BALKRISHNA INDUSTRIES LIMITED

Cyber Security and Data Privacy Policy

Policy Title	Cyber Security and Data Privacy Policy
Issue Number	1
Issue Date	27th May, 2023
Approved by	Board of Directors
Revision Number	0
Revision Date	

Policy brief and Purpose:

The purpose of this policy is to respect the privacy and safeguard the personal data of Balkrishna Industries Limited's (hereinafter referred to as "BKT" or "the Company") all employees, directors, senior executives, officers, employees (whether permanent, fixed-term or temporary), consultants, contractors, trainees, seconded staff, workers, interns, business partners, suppliers, community or any other person affiliated with BKT while also ensuring compliance with all relevant laws and regulations.
This policy serves as an overarching framework for IT security policy and standards. BKT acknowledges privacy regulations and standards for personal data protection. It believes that preventing harm to individuals whose data is at risk is critical to its reputation.
The purpose of the policy is to create awareness about cyber security and data privacy aspects. In addition, it provides guidance on various platforms available at BKT to raise any concern related to cyber security. (Email id – hemant.joshi@bkt-tires.com)

Scope and Coverage:

All employees, directors, senior executives, officers, employees (whether permanent, fixed-term or temporary), consultants, contractors, trainees, seconded staff, workers, interns, business partners, suppliers, community or any other person affiliated with BKT, have access to personal information gathered or processed, or who voluntarily provide information to the Company are subject to the terms and conditions of this policy.

Cyber Security and Data Privacy Policy Statements:

BKT understands the significance of protecting personal and sensitive data (as per the regulatory provisions such as price sensitive information, details of complainant in case of discrimination or POSH related incidents) and the requirement for appropriate controls while collecting, transferring, storing and processing personal data. It anticipates that all information shall be handled responsibly in accordance with the applicable laws. This policy defines the responsibility to:

- Maintain and uphold the availability, integrity and confidentiality of information
- Manage the risk of security exposure or compromise
- Reliable Information Technology (IT) environment
- Monitor systems for anomalies that might indicate compromise, data breach response and promote and increase the awareness of information security.
- Provide framework for ensuring that the necessary safeguards are in place to secure the confidentiality, integrity and availability of data. It also ensures that employees and all other affiliates are aware of their roles and responsibilities and have a sufficient understanding of security policy, processes and practices.

Responsibilities:

- The Company is responsible for:
  - Creating awareness and training on the fundamental information security protocols required to safeguard the confidentiality, integrity and availability of information entrusted
  - Preventing the misuse of resources or information by unauthorized parties
  - Preventing illegal use of sensitive and personal data
  - Reporting suspected information security incidents to the designated or dedicated incident reporting system
  - Monitoring the performance of cyber security management systems- Securus.
  - Providing resources to maintain information security control consistent with this policy
  - Regular risk assessment and audits on its cyber security systems internally and by engaging with independent experts/ agencies

Grievance Redressal Mechanism:

All stakeholder (who uses the company's system and data terminal or computer systems) shall report the incident which is subjected to a security breach or identifies any activity such as improper access or use of system shall immediately report the incident to the IT office via helpline, Incident Reporting System, Supervisor/Manager. All relevant stakeholders shall be aware of the grievance redressal mechanism on cyber security and data privacy

Enforcement:

Any stakeholder found to have violated this policy shall be subject to disciplinary action as per the company's policy and regulatory guidance.