SCHEDULE A

ZENNEY SECURITY SCHEDULE

Last Updated: 11 July 2026

1. Purpose

This Security Schedule describes the administrative, technical and organisational safeguards maintained by Zenney to protect Customer Data and support the secure delivery of the Services.

Zenney maintains commercially reasonable security measures designed to protect Customer Data against unauthorised access, use, disclosure, alteration, loss and destruction. Security measures may evolve over time to address changes in technology, security threats and operational requirements.

---

2. Security Principles

Zenney designs, develops and operates the Services using commercially reasonable security practices, including:

- Security by design;
- Least privilege access;
- Defence in depth;
- Risk-based security management;
- Continuous improvement.

Zenney regularly reviews its security practices and may modify security controls provided the overall level of security is not materially reduced.

---

3. Identity and Access Management

Zenney restricts access to Customer Data and production systems to authorised personnel who require access to perform their responsibilities.

Security controls may include:

- Role-based access control (RBAC);
- Least privilege access principles;
- Unique user accounts;
- Authentication controls;
- Multi-factor authentication where supported or appropriate;
- Prompt removal or modification of access when no longer required.

---

4. Customer Data Protection

Zenney implements commercially reasonable safeguards to protect Customer Data throughout its lifecycle.

These safeguards may include:

- Logical separation of Customer Data;
- Access restricted to authorised personnel;
- Confidential handling of Customer Data;
- Controls designed to prevent unauthorised access, disclosure or modification.

Customer retains ownership of Customer Data at all times.

---

5. Encryption

Data in Transit

Zenney uses industry-standard encryption protocols, where commercially reasonable, to protect Customer Data transmitted between users, integrations and the Services.

Data at Rest

Where commercially reasonable and technically supported, Customer Data stored by Zenney is protected using encryption or equivalent storage security controls appropriate to the deployment environment.

---

6. Infrastructure and Application Security

Zenney applies commercially reasonable security practices to the infrastructure and applications supporting the Services.

These practices may include:

- Secure software development practices;
- Code review and testing;
- Vulnerability assessment and remediation;
- Security patch management;
- Network and infrastructure security controls;
- Controlled deployment and change management.

Where the Services are deployed within Customer-controlled environments, Customer remains responsible for the security of that infrastructure unless otherwise agreed in writing.

---

7. AI Security

Where the Services utilise artificial intelligence, machine learning, semantic technologies, automation or software agents:

- Customer permissions continue to apply to AI features;
- AI features operate within Customer-authorised access controls;
- Identifiable Customer Data is not used to train foundation models made available to other customers;
- Aggregated, anonymised and de-identified information may be used to improve the Services, provided such information cannot reasonably identify Customer, any individual or Customer's Confidential Information;
- Customers remain responsible for reviewing and validating AI-generated Outputs before relying upon them.

---

8. Security Incidents

Zenney maintains procedures for identifying, investigating, responding to and remediating Security Incidents affecting the Services.

Zenney will notify affected Customers of a Security Incident involving Customer Data within 48 hours of confirming that a Security Incident has occurred.

Zenney may take any action reasonably necessary to contain, investigate or remediate a Security Incident, including temporarily restricting access to the Services where appropriate.

---

9. Customer Responsibilities

Customer is responsible for:

- Maintaining the security of Customer accounts and credentials;
- Managing user permissions and access rights;
- Protecting Customer-controlled devices, networks and infrastructure;
- Ensuring connected third-party systems are appropriately secured;
- Ensuring Customer Data has been lawfully collected and provided to Zenney;
- Reviewing and validating AI-generated Outputs before relying upon them.

---

10. Changes and Limitations

Zenney may modify or update its security practices, technologies and operational procedures from time to time, provided the overall level of security is not materially reduced.

No security system is completely secure. To the maximum extent permitted by law, Zenney does not warrant that the Services will be free from all Security Incidents and is not responsible for Security Incidents arising from Customer systems, Customer credentials, Customer-controlled infrastructure, third-party services selected or controlled by Customer, internet or telecommunications failures, or events beyond Zenney's reasonable control. This exclusion does not apply to the extent directly caused by Zenney's wilful misconduct.