### Data Protection and Privacy Policy

**Policy Number:** DPP/2024/005  
**Effective Date:** 2024-01-24

#### **1. Policy Statement:**

[Your Company Name] is committed to respecting and protecting the privacy and security of all personal and sensitive information that it handles. This Data Protection and Privacy Policy provides the framework for ensuring the confidentiality, integrity, and availability of personal data, in compliance with applicable data protection laws and regulations.

#### **2. Scope:**

This policy applies to all employees, contractors, and third parties who handle or have access to personal and sensitive information controlled by [Your Company Name], across all platforms and locations.

#### **3. Definitions:**

* **Personal Data:** Any information relating to an identified or identifiable natural person.
* **Sensitive Data:** Personal data that reveals racial or ethnic origin, political opinions, religious beliefs, trade union membership, genetic data, biometric data, health information, or data concerning a person's sex life or sexual orientation.

#### **4. Policy:**

**4.1 Data Collection and Consent:**

* Collect personal data lawfully, fairly, and transparently.
* Obtain explicit consent from individuals before collecting their personal data, where required, and inform them of the purpose for which the data will be used.

**4.2 Data Use and Processing:**

* Use and process personal data only for the purposes for which it was collected and in a manner consistent with the consent provided by the individual.
* Ensure that personal data is accurate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.

**4.3 Data Security and Protection:**

* Implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, protecting data against unauthorized or unlawful processing, accidental loss, destruction, or damage.
* Ensure that data protection measures are integrated into data processing activities and business practices.

**4.4 Data Access and Sharing:**

* Limit access to personal data to authorized personnel only, based on the necessity to know for business purposes.
* Ensure that any sharing or transfer of personal data to third parties is done securely and in compliance with applicable laws and agreements.

**4.5 Data Retention and Disposal:**

* Retain personal data only for as long as necessary for the purposes for which it was collected or as required by law.
* Dispose of personal data securely and in a manner that prevents its reconstruction or recovery.

**4.6 Employee Training and Awareness:**

* Provide regular training to all employees handling personal data to ensure awareness and understanding of data protection responsibilities.
* Foster a data protection culture within the organization.

**4.7 Incident Response and Notification:**

* Establish a robust incident response plan to address any data breaches or security incidents promptly.
* Notify the relevant authorities and affected individuals in case of a data breach, as required by law.

**4.8 Data Subject Rights:**

* Respect and facilitate the exercise of data subjects' rights, including the right to access, correct, delete, or transfer their personal data.

#### **5. Review and Modification:**

This policy will be reviewed annually or in response to changes in law, technology, organizational operations, or security incidents. All amendments to this policy must be approved by [Appropriate Authority/Department].