CYBERSECURITY POLICY OF SIGNATUREGLOBAL (INDIA) LIMITED

(Formerly known as Signatureglobal (India) Private limited)

(Approved by the ESG Committee on 03.03.2024)

Cybersecurity Policy

Updated: 03rd March 2025

1. Objective

The digital transformation of the real estate industry presents opportunities for operational excellence, stakeholder engagement, and innovation. However, it also brings heightened cybersecurity risks. This Cybersecurity Policy establishes Signatureglobal (India) Limited's commitment to protecting its digital infrastructure, sensitive data, and stakeholder trust from cybersecurity threats.

2. Scope

This policy applies to all employees, contractors, consultants, service providers, and third-party users who have access to Signatureglobal (India) Limited's IT systems, networks, applications, and data platforms.

3. Commitments & Measures

3.1 Cybersecurity Management System

Signatureglobal (India) Limited will maintain an enterprise-wide cybersecurity framework that includes:

- Identification, classification, and mitigation of **information security risks**
- Governance structures aligned with **ISO/IEC 27001** and **CERT-In** guidelines
- Policies covering data protection, access control, password management, endpoint security, and cloud services

3.2 Security Monitoring & Response

- Deploy **advanced cybersecurity tools** including firewalls, intrusion detection systems, and AI-based monitoring to detect anomalies in real-time
- Perform **penetration testing** and **vulnerability assessments** for all new platforms prior to deployment
- Establish and periodically test **Cyber Incident Response Plans (CIRPs)** for high-priority systems and business continuity
- Maintain logs of cybersecurity events and conduct **forensic investigations** where necessary

3.3 Compliance with Data Privacy Regulations

- Ensure adherence to the Digital Personal Data Protection Act, 2023
- Implement controls to protect Personally Identifiable Information (PII) and financial data of customers, employees, and vendors
- Retain and dispose of data in accordance with applicable retention laws and consent protocols

3.4 Third-Party and Vendor Security

- Evaluate IT vendors and software providers for cybersecurity risks prior to onboarding
- Include cybersecurity and data privacy clauses in contracts, with clear accountability and response timelines
- Require vendors to report incidents promptly and follow Signatureglobal (India) Limited's information security practices

3.5 Audit and Assurance

- Conduct periodic **internal and external cybersecurity audits** to evaluate control effectiveness
- Engage third-party security firms to perform **annual cybersecurity maturity assessments**
- Report key cybersecurity risks and response actions to the **ESG Steering Committee (also known as the ESG Committee)**

3.6 Employee Training & Awareness

- Deliver mandatory training to all staff on:
- Email phishing and social engineering threats
- Password hygiene and multi-factor authentication (MFA)
- Cyber incident reporting and escalation

- Display infographics, videos, and best practices on digital noticeboards and intranet platforms
- Include cybersecurity modules in employee onboarding and refresher programs

---

4. Governance & Oversight

The **Chief Technology Officer (CTO)** or equivalent IT security lead shall be responsible for:

- Implementing and updating this policy
- Coordinating incident response teams
- Reporting to the **Risk Management Committee** on major risks, policy revisions, and system improvements

---

5. Continuous Improvement

This policy shall be reviewed annually in light of:

- Evolving threat landscapes and technologies
- Emerging regulatory and legal developments
- Changes in Signatureglobal (India) Limited’s digital operating model