



Information Security and Data Privacy

2025-26



Data privacy and information security

As a global digital services organisation, Coforge recognises that strong data privacy, information security, and cyber resilience are foundational to digital trust, regulatory compliance, and long-term sustainable growth. The Company is committed to safeguarding the confidentiality, integrity, and availability of customer, employee, and stakeholder information across all its operations.

Governance, oversight, and accountability

Coforge maintains a robust governance structure to oversee information security and data protection across the enterprise. Executive leadership provides strategic direction through formal committees, including the Information Security Steering Committee (ISSC), Risk Management Committee (RMC), and Privacy Committee, ensuring accountability and alignment with business objectives. The CIO Office provides periodic (half-yearly) updates to the RMC on the organisation's information security posture, cyber risks, mitigation measures, and emerging threat landscape.

Information security, privacy, and acceptable use policies are reviewed at least annually or upon significant regulatory or organisational change. These policies are communicated to all employees and reinforced through training and internal awareness initiatives.

Certifications, standards, and framework alignment

Coforge follows a unified ISO-based governance approach to ensure consistent risk management, control implementation, and continual improvement across all delivery centres. The Company maintains formal certifications for:

- **ISO/IEC 27001** – Information Security Management System (ISMS)
- **ISO/IEC 27701** – Privacy Information Management System (PIMS)
- **ISO 22301** – Business Continuity Management System (BCMS)

In addition, Coforge aligns its controls with globally recognised frameworks such as the **NIST Cybersecurity Framework** and **CIS Critical Security Controls and Benchmarks** to strengthen technical safeguards, harden system configurations, and reduce exposure to common cyber threats. Independent assurance is further supported through certifications, including **SOC 2 Type II, Cyber Essentials Plus, HITRUST (E1), HIPAA**, and **CMMI Level 5**, providing customers with confidence in the design and operating effectiveness of Coforge's controls.

Data privacy and protection

Privacy-by-design and privacy-by-default principles are embedded across the data lifecycle at Coforge. The Company has implemented **ISO/IEC 27701-aligned PIMS across all India delivery locations**, strengthening its ability to manage personal data in line with global regulatory expectations. Key privacy practices include:

- Defined triggers for conducting Data Protection Impact Assessments (DPIAs) for high-risk processing activities
- Maintenance of data inventories, records of processing activities, and data flow mapping
- Structured mechanisms for managing data subject rights requests
- Privacy reviews integrated into project onboarding, solution design, and change management processes
- Data retention and secure disposal controls aligned with legal, regulatory, and contractual requirements
- Vendor privacy due diligence and contractual safeguards
- Privacy incident and breach management procedures, including regulatory assessment and notification requirements
- Regular privacy awareness and training programmes for employees handling personal data
- Periodic privacy compliance assessments, internal audits, and governance oversight to support continuous improvement

Coforge does not use customer or personal data for any secondary, unauthorised, or non-contractual purposes. During the reporting period, the Company did not receive any material or direct government or law enforcement requests for customer or employee data.

To enhance regulatory preparedness and breach response readiness, Coforge has also onboarded a leading global law firm to provide jurisdiction-specific legal guidance on data protection regulations, incident response, regulatory engagement, and notification obligations across geographies.

Zero substantiated complaints concerning breaches of customer privacy, losses of customer data, or identified incidents of leaks, thefts were reported during FY2025–26

During FY2025–26, Coforge did not receive any material requests from government or law-enforcement authorities for disclosure of customer data

Cybersecurity operations and threat management

Coforge operates a 24x7 Security Operations Centre (SOC) supported by global threat intelligence to continuously monitor critical systems and respond to threats in near real time. The cybersecurity ecosystem includes advanced capabilities such as next generation SIEM, AI-enabled SOAR, endpoint detection and response (EDR), data loss prevention (DLP), identity and access management, and network security controls.

Attack surface and exposure management practices, including periodic vulnerability assessments and penetration testing, are applied across delivery environments. Security incidents are addressed through a structured incident response framework aligned with defined escalation paths and recovery objectives.

Risk management and business continuity

Information security and privacy risks are integrated into Coforge's Enterprise Risk Management (ERM) framework. All delivery centres undergo periodic risk assessments, and findings are reviewed by senior management for corrective and preventive action.

