DATA PROCESSING ADDENDUM

Last Update: **22 July 2025**

1. INTRODUCTION

1.1. This Data Processing Addendum, including its appendices, ("**this DPA**") is between Aultech (Pty) Ltd ("**Aultech**") and the party identified as the customer ("**the Customer**") in the Aultech Services Agreement.

1.2. This DPA is incorporated into and forms part of the Services Agreement between the Parties, which requires the Processing of Personal Data provided by the Customer to Aultech.

1.3. This DPA adds supplementary requirements to the Services Agreement in respect of the Processing of the Customer Data and clarifies the relationship between Aultech and the Customer in terms of Data Protection Laws.

1.4. All capitalised terms used but not defined in this DPA will bear the meaning set out in the Services Agreement.

2. DEFINITIONS AND INTERPRETATION

2.1. In this DPA, unless clearly inconsistent with or otherwise indicated by the context:

2.1.1. "**this DPA**" means this Data Processing Addendum and any appendices hereto;

2.1.2. "**Controller**" means any person, organisation, or entity that determines the purposes and means of the processing of Personal Information, as defined under Data Protection Laws, irrespective of terminological differences (i.e. a 'responsible party' under POPIA);

2.1.3. "**Customer Data''** means the Personal Data contained within the Customer Content, made available to and/or processed by Aultech as a Processor, as described in Appendix 1 of this DPA; but excludes permanently and irreversibly anonymised data. Customer Data excludes data processed solely within sandbox or beta environments unless the Customer has activated such features via their platform configuration;

2.1.4. "**Data Protection Laws**" means all applicable local, national or international laws and regulations which relate to the protection or processing of the Personal Data in question, including, where applicable, EU/UK Data Protection Laws as amended or superseded from time to time;

2.1.5. "**Services Agreement**" means Aultech's Services Agreement for the provision of various enterprise SaaS tools and AI-driven solutions, entered into between the Customer and Aultech, and in terms of which Aultech Processes the Customer Data on the Customer's behalf to provide the Services;

2.1.6. "**EU Data Protection Laws**" means:

(a). all EU regulations applicable (in whole or in part) to the processing of Personal Data (such as Regulation (EU) 2016/679 (the "EU GDPR"));

(b). the national laws of each European Economic Area ("EEA") member state implementing any EU directive applicable (in whole or in part) to the processing of Personal Data (such as Directive 2002/58/EC); and

(c). any other national laws of each EEA member state applicable (in whole or in part) to the processing of Personal Data.

2.1.7. "**Non-Adequate Country**" means a country that is not considered by the European Commission or the Controller, to ensure an adequate level of protection of Personal Information, such that any transfer of Personal Information to that country is a Restricted Transfer

2.1.8. "**Personnel**" means any:

(a). director, employee, or other person who works (permanently or temporarily) under either party's supervision; or

(b). person who renders services to either Party for purposes of fulfilling their obligations under this DPA as their agent, consultant, contractor, or other representative;

2.1.9. "**POPIA**" means the Protection of Personal Information Act, 4 of 2013, as amended;

2.1.10. "**Processor**" means any entity that processes Personal Data on behalf of a Controller, in accordance with Data Protection Laws, irrespective of terminological differences (i.e. a 'operator' under POPIA);

2.1.11. "**Regulator**" means any competent regulatory authority, government body, or other legal entity responsible for overseeing and enforcing Data Protection Laws within the RSA or any other applicable jurisdiction. This includes, but is not limited to, the Information Regulator of RSA, and extends to any similar entities with authority over the parties, the Data, or the activities described under the Services Agreement;

2.1.12. "**Restricted Transfer**" means a transfer of Personal Information outside of the EEA, the UK, the RSA, or any other country or jurisdiction, which requires further steps to be taken under Data Protection Laws;

2.1.13. "**RSA**" means Republic of South Africa;

