**Privacy and Data Protection Policy (PDPP)**

**Policy ID:** SEC-PDPP-001  
**Version:** 1.0  
**Approval Date:** [Insert Date]  
**Next Review Date:** [Insert Date + 12 months]  
**Owner:** Chief Privacy Officer (CPO) / Chief Information Security Officer (CISO)  
**Applies To:** All employees, contractors, and service providers who collect, process, store, or share personal data on behalf of [COMPANY NAME]

**1. Purpose**

The purpose of this policy is to establish [COMPANY NAME]’s privacy principles, define personal data handling requirements, and ensure compliance with applicable laws and frameworks. It governs the protection of personal and sensitive information throughout its lifecycle.

**2. Scope**

This policy applies to all personal data processed by [COMPANY NAME], including employee, customer, vendor, and partner data in both digital and physical formats. It includes:

* Direct and indirect identifiers (e.g., name, ID numbers, IP address)
* Sensitive data (e.g., financial, health, biometric)
* Data processed within internal systems and by third parties
* Data collected via websites, mobile apps, or internal tools

**3. Policy Statements**

**3.1 Lawful and Transparent Processing**

* Personal data must be collected and processed based on a documented legal basis (e.g., consent, contract, legal obligation). *(GDPR Art. 6; CCPA §1798.100; NIST AR-4; ISO 27001 A.5.11)*
* Data subjects must be informed of the purpose, scope, and use of their data at the point of collection. *(GDPR Art. 12-14; ISO 27001 A.5.11)*

**3.2 Data Minimization and Purpose Limitation**

* Only the minimum amount of personal data required for a specific purpose may be collected and processed. *(GDPR Art. 5(1)(c); NIST DM-1; ISO 27001 A.5.12)*
* Personal data must not be used for new or unrelated purposes without obtaining additional lawful justification. *(GDPR Art. 6(4); CCPA §1798.100(b))*

**3.3 Data Subject Rights**

* Individuals have the right to access, correct, delete, restrict, and obtain a copy of their personal data. *(GDPR Art. 15–20; CCPA §1798.100–105; NIST AR-2; ISO 27001 A.5.11)*
* All data subject requests must be acknowledged and fulfilled within legally required timeframes. *(GDPR Art. 12(3); CCPA §1798.130)*

**3.4 Security of Personal Data**

* Personal data must be encrypted during storage and transmission using approved cryptographic methods. *(NIST SC-12, SC-13; ISO 27001 A.8.24, A.8.25)*
* Access to personal data must be restricted to authorized personnel only. *(NIST AC-6; ISO 27001 A.5.18; GDPR Art. 32)*
* Personal data breaches must be reported, investigated, and documented in accordance with legal obligations. *(NIST IR-6; ISO 27001 A.5.25; GDPR Art. 33–34)*

**3.5 Third-Party Processing**

* Third-party processors must be bound by a data processing agreement (DPA) that enforces equivalent data protection obligations. *(GDPR Art. 28; NIST SR-3; ISO 27001 A.5.20)*
* Vendors with access to personal data must be evaluated for privacy and security risks before onboarding. *(NIST SA-9; ISO 27001 A.5.21)*

**3.6 Data Retention and Disposal**

* Personal data must be retained only as long as necessary for business or legal reasons. *(GDPR Art. 5(1)(e); CCPA §1798.105(c); NIST DM-2; ISO 27001 A.8.10)*
* Data that is no longer required must be securely deleted, anonymized, or destroyed. *(NIST MP-6; ISO 27001 A.8.11)*

**3.7 Privacy by Design and Default**

* New systems and processes must incorporate privacy controls and default settings to limit data exposure. *(GDPR Art. 25; NIST PL-8; ISO 27001 A.5.11)*
* Data protection impact assessments (DPIAs) must be conducted before introducing high-risk processing activities. *(GDPR Art. 35; NIST AR-3)*

**4. Roles and Responsibilities**

|  |  |
| --- | --- |
| **All Users** | Follow privacy policies and report incidents or data handling issues. |
| **CPO / Privacy Team** | Oversee privacy governance, respond to rights requests, and maintain legal compliance. |
| **IT/Security Team** | Enforce access control, encryption, and breach response for personal data systems. |
| **Legal/Compliance** | Ensure policy alignment with applicable privacy laws and contracts. |
| **Third-Party Managers** | Ensure vendors with access to PII are risk-assessed and under DPAs. |

**5. Compliance and Enforcement**

Violations of this policy may result in legal penalties, regulatory investigations, financial loss, or internal disciplinary action. [COMPANY NAME] enforces this policy through training, monitoring, and periodic privacy audits.

**6. Review and Maintenance**

This policy shall be reviewed annually or following any significant changes in data protection regulations, business practices, or data systems. Updates must be approved by the Chief Privacy Officer and communicated to all relevant stakeholders.

**7. Acknowledgment and Agreement**

I acknowledge that I have read, understand, and agree to comply with [COMPANY NAME]’s Privacy and Data Protection Policy. I understand my responsibilities and the importance of protecting personal data in accordance with this policy.

|  |  |  |
| --- | --- | --- |
| **Name (Print):**  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | **Signature:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | **Date:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |