



SINCE 1987

ROYAL CHAIN LIMITED

(FORMERLY KNOWN AS ROYAL CHAIN PRIVATE LIMITED & ROYAL CHAINS PRIVATE LIMITED)

GST : 27AAGCR6146R1ZL CIN : U74120MH2013PLC247888

Registered Office : 1st Floor, 127/129, Office No. 101/102, Royal House, Shaikh Memon Street,
Zaveri Bazaar, Kalbadevi, Mumbai - 400002. Maharashtra.

Cyber Security Policy

Organization:	Royal Chain Limited	Prepared by:	IT Manager	
Department:	Information Technology	Reviewed by:	IT Head	Girish Surve
Revision:	v2	Approved by:	MD & CEO	Snneh Suresh Jain
Next Version by	Reviewed Every Year	Applies from Date:	01 st Aug 2026	

1.0 Purpose

This policy establishes Royal Chain Limited's ("RCL" / "the Company") commitment to protecting the confidentiality, integrity and availability of its information assets, systems and data - including customer, employee, vendor and business information - against cyber threats.

It provides the overarching framework under which the Company's detailed information security policies and procedures operate.

2.0 Scope

This policy applies to all employees (both on roll or off roll), directors, contractors, consultants and third parties who access or process Company information, and to all information systems, applications, networks, cloud services and devices owned, leased or used by the Company across all its locations.

3.0 Governance & Responsibilities

- The Management of the Company provides oversight of cyber security and reviews the cyber risk posture periodically.
- The IT Head is the designated owner of cyber security, responsible for implementation, monitoring and reporting of security measures and incidents to Management.

#HameshaKeLiyeRoyal



FACTORY ADDRESS : A-606/2, Trans Thane Creek Industrial Area, Shil Phata Mahape Road, Mahape Village,
Navi Mumbai, Thane, Maharashtra - 400710.

+91 22 2311 9999 +91 22 6996 3333 ✉ info@royalchains.com 🌐 www.royalchaingroup.com

- The IT team implements and operates security controls; HR drives user awareness and compliance; all users are responsible for adhering to this policy.
- Cyber risks are identified, assessed and monitored through the Company's Cyber Risk Management framework, reviewed periodically and during audits.

4.0 Security Principles

- Confidentiality, Integrity and Availability of information as the core objective.
- Least privilege and need-to-know based access to systems and data.
- Defense in depth - layered controls across network, endpoint, application and data.
- Security by design in selection and implementation of new systems and vendors.
- Accountability - user actions on Company systems are logged and attributable.

5.0 Security Controls Framework

The Company maintains, and periodically reviews, documented policies and controls covering the following domains:

- **Access Control & User Management** - formal authorisation for access, joiner-mover-leaver process, periodic user access reviews, and controlled privileged access.
- **Authentication & Password Management** - enforced password complexity, expiry and lockout standards; multi-factor authentication where supported.
- **Network & Endpoint Security** - perimeter firewall, network segmentation, antivirus/EDR on all endpoints and servers, hardened system configurations, and restricted use of removable media.
- **Data Protection & Privacy** - classification and handling of information per sensitivity; protection of personal data in line with applicable law including the Digital Personal Data Protection Act, 2023.
- **Backup & Recovery** - regular backups of critical data with defined retention, restoration testing, and a documented Disaster Recovery Plan.
- **Change & Patch Management** - authorised, tested and documented changes; timely application of security patches.
- **Vendor & Cloud Security** - security and confidentiality obligations for vendors and cloud/SaaS providers, with assurance obtained for outsourced services.
- **Physical & Environmental Security** - controlled access to premises, data center and sensitive areas with monitoring and environmental safeguards.
- **Vulnerability Management** - periodic vulnerability assessment and penetration testing with time-bound remediation.
- **Data disaster management and reboot:** A separate documented Disaster Recovery Plan defines RTO/RPO for critical applications, recovery teams and system restoration procedures. Critical applications are cloud-hosted with vendor-managed resilience; data is backed up daily and recoverability is validated through periodic restoration testing.

6.0 Cyber Incident Response

- The Company maintains an Incident Management procedure defining reporting channels, severity classification, response and escalation timelines, and root cause analysis.
- All users must report suspected security incidents to the IT department immediately.

- Significant cyber incidents are escalated to Top Management and reported to regulatory authorities (including CERT-In) where required under applicable directions.

7.0 Awareness & Training

The Company conducts periodic security awareness communication and training for employees, covering safe computing practices, phishing and social engineering, incident reporting, and acceptable use of Company IT resources.

8.0 Compliance

- This policy operates in conjunction with the Company's Information Technology Policy, Cyber Risk Management Policy and supporting IT policies and SOPs.
- The Company complies with applicable legal and regulatory requirements including the Information Technology Act, 2000, CERT-In directions, the Companies Act, 2013 (including audit trail requirements for books of account), and the Digital Personal Data Protection Act, 2023.
- Compliance with this policy is subject to periodic internal review and independent audit.

9.0 Policy Review

This policy is reviewed at least annually, and upon significant changes to the threat landscape, business operations or regulatory requirements.

10.0 Enforcement

Violation of this policy may result in disciplinary action in accordance with Company policies, and in the case of contractors or vendors, termination of contract or assignment. Where applicable, violations may also be reported to law enforcement authorities.

Revision History

v1 - Initial release.
v2 -Updated