2.1.14. "**Security Incident**" means any confirmed breach of security that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Customer Data processed by Aultech and/or its Sub-Processors in connection with the provision of the Services;

2.1.15. "**Services**" shall have the same meaning as set out in the Services Agreement;

2.1.16. "**Standard Contractual Clauses**" means (i) the relevant module of the standard contractual clauses for the transfer of Personal Information to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, implemented through Commission Implementing Decision (EU) 2021/914 of 4 June 2021("**EU SCCs**"), and (ii) where the UK GDPR applies, the 'International Data Transfer Addendum' to the EU SCCs issued by the Information Commissioner ("ICO") under s.119A(1) of the Data Protection Act 2018 ("**UK Addendum**"), or UK International Data Transfer Agreement ("**UK IDTA**") issued by the ICO, as may be revised from time to time; and (iii) where POPIA only applies, a written agreement substantially similar to the UK IDTA;

2.1.17. "**Sub-Processor**" means an Aultech Affiliate or third party authorised as another processor under this DPA to process Customer Data to support, provide or enable the provision of the Services;

2.1.18. "**UK Data Protection Laws**" means all laws relating to data protection, the processing of Personal Data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR, Data Protection Act 2018 and Privacy and Electronic Communications (EC Directive) Regulations 2003;

2.1.19. "**UK GDPR**" means the EU GDPR as amended and incorporated into UK law under the UK European Union (Withdrawal) Act 2018, and applicable secondary legislation made under that Act.

2.2. The terms **"Data Subject**", "**Personal Data**", "**Process**", "**Processing**", and "**Special Personal Data**" as used in this DPA will have the same meanings as defined by Data Protection Law or, absent any such meaning or law, by the EU Data Protection Law.

2.3. In this DPA, unless the context otherwise requires:

2.3.1. the appendices attached to this DPA shall be incorporated into and form part of this DPA;

2.3.2. the Standard Contractual Clauses (when they are incorporated into this DPA by reference in accordance with its terms) will be deemed to be an integral part of this DPA.

2.3.3. any phrase introduced by the terms "including", "include", "in particular" or any similar expression shall be construed as illustrative and shall not limit the sense of the words introduced by those terms.

2.4. In case of any conflicts concerning any provisions in respect of Personal Data, the following order of precedence shall apply to the extent necessary to resolve the conflict in interpretation:

2.4.1. Standard Contractual Clauses;

2.4.2. This DPA;

2.4.3. Services Agreement.

3. APPLICATION

3.1. This DPA applies when Aultech processes Customer Data on the Customer's behalf for specific activities as set out in the Services Agreement and to achieve the Customer's purposes described in Appendix 1 of this DPA.

3.2. This DPA will come into effect on the effective date of the Services Agreement and will replace any terms previously applicable to the processing and security of Customer Data.

3.3. Regardless of whether the Services Agreement has terminated or expired, this DPA will remain in effect until, and automatically expire when, Aultech deletes all Customer Data as described in this DPA.

4. RELATIONSHIP OF THE PARTIES AND INSTRUCTIONS TO PROCESS

4.1. **Aultech as Processor**. The Customer acts as the Controller and appoints Aultech as its Processor to process Customer Data on behalf of, and in accordance with, the Customer's instructions. The Customer will not instruct Aultech to process Customer Data in violation of any applicable law. Aultech will notify the Customer if it becomes aware that, in Aultech's opinion, an instruction from the Customer may infringe any Data Protection Laws (which shall not be construed as legal advice).

4.2. The Services Agreement, this DPA and Customer's configuration of their platform profile settings (as Customer may be able to modify from time to time), constitute the Customer's complete and final instructions to Aultech regarding the processing of Customer Data, unless otherwise agreed in writing.

4.3. **Processing instructions**. The Customer instructs Aultech to only process the Customer Data:

4.3.1. on the Customer's documented instructions;

4.3.2. to the extent necessary to perform its obligations under the Services Agreement;

4.3.3. to provide the Services to the Customer; and

4.3.4. as otherwise agreed to in writing.

