Data Privacy and Security

Safeguarding data is a fundamental priority for Dubai Taxi Company, reflecting its commitment to customer trust, regulatory compliance, and operational integrity. By maintaining stringent controls over data management and protection, DTC strengthens cybersecurity resilience and reinforces its reputation as a trusted, technology-driven sustainable mobility provider.

Management Approach

DTC's data governance is overseen by a dedicated IT Department, supported by a suite of internal policies that define security standards, protocols, and accountability mechanisms. At the same time, the data privacy systems and procedures are overseen by the Information Security and Governance Department. The privacy policy is embedded within the Company's corporate compliance and risk management system, with employees receiving mandatory training on privacy and data protection. This comprehensive approach ensures that information assets are managed responsibly and in line with regulatory and industry best practices.

Key policies governing data privacy and security include:
- Data Privacy and Security Policy
- IT Policy
- Data Confidentiality Policy
- Data Constancy Policy

With regard to disciplinary actions in cases of privacy policy breaches, Dubai Taxi Company has established internal procedures to address violations in accordance with company governance rules.

Cybersecurity and Data Protection Measures

As part of its ongoing IT transformation, DTC is advancing initiatives to strengthen cybersecurity, compliance, and operational efficiency. During 2025, the Company achieved the ISO 27001 certification, a milestone that formalised its information security management framework. As part of this achievement, the IT Department has completed a comprehensive risk review and developed an internal risk register aligned with ISO requirements.

DTC manages cybersecurity risks through a combination of people, process, and technology controls. Employee awareness is reinforced through regular training, monthly phishing simulations, and targeted sessions on identifying and responding to digital threats.

System resilience is supported through routine penetration testing, code reviews, and the phased adoption of secure platforms such as Oracle Fusion. Together, these measures strengthen IT governance, enhance data protection, and support consistent compliance with data privacy and security requirements.

0
Instances of legal proceedings associated with user privacy

Data Privacy and Security Enhancements in 2025

In 2025, DTC significantly strengthened its cybersecurity and data protection capabilities through the establishment of dedicated operational centres and enhanced threat management mechanisms.

The enhancements include:

- **24/7 Security Operations Center (SOC)** established to provide continuous monitoring, threat detection, and real-time cybersecurity oversight across systems and platforms.
- **24/7 Network Operations Center (NOC)** launched to ensure network performance, stability, and rapid issue resolution across digital infrastructure.
- Implementation of enhanced **Threat Intelligence capabilities**, enabling proactive identification of emerging cyber risks and vulnerabilities.
- Strengthened **Incident Response and Digital Forensics framework**, improving investigation speed, containment effectiveness, and recovery coordination.
- Deployment of a **company-wide cybersecurity awareness platform**, reinforcing staff vigilance through structured training and simulated threat exercises.

Together, these enhancements have elevated DTC's cybersecurity maturity, strengthening data protection governance, supporting safe and secure digital mobility operations.