Ddev Plastiks Industries Limited

CIN: L24290WB2020PLC241791
Registered Office: 2B, Pretoria Street, Kolkata- 700 071

Cyber Security and Data Privacy Policy

1. Objectives

Ddev Plastiks Industries Limited recognizes the critical importance of safeguarding information and acknowledges the pivotal role played by information technology in its operations. With increased digital usage and information sharing among authorized users of Ddev Plastiks' IT resources, the company aims to bolster its efforts to protect these resources. To address these requirements, Ddev Plastiks has developed this policy, which provides privacy guidelines and usage regulations for its Information Technology Resources.

This policy outlines measures to secure data and the technology infrastructure of the company. As dependency on technology for data collection, storage, and management grows, so do vulnerabilities to security breaches. Human errors, cyberattacks, and system failures could significantly harm the company's reputation and financial standing. Therefore, Ddev Plastiks has implemented robust security measures and defined instructions to mitigate these risks.

The objective of this policy is to ensure that all users utilize Ddev Plastiks' Information and Information Systems lawfully, ethically, and professionally to further the company's interests.

2. Scope and Applicability

This policy applies to all individuals with access to Ddev Plastiks' Information Technology Resources in India. Factory Managers and the IT Head at the corporate office are responsible for ensuring effective communication, understanding, and adherence to this policy.

The policy also extends to all contracted staff, vendors, and suppliers providing services to Ddev Plastiks. The HR/Admin department, in collaboration with respective Factory Managers, must ensure that these stakeholders receive a copy of this policy before access is granted.

The scope includes all company-owned or leased IT and communication resources, such as:

2.1. Computer-related equipment (e.g., desktops, laptops, terminals, workstations, PDAs, wireless devices, telecom equipment, networks, databases, printers, servers, shared computers).

2.2. Electronic communication devices (e.g., telephones, pagers, voicemail, email, fax machines, wired/wireless communication devices, internet/intranet services).

2.3. Software (e.g., purchased/licensed business applications, internally developed applications, operating systems, firmware).

2.4. Intellectual property and other data stored on company equipment.

2.5. Remote access to company resources through any networked connection or using company equipment.

2.6. Usage of the company website (https://www.ddevgroup.in/) is also governed by this policy.

Definitions

Information Technology Resources: These include all IT-related devices and services owned, licensed, or contracted by Ddev Plastiks, including computer hardware, printers, fax machines, voicemail, software, and network access.

User: Any individual accessing Ddev Plastiks' IT Resources, including employees, temporary staff, contractors, vendors, and suppliers.

Sensitive Personal Data: As per the Indian Information Technology Rules 2011, this includes data such as passwords, financial details, health records, biometric information, and sexual orientation provided for services.

3. Policy

Cyber Security Protecting sensitive data, such as unpublished financial information, customer/vendor data, patents, and new technologies, is of utmost importance. Employees must follow these guidelines:

Protection of Devices:

- Secure personal and company-provided devices with passwords.
- Use updated antivirus software and install security updates.
- Avoid leaving devices unattended or exposed.
- Use private, secure networks for accessing company systems.

Email Safety:

- Exercise caution with email attachments and links.
- Verify sender details to identify phishing attempts.
- Report suspicious emails to the IT Head or IT Team.

Password Management:

- Use strong, unique passwords with a mix of characters and symbols.
- Change passwords every two months and avoid sharing them unnecessarily.

Secure Data Transfer:

- Use company systems for transferring sensitive information.
- Ensure recipients have proper authorization.
- Report security incidents promptly to the IT Team.

Additional Precautions:

- Lock devices when unattended.
- Notify HR/IT of lost or damaged equipment.
- Avoid installing unauthorized software.

Responsibilities of the IT Team:

- Implement firewalls, anti-malware software, and access authentication.
- Conduct security training and regular updates for employees.
- Investigate security breaches thoroughly.

Remote Employees:

- Adhere to data encryption and protection standards while accessing company systems remotely.

Taking Security Seriously: Maintaining vigilance and prioritizing cybersecurity is essential to ensure stakeholder confidence.

Privacy Policy Ddev Plastiks acknowledges the risks of failing to protect personal data and comply with privacy regulations. Personal data collected from stakeholders is stored securely and used only for legitimate business purposes. The company ensures compliance with all relevant legal and ethical standards.

4. Disciplinary Actions

Violations of this policy will result in disciplinary measures, which may include counseling, warnings, removal of system privileges, demotion, suspension, or legal action, depending on the severity of the infraction. HR will determine the appropriate action in consultation with management.

5. Cyber Security and Data Privacy Governance

The governance structure includes the IT Head, Site IT Heads, and System Admins. These personnel are responsible for implementing, maintaining, and improving cybersecurity and data privacy measures.

6. Raise Your Concern

For inquiries or to report potential policy violations, employees can contact:

Grievance Officer:
IT Head
Registered Office 2B, Pretoria Street, Kolkata – 700071

E-mail: ithelpdesk@ddevgroup.in

9 AM – 5 PM (on all working days)

For compliance issues, contact the Compliance Team at tanvi.goenka@ddevgroup.in. Retaliation against individuals reporting concerns is strictly prohibited.