4.4. The Customer acknowledges that the Services provided are not intended for the storage or use of non-business related correspondence. The Customer shall be solely responsible for determining all categories and types of Customer Data it submits and transfers to Aultech through the Service. The Customer understands that access to beta or early access features is optional, provided on an 'as-is' basis, and subject to separate or supplementary terms, which may include additional risk warnings

4.5. **Controller's warranties**. The Customer warrants that it has, and will maintain for the duration of the Services Agreement:

4.5.1. all the necessary rights to provide the Customer Data to Aultech for the processing to be performed in relation to the Services; and

4.5.2. one (1) or more legal justifications set out in Data Protection Laws support the lawfulness of the processing to be performed by Aultech.

4.6. **Restrictions on use**. The Customer acknowledges that the Output generated by the Services is unsuitable for, and must not be used for, punitive purposes, disciplinary action, or employment termination decisions. The Customer warrants that it will use the Output solely to support and enhance customer services and training purposes, and not for selection or exclusion purposes. Any reports derived from the Output and shared with management are intended exclusively for coaching, performance improvement, and training enhancement.

5. CONFIDENTIALITY

5.1. **Treat Personal Data as confidential**. Aultech will treat all Customer Data as confidential in accordance with the terms of the Services Agreement.

5.2. **Inform Personnel of confidentiality**. Aultech will inform all its approved Sub-Processors or Personnel engaged in Processing the Customer Data of its confidential nature.

5.3. **Access Control**. The Service Provider must limit access to the Customer Data to those Personnel who need to know or access the relevant information as strictly necessary to render the Services (i.e., only authorised persons).

5.4. **Authorised persons confidentiality**. All Aultech Personnel handling Customer Data must be subject to confidentiality agreements or otherwise be bound by appropriate statutory obligations of confidentiality.

5.5. **Training**. Aultech must ensure their Personnel have received training and know how to handle Personal Information appropriately in accordance with its nature, volume, sensitivity and risk of harm to the Data Subject.

6. SECURITY AND AUDIT

6.1. **Data Security**. The Customer is responsible for the secure and appropriate use of the Service to ensure a level of security appropriate to the risk related to the Customer Data and agrees that compliance and security measures as set forth in this DPA are deemed sufficient safeguards for processing of any Customer Data that the Customer

provides to Aultech. These measures will include the security measures agreed upon between the parties in Appendix 2. Aultech may update these security measures from time to time, provided that such updates do not result in a material reduction of the security of the Services.

6.2. **Security policies**. The Customer and Aultech will each maintain and fully implement security policies that apply to Personal Data processing.

6.3. **Audits**. Subject to Clause 6.9 below, upon the Customer's written request, Aultech will allow for and contribute to 1 audit per year strictly for the sole purpose of assessing Aultech's compliance with this DPA, unless more frequent audits are required by law.

6.4. **Notice of audits**. The Customer's request for an audit must give at least 30 days' prior notice to Aultech.

6.5. **Audit terms**. The Customer may audit Aultech's premises and operations related to the Customer Data themselves or using a third-party auditor mutually agreed by both parties ("**Auditor**") who is bound by confidentiality obligations at least as protective as those contained in this DPA and the Services Agreement.

6.6. **Cooperation with audits**. Aultech will reasonably cooperate with these audits and provide the Customer or the Auditor with reasonable access to any documentation, data, certifications, reports, and records involved with Aultech's processing of the Customer Data.

6.7. **Access to information**. Aultech will provide the Customer or the Auditor with access to any information relating to the Customer Data processing as the Customer may reasonably require to audit Aultech's compliance with this DPA. The Customer or Auditor will not be entitled to receive any data or information pertaining to other customers of Aultech or any other Confidential Information of Aultech that is not directly relevant for the authorised purposes of the audit.