Coforge's BCMS, aligned with ISO 22301:2019, ensures operational resilience through defined Business Continuity and Disaster Recovery plans. These plans are validated through regular simulations, tabletop exercises, and testing to maintain service availability and protect data integrity during disruptive events.

Awareness, training and culture

Coforge fosters a strong culture of information security and digital responsibility. All eligible employees undergo mandatory pre-onboarding, induction, and annual information security and privacy training. Awareness initiatives are supplemented through phishing simulations, targeted advisories, newsletters, and leadership-driven campaigns.

Any violations of information security or privacy policies are addressed through defined disciplinary procedures in line with organisational policies and applicable regulatory requirements, reinforcing accountability and responsible data handling across the workforce.

Overall impact

These measures collectively reinforce Coforge's commitment to accountable data protection, regulatory compliance, and responsible digital practices. By continuously strengthening governance, technology safeguards, and workforce awareness, Coforge enables trusted digital operations and supports long-term sustainable growth in an evolving cyber and regulatory landscape.

Business continuity planning (BCP)

We have established a robust **Business Continuity Management (BCM) system**, demonstrating the maturity of our Business Continuity Planning. Coforge has achieved **ISO 22301:2019 certification**. This certification reflects our strong capabilities in maintaining resilient operations and ensuring uninterrupted service delivery across key locations.

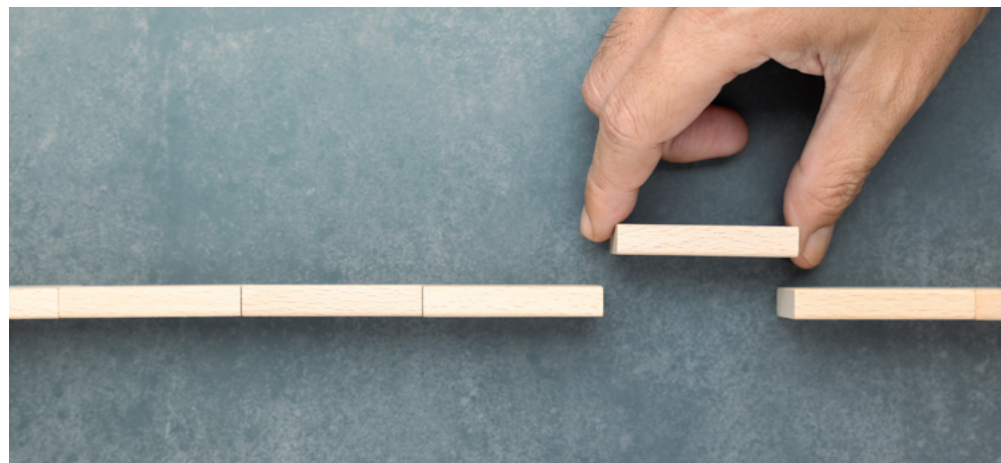
Advanced initiatives

In FY2025–26, we advanced our resilience framework through several new initiatives:

- **Enterprise-wide Privileged Access Management (PAM):** Ensures controlled, monitored, and Just in Time access to privileged accounts, reducing risks of misuse.
- **Automated detection and autonomous response:** Adoption of advanced technologies to rapidly contain threats such as ransomware, enhancing operational resilience.
- **Zero trust security framework:** A globally recognised, proactive approach to cybersecurity that prioritizes data protection and governance, maximizing the business value of customer data while minimising compliance risks.

Governance and oversight

- **Board and leadership commitment:** Oversight of BCP implementation and integration with enterprise risk management.
- **Continuous improvement:** Regular reviews and updates to incorporate lessons learned, evolving threats, and industry best practices.
- **Alignment with global standards:** Coforge's BCM system aligns with ISO 22301 and contributes to risk management, resilience, and cybersecurity.





Registered Office

Coforge Limited

Plot No. 13, Udyog Vihar, Phase-IV,
Sector-18, Palam Road,
Gurugram - 122015, Haryana, India

Tel: 0124-4627837

Corporate Office

Coforge Limited

SEZ Developer Unit,
Plot No TZ 2 & 2A, Sector Tech
Zone, Greater Noida, Gautam
Buddha Nagar, UP-201308.

Tel: 0120-4592300

Website: www.coforge.com | CIN: L72100HR1992PLC128382