PAKKA
Packaging with a Soul

CYBER SECURITY POLICY

1. Purpose

Pakka Limited ("the Company"), being a public listed company, is committed to safeguarding the confidentiality, integrity, availability, and lawful processing of its information assets. This Cyber Security Policy is framed in alignment with:

- The Information Technology Act, 2000 and rules made thereunder (including the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011)
- The Digital Personal Data Protection Act, 2023 (DPDP Act)
- SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 (SEBI LODR)
- CERT-In Directions dated 28 April 2022 and subsequent amendments
- Applicable labour laws, contractual obligations, and industry best practices

This policy establishes a structured framework to manage cyber security risks, ensure regulatory compliance, and protect stakeholder interests.

2. Scope

This Policy applies to:

- All Pakka team members (permanent, contractual, temporary)
- Board of Directors and Senior Management
- Consultants, contractors, vendors, service providers, and other third parties
- All information assets, systems, networks, applications, cloud services, and data (electronic or physical)

3. Definitions

Unless otherwise specified, terms used in this Policy shall have the meanings assigned under the IT Act, 2000 and the DPDP Act, 2023.

- **Company**: Pakka and its subsidiaries, divisions, and affiliates.
- **Information Assets**: Data, systems, applications, infrastructure, intellectual property, financial and operational records.
- **Personal Data**: As defined under the DPDP Act, 2023.

- **Sensitive Personal Data or Information (SPDI)**: As defined under the IT Rules, 2011 (where applicable).
- **Cyber Security Incident**: Any real or suspected event that compromises confidentiality, integrity, or availability of information assets.
- **Designated Personnel**: Officers authorised to manage cyber security, incident response, and compliance.

4. Governance and Accountability

4.1 Board and Senior Management

- The Board of Directors shall have oversight of cyber security risks as part of enterprise risk management in accordance with SEBI LODR.
- Senior Management shall ensure adequate resources, systems, and controls are implemented to manage cyber security risks.

4.2 Designated Officer / CISO

- The Company shall appoint a Designated Officer / Chief Information Security Officer (CISO) or equivalent.
- Responsibilities include policy implementation, risk assessment, incident response, regulatory reporting, and coordination with CERT-In.

4.3 Team Members and Users

- All users shall comply with this Policy and related procedures.
- Any suspected cyber security incident must be reported immediately to the Designated Personnel.

5. Risk Management and Controls

- Cyber security risks shall be identified, assessed, and mitigated through a formal risk management process.
- Reasonable security practices shall be implemented, including administrative, technical, and physical safeguards as required under the IT Act.
- Critical systems and data shall be classified and protected based on sensitivity and business impact.

6. Data Protection and Privacy

- Personal data shall be processed lawfully, fairly, and transparently in accordance with the DPDP Act, 2023.
- Collection and processing of personal data shall be limited to legitimate business purposes.
- Appropriate consent, notice, retention, and deletion mechanisms shall be implemented.

- Cross-border data transfers, where applicable, shall comply with applicable Indian laws and regulatory guidance.

7. Access Control and Acceptable Use

- Access to information assets shall be granted strictly on a need-to-know and role-based basis.
- Strong authentication, password management, and periodic access reviews shall be enforced.
- Company systems shall be used only for authorised business purposes.

8. Incident Management and Reporting

- All cyber security incidents (actual or suspected) shall be promptly reported and investigated.
- The Company shall maintain an Incident Response Plan aligned with CERT-In requirements.
- Reportable cyber incidents shall be notified to CERT-In within prescribed timelines.
- Material cyber security incidents shall be disclosed to stock exchanges as required under SEBI LODR.

9. Vulnerability Assessment and Monitoring

- Periodic vulnerability assessments and penetration testing shall be conducted through internal and/or external experts.
- Logs and records shall be maintained in accordance with CERT-In Directions.
- Systems shall be continuously monitored for unauthorised access or anomalies.

10. Third-Party Risk Management

- Third parties with access to Company systems or data shall be subject to due diligence.
- Contracts shall include appropriate cyber security and data protection obligations.
- Third-party compliance shall be periodically reviewed.

11. Training and Awareness

- Mandatory cyber security and data protection awareness training shall be conducted annually for all Team Members.
- Specialised training shall be provided to personnel handling critical systems and personal data.

12. Audit, Compliance, and Review

- Compliance with this Policy and applicable laws shall be periodically audited.
- The Policy shall be reviewed at least annually or upon any material regulatory or business change.
- All statutory, regulatory, legal, and contractual cyber security requirements shall be complied with.

13. Non-Compliance and Disciplinary Action

- Non-compliance with this Policy may result in disciplinary action, including termination of employment or contracts, and legal action where applicable.

14. Grievance Redressal

- Any concern, grievance, or complaint relating to cyber security or data protection may be raised with the Designated Officer / Grievance Officer.

Approved by: Seva Sangh

Effective Date: 1st April 2026

Review Cycle: 3 Years