PRESS RELEASE

IFSCA Issues Comprehensive Cybersecurity Guidelines for Market Infrastructure Institutions in GIFT IFSC

The International Financial Services Centres Authority (IFSCA) today issued the "Guidelines on Cyber Security and Cyber Resilience for Market Infrastructure Institutions (MIIs) in IFSC" **(Circular No. IFSCA-CSD/MSC/2/2026-DCS),** establishing a prescriptive and comprehensive cybersecurity framework tailored for stock exchanges, clearing corporations, depositories, and the bullion exchange operating within GIFT IFSC.

Building upon IFSCA's baseline cybersecurity guidelines issued on March 10, 2025 for all Regulated Entities, the guidelines recognise the systemic importance of MIIs and prescribes a heightened, more granular set of obligations. The Guidelines are structured around seven core cybersecurity functions: Govern, Identify, Protect, Detect, Respond, Recover, and Resilience, mirroring globally recognised frameworks while embedding the operational and jurisdictional realities of GIFT IFSC.

KEY HIGHLIGHTS OF THE GUIDELINES

Board-Level Governance & Accountability: MIIs are required to have a Board-approved Cyber Security and Cyber Resilience Policy, with a dedicated Chief Information Security Officer (CISO) reporting directly to the MD/CEO.

Future-Ready: Post-Quantum Cryptography (PQC): In a forward-looking provision, MIIs must conduct annual Cryptographic Risk Assessments and establish roadmaps for adopting PQC standards (e.g. NIST FIPS 203, 204 and 205) to future-proof critical systems against quantum computing threats.

24x7 Cyber Security Operations Centre (C-SOC): All MIIs shall have a round-the-clock C-SOC with contingent capabilities at Disaster Recovery sites, and implement User and Entity Behaviour Analytics (UEBA) for advanced threat detection.

Robust Incident Response & Reporting: MIIs must notify IFSCA and CERT-In within 6 hours of detecting any cyber incident, submit an interim report within 3 days, and provide a full root-cause analysis within 30 days.

Third-Party & Supply Chain Risk: A risk-based approach to third-party management is mandated, including concentration risk management and contractual cyber security obligations for all critical service providers.

ISO 27001 Certification: All MIIs are required to obtain ISO 27001 certification within two years of issuance of the Guidelines.

Alignment with National Standards: The framework is aligned with the IT Act 2000, the Digital Personal Data Protection Act 2023, and directives from CERT-In, NCIIPC, MeitY, and NQM, ensuring seamless integration with India's national cybersecurity architecture.

Effective Date: The Guidelines came into effect on April 1, 2026. MIIs are required to achieve full compliance within the timelines prescribed in the respective provisions of the Guidelines.

The circular is available on the IFSCA website at **www.ifsca.gov.in**

ABOUT IFSCA

The International Financial Services Centres Authority (IFSCA) is the unified regulatory authority for the development and regulation of financial products, financial services, and financial institutions in International Financial Services Centres (IFSCs) in India. Established under the IFSCA Act, 2019, it regulates banking, capital markets, insurance, and fund management activities within GIFT IFSC, India's first and only operational IFSC.

April 20, 2026
GIFT City, Gandhinagar