6.8. **Audit Costs**: All costs associated with all audits initiated by the Customer shall be borne solely by the Customer.

6.9. **Evidence of compliance**. Instead of submitting to an audit, Aultech may provide certifications or documents demonstrating adherence to an approved code of conduct recognised under Data Protection Laws or to a certification mechanism to demonstrate compliance with Data Protection Law requirements, provided that the code of conduct or certification mechanism also addresses the security requirements contained in Appendix 2.

6.10. **Corrective Action**. If any material non-compliance is identified by an audit, Aultech will take prompt action to correct such non-compliance.

7. USE OF SUB-PROCESSORS

7.1. **General written authorisation**. The Customer generally authorises Aultech to appoint any Sub-Processors in accordance with this clause. With respect to each Sub-Processor, Aultech will:

7.1.1. perform reasonable due diligence on the data privacy and security measures when selecting and appointing a Sub-Processor;

7.1.2. ensure the Sub-Processor can demonstrate compliance with Data Protection Laws;

7.1.3. ensure the Sub-Processor applies technical and organisational measures to ensure the security of Customer Data at standards equivalent to or higher than those measures set out in this DPA;

7.1.4. ensure the Sub-Processor has a proven track record and reputation for reliable and responsible data processing activities;

7.1.5. ensure the Sub-Processor is located in a jurisdiction that provides an adequate level of data protection or otherwise has a written contract ensuring appropriate safeguards are in place;

7.1.6. ensure that Data Subject rights can be exercised, fulfilled and enforced against the Sub-Processor under Data Protection Laws;

7.1.7. ensure that if the use of a Sub-processor involves a Restricted Transfer, it will guarantee that the Standard Contractual Clauses, or other legally valid cross-border transfer mechanism, are at all relevant times incorporated into the relevant agreement(s) between Aultech and the Sub-Processor; and

7.1.8. allow for audits and monitoring of their data processing activities to ensure compliance with the agreed-upon terms and data protection standards.

7.2. **Prior specific authorisation**. The Customer hereby approves Aultech's use of the Sub-Processors listed in Appendix 3 for the data processing activities related to the Services, including those used in delivering AI services, email agent functions, or document automation.

7.3. **Sub-Processor changes**. Whether generally or specifically authorised, Aultech shall inform the Customer of any intended addition or replacement of Sub-Processors and give the Customer at least 30 days' notice to object to such changes before implementing them. However, the Customer may only object to a new Sub-Processor based on reasonable grounds for concern that the Sub-Processor cannot meet Data Protection Law requirements.

7.4. **Valid objections**. In the event the Customer submits a valid objection to a new Sub-Processor, Aultech will use commercially reasonable efforts to provide the Customer with an alternative configuration or adjustment to the Service to avoid processing of Customer Data by the objected-to Sub-Processor. If Aultech determines, at its sole discretion, that it is unable to make available such change within a reasonable period, which will not exceed 30 (thirty) days from the date of the objection, either Party may upon written notice terminate, without penalty, the affected Service(s) and the Customer may request a pro-rated refund of the applicable Fees within a reasonable time.

7.5. **Processor remains liable**. Aultech remains fully liable to the Customer for any Sub-Processor's failure to perform their data protection obligations despite the Customer's authorisation, except where such failure arises from a Force Majeure Event.

7.6. **Processor's Sub-Processor obligations**. Aultech will make sure that the Sub-Processor is bound by data protection obligations compatible with those of Aultech under this DPA, supervise compliance with those obligations, and impose on its Sub-Processors the obligation to implement Appropriate technical and organisational measures in such a manner that the processing will meet the requirements of Data Protection Laws.

7.7. **Controller's verification right**. The Customer may make sure that Aultech has complied with its obligations that the Customer has imposed on them in conformity with this DPA by requesting that Aultech audit a third-party Sub-Processor or request proof of certification, providing confirmation that such an audit has occurred, or getting or helping the Customer get a third-party audit report concerning the third-party Sub-Processor's operations, where available.

