CIRCULAR

IFSCA-CSD/MSC/05/2026-DCS **November 25, 2026**

To,

All Regulated Entities in the International Financial Services Centres (IFSCs)

Dear Madam/Sir,

Sub: Adherence to advisories and vulnerability notes issued by the Indian Computer Emergency Response Team (CERT-In)

1. IFSCA, vide circular dated March 10, 2025, issued the 'Guidelines on Cyber Security and Cyber Resilience for Regulated Entities in IFSCs', as amended vide circular IFSCA-CSD/MSC/1/2026-DCS dated March 10, 2026 (hereinafter referred to as the 'Guidelines on Cyber Security for all REs'), prescribing a principles-based minimum baseline framework applicable to all Regulated Entities (REs). Subsequently, vide circular IFSCA-CSD/MSC/2/2026-DCS dated April 20, 2026, IFSCA issued the 'Guidelines on Cyber Security and Cyber Resilience for Market Infrastructure Institutions (MIIs) in IFSC' (hereinafter referred to as the 'Guidelines on Cyber Security for MIIs').

2. The Indian Computer Emergency Response Team (CERT-In), the national agency for incident response under Section 70B of the Information Technology Act, 2000 (hereinafter referred to as the 'IT Act'), regularly issues advisories and vulnerability notes on cyber threats and vulnerabilities affecting software, hardware and services, along with the recommended countermeasures. These are published on the website of CERT-In (www.cert-in.org.in).

3. The Guidelines on Cyber Security for MIIs, inter alia, require the MIIs to:

   i) align their log retention policy with the guidelines and directions issued by CERT-In

   ii) align their Vulnerability Assessment and Penetration Testing with the applicable guidelines and requirements prescribed by the National Critical Information Infrastructure Protection Centre (NCIIPC) and CERT-In

iii) report cyber incidents to CERT-In in accordance with the guidelines and directions issued by CERT-In from time to time.

4. Accordingly, with a view to strengthening cyber resilience and ensuring timely identification, assessment and remediation of known vulnerabilities across the IFSC ecosystem, it has been decided that all REs shall ensure compliance with the applicable advisories and vulnerability notes issued by CERT-In from time to time. Such compliance shall extend to all relevant IT systems, applications, network infrastructure and services deployed, operated or managed by the REs, including those hosted, operated or managed on their behalf by parent entities, group entities or third-party service providers.

REs shall be responsible for ensuring compliance with these requirements, irrespective of the ownership, hosting or operational management arrangements governing such systems and services.

Towards this effect, all REs, including the MIIs, shall:

a) Put in place a mechanism for the timely receipt, monitoring and tracking of advisories and vulnerability notes issued by CERT-In. This shall include regular monitoring of the official CERT-In website, subscription to CERT-In alerts and maintenance of an appropriate internal tracking mechanism to ensure that relevant advisories are promptly identified and acted upon.

b) Assess, without undue delay, each advisory and vulnerability note for its applicability to the RE's IT systems, applications, network devices and services, including those hosted, operated or managed on its behalf by its parent entity, group entity or third-party service provider.

c) Implement the countermeasures recommended by CERT-In, such as patches, configuration changes or compensating controls, within the timelines specified in the patch management policy of the RE, which shall be commensurate with the severity of the vulnerability. Vulnerabilities rated as critical or high severity by CERT-In in the relevant advisory or vulnerability note, those known to be actively exploited and those affecting internet-facing systems shall be accorded the highest priority for remediation.

d) Where a recommended countermeasure cannot be implemented within the timelines referred to in clause (c) above, the RE shall formally document:

- the reasons thereof
- the associated risks
- the compensating controls adopted
- the expected date of implementation

with the approval of the Designated Officer referred to in para 6 of the Guidelines on Cyber Security for all REs, or in the case of MIIs, the Chief Information Security Officer (CISO) appointed in terms of para 7 of Annexure A to the Guidelines on Cyber Security for MIIs.

e) Maintain adequate and verifiable records of the assessment of each CERT-In advisory and vulnerability note and the action taken thereon. Such records shall be made available to IFSCA as and when sought and to the cyber security auditor for examination during the course of the cyber security audit.

5. Clauses (b) to (e) of para 4 above shall apply to the advisories and vulnerability notes issued by CERT-In on or after the date of this circular.

6. REs operating within group-wide security arrangements may rely on group-level arrangements for compliance with para 4 above, provided that such arrangements cover the systems supporting their operations in the IFSC and the records referred to in para 4(e) above are available with the RE and can be produced to IFSCA as and when sought. The responsibility for compliance shall remain with the RE.

7. REs are also reminded that the Directions issued by CERT-In under Section 70B(6) of the IT Act, vide No. 20(3)/2022-CERT-In dated April 28, 2022, apply to them independently of the guidelines issued by IFSCA. These include the requirements to report cyber incidents to CERT-In within six (6) hours of noticing such incidents or being brought to notice about such incidents, and to maintain logs of all ICT systems securely for a rolling period of 180 days. The REs shall also ensure that logs maintained on their behalf by their parent entity, group entity or third-party service provider are maintained, and can be produced to CERT-In, in accordance with the said Directions.

8. Compliance with this circular shall be covered in the annual cyber security audit of the RE under the Guidelines on Cyber Security for all REs, or in the case of MIIs, the annual cyber audit under the Guidelines on Cyber Security for MIIs. This para shall

not apply to the REs exempted from the annual cyber security audit under para 23 of the Guidelines on Cyber Security for all REs.

9. REs shall put in place the mechanism referred to in para 4(a) above within thirty (30) days from the date of this circular.

10. This Circular is issued in exercise of the powers conferred by Sections 12 and 13 of the International Financial Services Centres Authority Act, 2019, to develop and regulate the financial services market in the International Financial Services Centre.

This Circular shall come into force with immediate effect. A copy of this circular is available on the website at www.ifsca.gov.in.

Yours Faithfully,

Praveen Kamat
Chief General Manager & CISO
Division of Cyber Security
Email: praveen.kamat@ifsca.gov.in
Tel: +91- 079 - 61809820