LizzyAI – Security Addendum

Last modified: November 15th, 2025 / v-SA1811250000

We recognize that the security and privacy of your data are of the utmost importance. This Security Addendum outlines our commitment to maintaining robust information security and data protection practices. We implement commercially reasonable technical and organizational measures to secure the Software and protect Customer Data, including the policies and practices listed below (or materially equivalent alternatives that provide a substantially similar level of security). This Data Protection Policy is governed by our Data Processing Addendum ("**DPA**"), as published on our website and updated from time to time (currently available at lizzyai.com/dpa). Defined terms used but not defined herein shall have the meanings ascribed to them in the DPA.

---

1. Software controls.

1.1. **No training on Customer Data:** Customer Data shall not be used to train AI models, except with Customer's prior written consent for models private to the Customer.

1.2. **No retention of Customer Data:**

1.2.1. The content of end-user chats, such as inputs, outputs and uploaded files ("**User Chats**"), is retained for a default retention period of up to 45 days, unless extended via Customer Instructions.

1.2.2. Any other Customer Data shall be permanently deleted within 45 days of Subscription termination, as detailed in the DPA.

1.3. **Encryption of Customer Data:** Customer Data is encrypted at rest (AES-256 +) and in transit (TLS 1.2+).

1.4. **Privacy of User Chats**: User Chats are encrypted with a personal key and are accessible only by the user. No third party, including Provider or other users, can view the content of such chats, unless a chat is proactively shared with them.

1.5. **Secure authentication:** Authentication to the Software is managed exclusively through reputable third-party providers, such as Google and Microsoft, or via the Customer's SSO service. The Provider does not manage, store, or process end-user passwords directly.

1.6. **Customer's systems isolation:** The Provider shall not be given access to Customer's systems. The Software shall not interact with Customer's systems without proactive enablement by the Customer (e.g. SSO, Office 365 add-ins, linking data sources, etc.).

1.7. **External audits:** External, third-party security audit is conducted on the Software at least annually.

1.8. **Firewall:** permitted sites (such as AI API providers) may be accessed only via firewall rules.

1.9. **Data segregation:** By default, the Software is provided via secure multi-tenant infrastructure, with logical data segregation (at minimum, via data encryption). Tenant separation options are available against additional charge if specifically agreed by the parties (for removal of doubt, tenant separation shall not apply to direct communication channels, such as email, support tickets or other communication channels).

1.9.1. **Private tenant:** Single tenant infrastructure, with server level separation and common network (shared firewall and load balancer).

1.9.2. **VPC:** Virtual Private Cloud (VPC) with network level separation (including private firewall and load balancer).

2. Internal policies.

2.1. **Officers:** Provider shall appoint Information Security, Data Protection and AI Compliance officers.

2.2. **Security policy:** Provider shall maintain an internal security policy that will include the internal controls and policies listed in this Addendum ("**Security Policy**").

2.3. **Personnel training:** All personnel with access to production systems must review and approve the Security Policy and re-review it at least once per annum.

2.4. **Personnel confidentiality**: All personnel with access to production systems must be subject to confidentiality undertakings or appropriate statutory obligations of confidentiality.

2.5. **Security ledger:** Provider shall document, in a ledger, application or otherwise, critical security information, including, production access permissions, security incidents and external reviews.

2.6. **Endpoint security:** All computers with access to production resources are required to: (a) run an approved ESS (Endpoint Security Software), (b) comply with Provider password policy, (c) be configured to automatically lock when inactive, (d) be physically locked when not used.
2.7. **Production separation:** Separate production and non-production environments.
2.8. **Access management:** Access to production systems should comply with the following: (a) Enable MFA, (b) Apply least privilege access principles, so that access is granted only to personnel who need it, with the minimal necessary permissions to perform their job functions, (c) established procedures for access revocation.
2.9. **Logging and monitoring:** Provider shall collect logs and monitor the Software.
2.10. **Record keeping:** Provider shall maintain records as required by applicable law.
2.11. **Business continuity:** Provider shall maintain a business continuity plan that shall, at minimum, list key continuity risks and associated mitigations.