8. RESTRICTED TRANSFERS

8.1. The Customer authorises Aultech to make Restricted Transfers to its Sub-Processors described in Appendix 2, solely for the limited purposes of carrying out the Services and as described in Appendix 2.

8.2. Aultech shall only carry out a Restricted Transfer in compliance with Data Protection Laws and shall implement appropriate safeguards to the extent necessary under such laws.

8.3. Where the EU Data Protection Laws apply to a Restricted Transfer that occurs between Aultech and a Sub-Processor located in a Non-Adequate Country, and no other valid transfer mechanism applies to such transfer under Data Protection Laws, then Module 3 (Processor to Processor) of the relevant EU SCCs will apply.

8.4. Where the UK Data Protection Laws apply to a Restricted Transfer that occurs between Aultech and a Sub-Processor located in a Non-Adequate Country, and no other valid transfer mechanism applies to such transfer under Data Protection Laws, the UK IDTA will apply.

8.5. Where the EU Data Protection Laws and UK Data Protection Laws both apply to Restricted Transfers between Aultech and a Sub-Processor located in a Non-Adequate Country, and no other valid transfer mechanism applies to such transfers under Data Protection Laws, the EU SCCs together with the UK Addendum will apply.

9. SECURITY INCIDENT MANAGEMENT

9.1. **Notification**. Aultech shall notify the Customer without undue delay upon becoming aware of a confirmed Security Incident involving the Customer Data, as required under Data Protection Laws.

9.2. **Content of Notification**. Aultech shall ensure that the notification, to the extent possible, includes:

9.2.1. a description of the nature of the Security Incident, including the categories and approximate number of Data Subjects and Personal Data records affected;

9.2.2. the contact details of Aultech's information officer or data protection officer;

9.2.3. a description of the likely consequences of the Security Incident; and

9.2.4. a description of measures taken or proposed by Aultech to mitigate any possible adverse effects.

9.3. Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

9.4. **Customer's instructions**. Aultech will act according to the Customer's reasonable instructions regarding the Security Incident and provide assistance as necessary to meet the Customer's regulatory obligations regarding such Security Incident notifications.

10. DATA SUBJECT RIGHTS

If Aultech receives a request from a Data Subject (such as for access, rectification or erasure), it will promptly redirect the request to the Customer, and will not respond further except per the Customer's documented instructions.

11. DELETION OF DATA ON TERMINATION

Unless prohibited by applicable law, all Customer Data shall be permanently deleted by Aultech within thirty (30) days, including within all backup environments within 180 days of deletion initiation Upon request, Aultech shall provide written certification to the Customer that it has complied fully with this clause, within 10 days of receiving such request.

12. ASSISTANCE TO CONTROLLER

12.1. Aultech will use its commercially reasonable endeavours to assist the Customer, within a reasonable time upon request, to:

12.1.1. assist the Customer in fulfilling its obligations to respond to Data Subject requests, such as those related to access, rectification, erasure, or restriction of processing;

12.1.2. assist the Customer with its obligations, under Data Protection Laws, related to the Processing performed by the Service Provider, including notifying Regulators and Data Subjects in the event of an actual Security Incident suffered by Aultech;

provided that the Customer will be responsible for reasonable costs Aultech incurs in providing this assistance.

12.2. Requests involving data processed solely in beta or sandbox environments may be limited in scope or fulfillment capacity due to system configuration

13. LIMITATION OF LIABILITY

The liability of each party under this DPA (including the Standard Contractual Clauses) shall be subject to the exclusions and limitations of liability set out in the Services Agreement.

14. INDEMNIFICATION

The Customer's obligation to indemnify Aultech and its Affiliates under this DPA (including the Standard Contractual Clauses) shall be governed by the indemnification terms set out in the Services Agreement.

