EMPLOYEE DATA PROTECTION POLICY

Effective Date: [Insert Date]
Last Revised: [Insert Date]

INTRODUCTION

This Employee Data Protection Policy ("Policy") is established by **[Company Name]** ("Company") to ensure the lawful, fair, and transparent processing of employee personal data in compliance with the **Digital Personal Data Protection Act, 2023 ("DPDP Act")** and other applicable laws. The Company is committed to safeguarding employee privacy and ensuring data protection while fulfilling legal and operational requirements.

OBJECTIVES

1. Ensure compliance with the DPDP Act and related regulations.
2. Protect the confidentiality, integrity, and availability of employee personal data.
3. Provide guidelines for the collection, use, storage, and secure disposal of employee personal data.
4. Outline the rights of employees regarding their personal data and the Company's obligations.

SCOPE

This Policy applies to:

- **Individuals**: Current, former, and prospective employees, interns, contractors, consultants, and temporary workers.
- **Data Types**: Personal and sensitive personal data processed in any format (electronic, physical, or verbal).
- **Processing Activities**: All activities related to the collection, use, storage, sharing, and deletion of employee personal data.

DEFINITIONS

1. **Personal Data**: Information identifying an individual, such as name, address, contact details, and identification numbers.

2. **Sensitive Personal Data**: Data related to health, financial status, biometrics, or other categories defined under the DPDP Act.
3. **Processing**: Any operation on personal data, including collection, recording, storage, sharing, or deletion.
4. **Data Subject**: An employee whose personal data is processed.
5. **Data Protection Officer (DPO)**: The individual responsible for overseeing data protection compliance within the Company.

PRINCIPLES OF DATA PROCESSING

The Company adheres to the following principles:

1. **Lawfulness, Fairness, and Transparency**: Inform employees about the purpose and use of their data.
2. **Purpose Limitation**: Collect and use data only for specified, legitimate purposes.
3. **Data Minimization**: Collect only data necessary for specific purposes.
4. **Accuracy**: Ensure data is accurate and updated promptly.
5. **Storage Limitation**: Retain data only as long as necessary for its original purpose.
6. **Security**: Protect data against unauthorized access, loss, or damage.

CATEGORIES OF DATA COLLECTED

The Company may collect the following data from employees:

- **Identification Information**: Name, date of birth, gender, employee ID, and photographs.
- **Contact Information**: Address, phone number, and email.
- **Employment Information**: Job title, department, performance evaluations, and work history.
- **Financial Information**: Bank account details, salary information, and tax identification numbers.
- **Health Information**: Medical records and fitness assessments.
- **Biometric Data**: Fingerprints or facial recognition (if applicable).

USE OF EMPLOYEE DATA

Employee data is used for:

1. Recruitment and onboarding processes.
2. Payroll and benefits administration.
3. Performance evaluations and career development.

4. Legal and regulatory compliance.
5. Operational requirements, such as communication and resource allocation.
6. Workplace security and safety monitoring.

DATA PROTECTION MEASURES

1. **Access Controls**: Limit access to employee data to authorized personnel.
2. **Encryption**: Encrypt data stored electronically to prevent unauthorized access.
3. **Physical Security**: Store physical records securely in locked cabinets or restricted areas.
4. **Training**: Provide regular training to employees handling personal data.
5. **Breach Management**: Implement an incident management framework for prompt breach response.

DATA RETENTION

Employee data will be retained for the duration of employment and as required by law. Upon termination, data will be archived or securely deleted, following applicable retention policies.

EMPLOYEE RIGHTS

Employees have the following rights concerning their personal data:

1. **Right to Access**: Request access to personal data held by the Company.
2. **Right to Rectification**: Request corrections to inaccurate or incomplete data.
3. **Right to Erasure**: Request deletion of unnecessary data.
4. **Right to Restrict Processing**: Limit data processing in specific circumstances.
5. **Right to Data Portability**: Request data in a portable format.
6. **Right to Withdraw Consent**: Revoke consent for specific data processing activities.

To exercise these rights, employees may contact the DPO at:

- **Email**: [Insert DPO Email Address]
- **Phone**: [Insert DPO Phone Number]

NON-COMPLIANCE

Failure to comply with this Policy or applicable data protection laws may result in disciplinary action, including termination of employment and legal consequences.

REVIEW AND UPDATES

This Policy will be reviewed annually or as required by changes in laws, regulations, or operational practices. Any updates will be communicated to employees promptly.

CONTACT INFORMATION

For questions or concerns, contact:

- **Data Protection Officer (DPO)**: [Insert Name]
- **Email**: [Insert DPO Email Address]
- **Phone**: [Insert DPO Phone Number]

Approved by:
Name: [Insert Approver Name]
Title: [Insert Approver Title]
Date: [Insert Approval Date]