DEE Development Engineers Limited

Data Governance and Cybersecurity Policy

Issued By: Chief Operating Officer (COO)

Issued on September 18, 2024

INTRODUCTION

DEE Development Engineers Ltd. (hereinafter referred as “DEE Piping” or “Company”) recognises that data and information systems are vital assets essential to a company’s operational integrity, competitive advantage, and reputation. This policy establishes the framework for the governance, protection, and responsible use of data across the company to ensure its confidentiality, integrity, and availability.

PURPOSE

The purpose of this policy is to:

- Protect company, employee, customer, and partner data from unauthorized access, disclosure, alteration, or destruction.
- Define principles for the appropriate classification, handling, and storage of data.
- Ensure compliance with applicable data protection and privacy laws and regulations.
- Minimize the risk of cybersecurity incidents and ensure resilience.

SCOPE

This policy applies to all employees, contractors, consultants, and other third parties who access, process, or store DEE Piping data or utilize DEE Piping information technology assets, regardless of location or device.

CORE PRINCIPLES

Data Governance

DEE Piping manages its data as a strategic asset. This includes:

- **Data Classification:** Data is classified based on its sensitivity, criticality, and regulatory requirements.

- **Data Ownership:** Business owners are identified and responsible for the accuracy, integrity, and security of their data domains.
- **Data Quality:** Processes are in place to ensure data is accurate, complete, and reliable for its intended use.
- **Data Lifecycle:** Data is managed securely throughout its lifecycle, from creation and processing to storage and secure disposal.

Cybersecurity

DEE Piping implements reasonable and appropriate technical and organizational measures to protect its information assets. These measures include:

- **Access Control:** Adherence to the principle of least privilege to ensure individuals have access only to the data necessary for their job functions.
- **Network Security:** Protections that safeguard the integrity of networks and infrastructure housing company data.
- **Endpoint Security:** Secured devices (e.g., laptops, mobile phones) that access the corporate network.
- **Security Awareness:** Training for employees on cybersecurity threats and their responsibilities.
- **Incident Response:** A maintained plan to detect, respond to, and recover from cybersecurity incidents.

Privacy and Compliance

DEE Piping complies with applicable data privacy laws and regulations. Personal data is collected and processed lawfully, fairly, and transparently.

ROLES AND RESPONSIBILITIES

- **Senior Management** provides the resources and leadership to support this policy.
- **The IT Department** implements and maintains technical security controls.

- **Data Owners** define classification and handling rules for their data.
- **All Users** understand and adhere to this policy, including using strong passwords, recognizing phishing attempts, and reporting security incidents immediately.

INCIDENT REPORTING

Any suspected or actual cybersecurity incident (e.g., data breach, malware infection, phishing attack) is reported immediately to the IT Department.

POLICY REVIEW

This policy is reviewed regularly to ensure compliance with applicable regulations and oversight.