Policy Name: Enterprise Data Privacy & Security Standards
Version: 3.2
Last Updated: January 2024

1. Purpose

This policy ensures that all vendors handling sensitive or personal data comply with international data protection regulations, including **GDPR**, **CCPA**, and **ISO 27001 standards**.

2. Data Protection Requirements

- **Encryption:** All sensitive data must be encrypted using at least **AES-256 encryption** during storage and transmission.
- **Access Control:** Multi-factor authentication (MFA) is required for accessing customer data.
- **Data Retention:** Vendors must specify a **clear data retention and deletion policy** that aligns with **GDPR Article 5**.
- **Data Minimization:** Vendors must collect only the data required for processing and avoid excessive data storage.

3. Compliance with GDPR & Other Regulations

- Vendors must ensure **explicit consent** is obtained before collecting personal data.
- Data subjects must have the right to **access, modify, and delete** their personal data upon request.
- Vendors handling EU citizen data must appoint a **Data Protection Officer (DPO)** and have a **GDPR compliance framework** in place.

4. Breach Notification Policy

- Vendors must **report any security breaches within 72 hours** of detection.
- A **detailed incident response plan** must be provided, specifying how breaches are handled.

5. Vendor Audit Requirements

- The company reserves the right to **audit vendor security controls annually**.
- Failure to meet security compliance will result in **contract termination or penalty clauses**.