DCM SHRIRAM
Growing with trust

Enterprise Information Security & Management Policy Statement

1. Introduction

DCM Shriram Limited recognizes information as a vital corporate asset essential for safe, secure, and uninterrupted business operations. This policy statement integrates the principles of global best practices while reflecting DCM Shriram's own security governance framework, including policies for Network Security, Application Security, Cloud Security and Information Asset Classification & Handling.

The Company is committed to protecting the confidentiality, integrity and availability of all information—whether physical, digital, cloud-based or operational technology (OT)—to uphold business resilience, regulatory compliance and stakeholder trust.

2. Purpose

This document establishes DCM Shriram's overarching commitment to:

- Govern and manage information security risks consistently across the enterprise.
- Ensure secure handling of all information assets throughout their lifecycle.
- Create a unified policy foundation for implementation across all business units, SBUs and shared services.
- Reinforce accountability and clearly defined roles in maintaining a secure information environment.

3. Scope

This policy applies to:

- All DCM Shriram businesses, divisions, SBUs, manufacturing units and corporate/shared service functions.
- All employees, contractual staff, trainees, vendors, consultants and third-party service providers.
- All forms of information—digital, physical, cloud-hosted, application-generated, operational technology and network-connected assets—across all operating locations.

4. Policy Commitments

4.1 Governance & Oversight

- Maintain an integrated Information Governance and Security framework aligned with DCM Shriram's business objectives.
- Ensure compliance with applicable statutory, regulatory, contractual and internal policies.
- Conduct periodic reviews and audits to maintain effectiveness and adapt to emerging risks.
- Establish clear accountability structures across functions for implementing security controls.

4.2 Information Security Management

- Protect all information assets to ensure confidentiality, integrity and availability.
- Define and enforce information classification and handling guidelines.
- Apply secure processes for storing, accessing, transmitting and disposing of information.
- Monitor access to systems and ensure logging of critical system events.

4.3 Technology, Application & Cloud Security

- Integrate secure development practices across the application lifecycle.
- Implement controls for cloud security, including identity management, encryption, third-party provisioning and data residency.
- Ensure appropriate technical safeguards for IT/OT environments and interfaces.

4.4 Network, System & Endpoint Security

- Maintain secure network architecture including firewalls, intrusion detection/prevention and continuous monitoring.
- Ensure systems remain updated with relevant patches, antivirus and malware protection.
- Enforce authentication standards, including multi-factor authentication where required.
- Secure endpoint devices including laptops, desktops, mobile devices and IoT/OT assets.

4.5 Physical & Facility Security

- Safeguard premises, data centers, server rooms and sensitive operational areas from unauthorized access, damage and interference.
- Apply layered access controls and surveillance mechanisms wherever necessary.

4.6 Third-Party & Supplier Security

- Ensure vendors and service providers adhere to DCM Shriram's information security requirements.
- Conduct regular assessments, audits and performance reviews.
- Define clear contractual obligations including confidentiality, data protection and incident reporting.

5. Roles & Responsibilities

- **Business/Functional Leadership**: Enforce compliance within respective units; ensure implementation of security controls.
- **Corporate IT & Information Security**: Develop policies, deploy controls, monitor compliance and manage incident response.
- **Employees & Authorized Users**: Safeguard information, follow usage guidelines, maintain password hygiene, prevent misuse and report anomalies.
- **Third-Party Providers**: Adhere to contractual security requirements and cooperate with audits, assessments and incident procedures.

6. Incident Reporting & Response

- All suspected or confirmed information security incidents must be reported immediately to Corporate IT & Information Security.
- A structured response mechanism—including investigation, containment, remediation and communication—will be followed.
- Documentation and root-cause analysis will guide improvements to prevent recurrence.

7. Policy Review & Continuous Improvement

This policy will be reviewed at least once every two years, or earlier when required due to:

- Regulatory or statutory changes
- Business expansion or technology transformation
- Emerging threats or security incidents

Continuous improvement will be driven through internal audits, assessments and evolving best practices.

21st May 2026

Approved by
ED and Group Chief Information Officer