15. AMENDMENT OR SUBSTITUTION OF THIS DPA

15.1. Aultech reserves the right to amend or substitute this DPA as it deems necessary to:

15.1.1. comply with Data Protection Laws, including any changes, updates, or new regulations that affect the processing of Personal Data; or

15.1.2. reflect changes in the Services provided by Aultech, including but not limited to modifications, enhancements, or discontinuations of features or functionalities.

15.2. Aultech shall provide the Customer with at least thirty (30) days' prior written notice of any material changes to this DPA. Such notice shall be provided following the corresponding provisions of the Services Agreement regarding material changes.

15.3. The amended or substituted DPA shall supersede and replace this version of the DPA in its entirety from its effective date onward.

16. GENERAL

16.1. The provisions of this DPA are severable. If any phrase, clause or provision is invalid or unenforceable in whole or in part, such invalidity or unenforceability will affect only such phrase, clause or provision, and the rest of this DPA will remain in full force and effect.

16.2. Aultech may amend this DPA from time to time to ensure compliance with Data Protection Laws or to reflect any intended changes in Aultech's processing activities. Updates to this DPA will become effective on the date they are published on Aultech's Website .

16.3. Any notice, letter or other communication contemplated by this DPA will be communicated in writing to the addresses set out in the Services Agreement.

16.4. The provisions of this DPA will endure to the benefit of and will be binding upon the parties and their respective successors and permitted assigns.

16.5. This DPA is governed by the laws of RSA.

16.6. Any disputes arising from or in connection with this agreement will be brought exclusively before the competent court of the jurisdiction specified in the relevant provisions of the Services Agreement or Standard Contractual Clauses, as may be applicable.

APPENDIX 1

Data Processing Description

This Appendix 1 forms part of this DPA and describes the processing that the Aultech will perform on behalf of the Customer.

Subject Matter and Duration of Processing

Aultech will process Personal Data to provide software services via its services (including, but not limited to Document Control, Scout, Bob Agentic AI, and other Aultech ecosystem tools. , as well as associated AI and cloud infrastructure. These services include project management, document automation, generative AI assistance, workflow management, and real-time analytics and insights.

Frequency of Processing

Customer Data will be processed continuously and on an ongoing basis as required to deliver the Services to the Customer during the Service Term (as defined in the Services Agreement). Retention Periods agreed in the Services Agreement will apply, unless configured otherwise by the Customer in the Services platform.

Nature and Purpose of Processing

The Processor will collect, store, transmit, analyse, and otherwise process Personal Data for the following purposes:

(a) Project and Workflow Management: Facilitating the creation, assignment, tracking, and management of tasks, documents, and workflows across project teams.
(b) Communication and Document Automation: Processing email data, attachments, calendar invites, and related metadata for centralised dashboard visibility, reporting, and automatic document generation.
(c) Generative Artificial Intelligence (GenAI): Using OpenAI and other models via Azure integrations to summarise communications, suggest tasks, generate letters or notices, and support legal drafting under Customer instruction.
(d) Identity Management and Authentication: Processing user profile information for authentication and secure access to services.
(e) Security Monitoring: Logging and reviewing system activity, access control, threat monitoring, and audit trailing.
(f) Service Improvement: Analysing anonymised and aggregated usage data to improve Aultech's products and services, with explicit consent where applicable.
(g) Customer Support and Issue Resolution: Providing support services, troubleshooting, and resolving technical or user-related issues.

Types of Personal Data Processed

The following types of Personal Data may be processed:

- Identification and Contact Data: Names, roles, job titles, unique identifiers, email addresses.
- Authentication Data: Usernames, passwords (hashed), login metadata.
- Communication and Content Data: Email messages, task comments, documents, attachments, calendar entries.
- Project and Workflow Data: Task names, due dates, status fields, metadata associated with workflows.
- AI Input and Output: Instructions, prompts, summaries, and AI-generated content, including data processed via the email agent functionality, predictive task alerts, and automated document generation workflows
- Usage Data: Logs, system access times, device identifiers, interactions with the platform.

