CIRCULAR

IFSCA-CSD/MSC/3/2026-DCS **June 04, 2026**

To,

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

Dear Madam/Sir,

Sub: Advisory on Heightened Cyber Security Risks arising from Frontier Artificial Intelligence Models

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, prescribing a principles-based minimum baseline framework applicable to all Regulated Entities. 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'. This advisory shall be read in conjunction with the applicable guidelines, and does not dilute any obligation thereunder.

2. Recent advances in frontier Artificial Intelligence (AI) models represent an accelerated change in offensive cyber capabilities. Such models can analyse large and complex codebases, identify known and previously unknown (zero-day) vulnerabilities, reason about exploitability, and generate working exploits, at a speed, scale and cost that significantly lowers the barrier to mounting sophisticated attacks, compressing the time between disclosure of a vulnerability and its exploitation from weeks to hours.

3. Although the most capable of these models are presently subject to restricted availability, such capabilities are expected to diffuse rapidly. Accordingly, REs should strengthen their security posture ahead of the wider availability of such models and should reassess their cyber security risk and implement mitigating controls in accordance with the principle of proportionality.

4. REs are encouraged to comply with the measures set out in Annexure A.

5. 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
Division of Cyber Security
Email: praveen.kamat@ifsca.gov.in
Tel: +91- 079 - 61809820

ANNEXURE A

1. REs shall presume that newly disclosed critical vulnerabilities are exploitable within hours of publication. Accordingly, REs should prepare for vulnerability patch waves, wherein a large number of vulnerabilities across the technology stack are identified and weaponised within a compressed window.
2. REs shall explicitly incorporate the capabilities and risks arising from Frontier AI Models as a defined scenario within their cyber security risk assessments. Such assessments shall be periodically reviewed and placed before the Board, and, in the case of Market Infrastructure Institutions (MIIs), before the Standing Committee on Technology.
3. REs shall maintain a Software Bill of Materials (SBOM) including, but not limited to open-source components, to enable timely and effective impact assessment during a vulnerability patch wave.
4. REs are encouraged to implement phishing-resistant Multi-Factor Authentication (MFA) for all internet-facing systems and privileged access. MFA enrolment, as well as any modification to a registered MFA device, shall be permitted only through an authorised process supported by robust identity verification. For critical and production systems, REs are encouraged to use strong identity controls, such that compromise of credentials alone does not result in unauthorised access.
5. REs are encouraged to prioritize patching of the vulnerabilities most likely to be exploited.
6. REs shall maintain a comprehensive inventory of all APIs and the applications consuming them. REs shall implement appropriate rate-limiting and throttling controls to detect and prevent automated abuse and shall restrict API connectivity to a whitelist of authorised entities.
7. REs shall require their critical service providers to assess the risks arising from Frontier AI Models and to furnish evidence of preparedness for accelerated exploit timelines. REs shall ensure timely and scalable remediation of vulnerabilities identified in, or attributed to, third party systems and dependencies.
8. REs shall strengthen monitoring and detection capabilities to identify activity indicative of AI-driven attacks, including automated reconnaissance, abnormally rapid scanning or access patterns, and attack sequences that exceed plausible human-operated timelines.
9. REs are encouraged to establish rapid response mechanisms for credential compromise, including automated credential resets, account lockouts and

continuous monitoring, with the objective of enabling response within minutes rather than hours.

10. REs are encouraged to adopt AI-assisted vulnerability detection tools commensurate with the speed and scale of AI-driven threats. Where the use of such tools involves transmission of source code, configurations, logs or other sensitive or regulated information to an AI model, REs shall ensure that:

    a) such use is authorised,

    b) sensitive or regulated data is not exposed to unapproved external services, and

    c) the model provider's data-handling, retention and confidentiality terms are adequate.

11. Where AI or automation is utilized for vulnerability identification or remediation, REs shall ensure appropriate human oversight and shall subject AI-generated or AI-remediated code to rigorous security testing prior to deployment in production environments.

***