:	By: Robert Mally Title: CFO Auditoria.ai, Inc.

SCHEDULE 1

Details of Processing

1. **Categories of Data Subjects**. This DPA applies to Auditoria's Processing of Customer Personal Data relating to Customer's employees, contractors, and end users of the Auditoria Solution ("Data Subjects").
2. **Types of Personal Data**. The extent of Customer Personal Data Processed by Auditoria is determined and controlled by Customer in its sole discretion and includes names, contact information, e-mail address, and any other Personal Data that may be transmitted through the Auditoria Solution by Data Subjects.
3. **Subject-Matter and Nature of the Processing**. Customer Personal Data will be subject to the Processing activities that Auditoria needs to perform in order to provide the Auditoria Solution pursuant to the Agreement.
4. **Purpose of the Processing**. Auditoria will Process Customer Personal Data for purposes of providing the Auditoria Solution as set out in the Agreement.
5. **Duration of the Processing**. Customer Personal Data will be Processed for the duration of the Agreement, subject to Section 9 of the DPA.

SCHEDULE 2

Security Overview

1. Purpose. Auditoria is committed to maintaining customer trust. The purpose of this Security Overview is to describe the security program for the Auditoria Solution. This Security Overview describes the minimum security standards that Auditoria maintains in order to protect Customer Personal Data from unauthorized use, access, disclosure, theft, or manipulation. As security threats shift and evolve, Auditoria continues to update its security program and strategy to help protect Customer Personal Data. Auditoria reserves the right to update this Security Overview from time to time; provided, however, any update will not materially reduce the overall protections set forth in this Security Overview. Any capitalized term not defined in this Security Overview will have the meaning given in the Agreement or the DPA.

2. Auditoria Solution Covered. This Security Overview describes the architecture, administrative, technical and physical controls as well as third party security audit certifications that are applicable to the Auditoria Solution.

3. Security Organization & Program. Auditoria maintains a risk-based assessment security program. The framework for Auditoria's security program includes administrative, technical, and physical safeguards reasonably designed to protect the confidentiality, integrity, and availability of Customer Personal Data. Auditoria's security program is intended to be appropriate to the nature of the Auditoria Solution and the size and complexity of Auditoria's business operations. Auditoria's security framework includes programs covering: Policies and Procedures, Asset Management, Access Management, Cryptography, Physical Security, Operations Security, Communications Security, Business Continuity Security, People Security, Product Security, Cloud and Network Infrastructure Security, Security Compliance, Third-Party Security, Vulnerability Management, as well as Security Monitoring and Incident Response. Information security policies and standards are reviewed and approved by management at least annually and are made available to all Auditoria employees for their reference.

4. Confidentiality. Auditoria has controls in place to maintain the confidentiality of Customer Personal Data that Customer makes available to the Auditoria Solution, in accordance with the Agreement. All Auditoria employees and contract personnel are bound by Auditoria's internal policies regarding maintaining confidentiality of Customer Personal Data and contractually commit to these obligations.

5. People Security.

5.1. *Employee Background Checks*. Auditoria carries out background checks on individuals joining Auditoria in accordance with applicable local laws. Auditoria currently verifies the individual's education and previous employment, and also carries out reference checks. Where local labor law or statutory regulations permit, and dependent on the role or position of the prospective employee, Auditoria may also conduct criminal, credit, immigration, and security checks.

5.2. *Employee Training*. At least once a year, all Auditoria employees must complete the Auditoria security and privacy training which covers Auditoria's security policies, security best practices, and privacy principles. Employees on a leave of absence may have additional time to complete this annual training.

6. Third Party Auditoria Management.

6.1. *Auditoria Assessment*. Auditoria may use third party vendors to provide the Auditoria Solution. Auditoria carries out a security risk-based assessment of prospective vendors before working with those vendors to validate that prospective vendors meet Auditoria's security requirements. Auditoria periodically reviews each third party in light of Auditoria's security and business continuity standards, including the type of access and classification of data being accessed (if any), controls necessary to protect data, and legal/regulatory requirements. Auditoria ensures that Customer Personal Data is returned and/or deleted at the end of an Auditoria relationship. For the avoidance of doubt, third-party services that Customer chooses to integrate via the Auditoria Solution are not considered subcontractors of Auditoria.

6.2. *Auditoria Agreements*. Auditoria enters into written agreements with all of its vendors which include confidentiality, privacy and security obligations that provide an appropriate level of protection for the personal data contained within the Customer Personal Data that these vendors may process.

7. Security Certificates.

7.1. *AWS Certifications*. The Auditoria Solution uses and leverages Amazon Web Services ("AWS") data centers, with a reputation of being highly scalable, secure, and reliable. Information about AWS audit certifications are available at the AWS Cloud Security website https://aws.amazon.com/security/.

8. Architecture and Data Segregation. The cloud communication platform for the Auditoria Solution is hosted by AWS. The current location of the AWS data center infrastructure used in providing the Auditoria Solution is located in the United States. Further information about security provided by AWS is available from the AWS security webpage available at https://aws.amazon.com/security/. Auditoria separates Customer Personal Data using logical identifiers tagging all communications data with the associated Customer ID to clearly identify ownership. Auditoria's APIs are designed and built to designed and built to identify and allow access only to and from these tags and enforce access controls to ensure the confidentiality and integrity requirements for each Customer are appropriately addressed. These controls are in place so one customer's communications cannot be accessed by another customer.