Categories of Data Subjects

- **Customer's End Users:**
  - Individuals granted access to the Services by the Customer.
- **Representatives of Contractors, Suppliers, and clients of the Customer:**
  - Individuals whose information is included in tender documents, evaluations, and communications.
- **Other Individuals:**
  - Any other persons whose Personal Data is uploaded or processed within the platform by the Customer.

Special Categories of Data

- None is intended to be transferred unless the End User or Customer includes it unexpectedly in unstructured data. However, the Customer is responsible for ensuring that it does not upload special categories of data (e.g. health, political affiliation, children, biometrics) unless the Customer has a valid legal justification to do so, and the Services are configured to support such processing lawfully and securely. Customers enabling

Commented [MB1]: Model can distinguish business from personal. It will not process the personal correspondence. Mistakes are possible.

Commented [MB2R1]: Emphasise incidental processing

beta features must ensure those environments are not used to process Special Category Data unless explicitly supported.

Transfers to Sub-Processors

Aultech may engage Sub-Processors to deliver certain aspects of the Services, such as hosting providers or support services. Any Sub-Processors will process Personal Data strictly for the purposes of providing the Services (e.g., cloud hosting, support services, firewalls, analytics, and AI infrastructure). In each case, in compliance with this DPA and Data Protection Laws.

Aultech will ensure that:

- Sub-Processor Agreements: Sub-Processors are bound by written agreements that require them to provide at least the same level of data protection as required by this DPA and POPIA;
- Notification and Consent: The Customer is informed of and, where required, consents to the engagement of Sub-Processors in accordance with the terms of the DPA.

Supervisory Authority

The competent supervisory authority shall be the data protection authority of the jurisdiction in which the Data Subjects are primarily located. If no such authority exists or applies, the Information Regulator of South Africa shall be deemed the competent supervisory authority.

APPENDIX 2

Security Measures

This Appendix 2 forms part of the Data Processing Agreement ("**DPA**") and outlines the technical and organisational measures implemented by Aultech to protect Customer Data processed on behalf of the Customer in connection with the Services. Aultech is committed to continuously improving its security posture and is actively working towards certifications, with SOC 2 as a future objective.

For the most current and comprehensive information on Aultech's security measures, including updates on Aultech's progress towards certification, please refer to our Security Measures page on our trust portal or other designated Documentation as updated from time to time.

Approach to Security Measures

Aultech shall determine appropriate security measures based on:

- The type and sensitivity of the Personal Data processed (e.g., communications, documents, identity information).
- The context and volume of processing, including automated AI-driven processing, API usage, and collaboration features.
- The risk of harm in the event of loss or unauthorised access.

Controls are adapted to changes in processing context, threat landscape, and regulatory guidance.

Technical Measures

2.1 Encryption and Data Protection:

- TLS 1.2 or higher is used for all data transmissions.
- AES-256 or equivalent encryption is used for data at rest.
- Azure's native security controls are leveraged including disk encryption and key vaults.

2.2 Access Controls:

- Role-based access permissions are applied based on the least privilege principle.
- Multi-factor authentication (MFA) is enforced for administrator and privileged access.
- SSH key-based authentication is used for server access by technical teams.
- Unique login credentials are assigned to each authorised user.
- Access rights are reviewed periodically to ensure appropriateness.
- Access is revoked immediately upon termination of employment or engagement.

2.3 System Monitoring:

- Security information and event management (SIEM) tools monitor access, performance, and incident alerts.
- Elastic (within the ALG stack) is used for centralised log collection, indexed search, and reporting.
- Audit logs are retained for no less than 12 months.

2.4 Physical and Hosting Security:

- Hosting is limited to secure Azure and/or Terraco data centres in South Africa and the EU.
- Data centres enforce strict physical access controls, including keycards, biometrics, and CCTV.

