PEARL GLOBAL

Exceeding Expectations...Always

PGIL -Cyber Security Policy

Company Name: Pearl Global Industries Limited
Effective Date: 4th May 2025
Reviewed By: IT & Compliance Team
Next Review Date: 3rd May 2026

1. Purpose

To protect the company's digital assets, customer data, employee information, and operational systems from cyber threats including unauthorized access, data breaches, malware, and other cyber risks.

2. Scope

This policy applies to all employees, contractors, third-party vendors, and anyone accessing the company's IT systems, applications, cloud infrastructure, or data.

3. Key Objectives

- Maintain the confidentiality, integrity, and availability of company data.
- Prevent, detect, and respond to cybersecurity threats.
- Ensure compliance with data protection laws and industry standards.

4. Acceptable Use

- Use company IT resources only for business-related activities.
- Avoid accessing suspicious websites, pirated software, or unknown email links.
- Use strong passwords and never share login credentials.

5. Access Control

- Role-based access to systems and data (minimum necessary privilege).
- Multi-Factor Authentication (MFA) where feasible.
- Immediate revocation of access upon employee exit or role change.

6. Data Protection

- Sensitive data (customer, financial, HR) must be encrypted both in transit and at rest.
- Regular data backups to be maintained on secure servers.
- Personal devices must be secured before accessing company systems.

7. Email & Internet Security

- Company email to be used for business only.
- All incoming emails are scanned for malware and phishing.
- Employees are trained to identify phishing and report suspicious messages.

PEARL GLOBAL INDUSTRIES LTD.
Authorised Signatory

8. Device Security

- All devices must have updated antivirus and firewall protection.
- Automatic locking enabled after inactivity.
- Lost/stolen devices must be reported immediately.

9. Software Management

- Only licensed and approved software may be installed.
- Regular patching and updates to operating systems and applications.
- Unauthorized downloads or installations are strictly prohibited.

10. Incident Response

- All cybersecurity incidents must be reported to the IT team within 24 hours.
- A defined incident response plan will be activated, involving:
    - Detection
    - Containment
    - Investigation
    - Resolution
    - Post-incident review

11. Third-Party & Vendor Security

- Vendors must comply with equivalent cyber security standards.
- Data sharing with third parties is limited, monitored, and logged.

12. Training & Awareness

- Mandatory annual cybersecurity training for all employees.
- Regular awareness sessions on evolving threats and best practices.

13. Disciplinary Action

Violations of this policy may result in disciplinary action, including termination and/or legal consequences.

14. Policy Review

This policy will be reviewed annually or upon any major IT infrastructure change.

PEARL GLOBAL INDUSTRIES LTD.
★ Authorised Signatory ★