9. Physical Security.

9.1. AWS data centers that host the Auditoria Solution are strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff. These facilities are designed to withstand adverse weather and other reasonably predictable natural conditions. Each data center has redundant electrical power systems that are available twenty-four (24) hours a day, seven (7) days a week. Uninterruptible power supplies and on-site generators are available to provide back-up power in the event of an electrical failure. In addition, Auditoria headquarters and office spaces have a physical security program that manages visitors, building entrances, CCTVs (closed circuit television), and overall office security. All contractors and visitors are required to wear identification badges.

10. Security by Design. The Auditoria's Software Development Lifecycle (SDLC) standard defines the process by which Auditoria creates secure products and the activities that the product teams must perform at different stages of development (requirements, design, implementation, and deployment). Auditoria engineers perform numerous security activities for the Auditoria Solution including:

10.1. internal security reviews before products are launched;

10.2. periodic penetration tests performed by independent third-party contractors; and

10.3. conduct threat models for the Auditoria Solution including documenting any detection of attacks.

11. Access Controls.

11.1. *Provisioning Access*. To minimize the risk of data exposure, Auditoria follows the principles of least privilege when provisioning system access. Auditoria personnel are authorized to access Customer Personal Data based on their job function, role and responsibilities, and such access requires approval of the employee's manager. Access rights to production environments are reviewed at least semi-annually. An employee's access to Customer Personal Data is promptly removed upon termination of their employment. Before an Auditoria employee is granted access to the production environment, access must be approved by management and the employee is required to complete internal trainings for such access including trainings on the relevant team's systems. Auditoria logs high risk actions and changes in the production environment. Auditoria

leverages automation to identify any deviation from internal technical standards that could indicate anomalous/unauthorized activity to raise an alert within minutes of a configuration change.

11.2. *Password Controls*. Auditoria's current policy for employee password management follows a strict password standard, and as such, our policy is to use longer passwords, with multi-factor authentication but not require frequent changes. The Auditoria Solution supports Single Sign On as well as application based custom authentication. In the case when custom authentication mechanism is leveraged, the Auditoria solution stores Customer passwords in encrypted form.

12. Change Management. Auditoria has a formal change management process to manage changes to software, applications and system software that will be deployed within the production environment. Change requests are documented using a formal, auditable, system of record. Prior to a high-risk change being made, an assessment is carried out to consider the impact and risk of a requested change, evidence acknowledging applicable testing for the change, approval of deployment into production by appropriate approvers(s) and roll back procedures. A change is reviewed and tested before being deployed to production.

13. Encryption. For the Auditoria Solution, Auditoria's cloud platform supports TLS 1.2/1.3 to encrypt network traffic transmitted between a Customer application and Auditoria's cloud infrastructure. When supported by integrations selected by Customer, Auditoria's cloud platform will also encrypt network traffic between Auditoria's cloud infrastructure and the integration provider. All Customer Personal Data is stored encrypted using 256-bit Advanced Encryption Standard (AES-256).

14. Vulnerability Management. Auditoria maintains controls and policies to mitigate the risk from security vulnerabilities in a measurable time frame that balances risk and the business/operational requirements. Auditoria uses a third-party tool to conduct vulnerability scans regularly to assess vulnerabilities in Auditoria's cloud infrastructure and corporate systems. Critical software patches are evaluated, tested and applied proactively.

15. Penetration Testing. Auditoria performs penetration tests and engages independent third-party entities to conduct application-level penetration tests. Results of penetration tests are prioritized, triaged and remediated promptly by Auditoria's engineering team.

16. Security Incident Management. Auditoria maintains security incident management policies and procedures in accordance with industry standards and best practices. Auditoria assesses the threat of all relevant vulnerabilities or security incidents and establishes remediation and mitigation actions for all events. Auditoria utilizes AWS platforms and third-party tools to detect, mitigate, and to help prevent Distributed Denial of Auditoria Solution (DDoS) attacks.

17. Discovery, Investigation and Notification of a Security Incident. Upon discovery or notification of any Security Incident, Auditoria will:

17.1. promptly investigate such Security Incident;

17.2. to the extent that is permitted by applicable law, promptly notify Customer.

18. Resilience and Auditoria Solution Continuity. Auditoria infrastructure for the Auditoria Solution uses a variety of tools and mechanisms to achieve high availability and resiliency. For the Auditoria Solution, Auditoria's infrastructure spans multiple fault-independent AWS availability regions. For the Auditoria Solution, there are manual or automatic capabilities to re-route and regenerate hosts within Auditoria's infrastructure. Auditoria leverages specialized tools that monitor server performance, data, and traffic load capacity within each availability zone.. Auditoria will also be notified immediately and have the ability to take prompt action to correct the cause(s) behind these issues.

19. Backups and Recovery. Auditoria performs regular backups of the Auditoria Solution account information, message templates, message logs and other critical data using AWS cloud storage. Backup data are retained redundantly across availability zones and are encrypted in transit and at rest using 256-bit Advanced Encryption Standard (AES-256) server-side encryption.

Schedule 3

Subprocessors

Auditoria maintains its list of subprocessors at https://www.auditoria.ai/auditoria-subprocessors/