2.5 Backup and Disaster Recovery:

- Daily encrypted backups are scheduled and stored redundantly in Azure.
- Backups are retained for 180 days and subject to regular integrity testing .
- Aultech maintains adisaster recovery plan annually to ensure recovery within reasonable timeframes.

2.6 Threat Detection:

- CrowdStrike is used for endpoint protection, including real-time threat detection and malware prevention.
- Microsoft Defender tools are enabled for integrated Azure threat analytics.
- Physical firewalls. Perimeter protection is supplemented by Cloudflare's network-level firewall and bot mitigation systems.

2.7 Software and Patch Management:

- Platform dependencies are containerised using Docker and managed via Kubernetes.
- Security updates and patches are deployed via CI/CD pipelines under version control.

2.8 Identity and Customer Access Management:

- Aultech uses its identity access management systems to authenticate customer identities.
- Customer Data is logically separated by account and access is strictly permissioned per user role.

2.9 Web Application Firewall:

- Aultech uses Cloudflare's Web Application Firewall (WAF) to monitor and filter HTTP traffic between external users and its cloud infrastructure.
- The WAF helps detect and block common web application attacks such as SQL injection, cross-site scripting (XSS), and bot-driven abuse.
- Protection profiles and rulesets are regularly reviewed and updated to reflect evolving threat landscapes and to maintain alignment with OWASP Top 10 vulnerabilities.
- WAF logs are integrated into Aultech's centralised log management platform for real-time threat detection and historical analysis.

Organisational Measures

3.1 Confidentiality:

- All employees and contractors are bound by written confidentiality undertakings.
- Personnel with access to Personal Data are trained on secure handling obligations.

3.2 Awareness and Training:

- Mandatory security awareness and data protection training is conducted for all relevant personnel.
- Additional, role-specific training is provided to engineering and support staff.

3.3 Policy and Governance:

- Aultech maintains policies covering data protection, information security, incident response, and acceptable use.
- Risk assessments are carried out for high-risk or high-volume processing activities.

3.4 Incident Response:

- Aultech maintains an incident response plan covering detection, containment, mitigation, and breach notification.
- Security incidents are logged and reviewed, and affected Customers will be notified without undue delay.

3.5 Disclosure and Data Minimisation Controls:

- Encryption is applied to data in transit and at rest.
- Full-disk encryption is enabled on company-issued devices.
- Use of removable media is restricted.
- Customer Data can be deleted upon request, in accordance with the DPA.

3.6 Availability and Redundancy:

- Redundant systems and backups support service continuity.
- Monitoring tools and automated alerts detect downtime or anomalies.

3.7 Third-Party Services and Sub-Processor Risk Management:

- Sub-Processors are vetted through commercially reasonable due diligence processes.
- Written contracts require sub-processors to maintain equivalent data protection safeguards.

APPENDIX 3

Sub-Processors

This Appendix 3 forms part of the Data Processing Addendum ("DPA") and lists the Sub-Processors engaged by Aultech (the "Processor") to process Customer Data on behalf of the Customer (the "Controller").

Sub-processor	Purpose	Location	Transfer Mechanism
Microsoft Corporation (Azure)	Hosting infrastructure, data storage, and AI platform integrations	South Africa / European Union	EU Adequacy / Local compliance
OpenAI, LL.C. (via Microsoft Azure)	Generative AI functionality, Custom logic-based email agent processing, processed within Azure enterprise scope	South Africa / European Union	EU Adequacy / Local compliance
Teraco	Physical co-location	South Africa	Not applicable
CrowdStrike Holdings, Inc.	Endpoint protection, breach detection and isolation	South Africa / Global	Global DPA / Data residency configurations
Netcash (Pty) Ltd	Debit order and subscription payment processing	South Africa	Not applicable
Cloudflare, Inc.	Web Application Firewall (WAF), DDoS protection, and secure content delivery	Global	Standard Contractual Clauses