CIRCULAR

IFSCA-CSD0MSC/13/2025-DCS **March 10, 2025**

To,

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

Dear Madam/Sir,

Subject: Guidelines on Cyber Security and Cyber Resilience for Regulated Entities in IFSCs

1. As the IFSC continues to evolve as a global financial hub, the sophistication of cyber threats targeting financial entities is also expected to grow. In such an international jurisdiction, where institutions cater to a diverse global client base, maintaining robust cyber security becomes fundamental. The ability of financial entities to protect their IT systems from being compromised by threat actors—whether through fraudulent financial transactions, breach of sensitive data, or the disruption of critical IT infrastructure—directly impacts the trust placed in the jurisdiction.

   Consequently, cyber security is not just a necessity but a foundational pillar for ensuring the stability, resilience, and credibility of the financial services offered within the GIFT IFSC. These Guidelines on cyber security and cyber resilience intend to lay down International Financial Services Centres Authority (IFSCA)'s broad expectations from its Regulated Entities ("REs"). For the purpose of these Guidelines, REs shall include any entity which is licensed, recognised, registered or authorised by IFSCA. The implementation of these Guidelines shall be undertaken in accordance with the **principle of proportionality**, after taking into due consideration:

a. the scale and complexity of operations,
b. the nature of the activity the entity is engaged in,
c. its interconnectedness with the financial ecosystem and
d. the corresponding cyber risks the entity is exposed to.

2. The key components of the Guidelines are categorized into:

I. Governance
II. Cyber security and cyber resilience framework
III. Third party risk management
IV. Communication & awareness
V. Audit

I. Governance

3. The REs shall have adequate governance mechanisms, with a clear set of roles and responsibilities to manage cyber risk. The set of stakeholders involved in the governance of an RE's cyber risk management mechanism shall collectively be referred to as the "Oversight Body" of the RE and may include one or more of the following:

i. Governing Board, or
ii. Senior management personnel which include the Managing Director (MD), Chief Executive Officer (CEO), Chief Information Security Officer (CISO), Chief Technology Officer (CTO), Principal officer, Compliance officer or
iii. Committee(s) involving/ designated by any of the above for the purpose of technology or cyber risk management of the RE

4. The REs shall ensure that their Governing Board and the senior management possesses sufficient expertise and knowledge to effectively understand and manage cyber risk. The Governing Board and senior management shall set the tone at the highest levels

and cultivate a strong culture of cyber risk management and awareness at all levels of staff within the entity.

5. The REs shall appoint a CISO or alternatively, designate a senior employee/ management personnel to
    a. assess, identify and reduce cyber security risks,
    b. respond to incidents, establish appropriate standards and controls, and
    c. direct the establishment and implementation of processes and procedures as approved by the Oversight Body of the RE

6. The CISO or senior employee/ management personnel so designated shall henceforth be referred to as the "Designated Officer".

II. Cyber Security and Cyber Resilience framework

7. The REs shall formulate the Cyber Security and Cyber Resilience Framework to maintain the Confidentiality, Integrity and Availability of their IT assets. The said framework, inter alia, shall:

    i. aim to maintain and promote the RE's ability to anticipate, withstand, contain, and recover from cyber-attacks.
    ii. take an integrated and comprehensive view of the potential cyber threats, including third party risks that the RE faces.
    iii. define the RE's cyber risk appetite and cyber resilience objectives.
    iv. outline the RE's people, process and technology requirements for managing cyber risks.
    v. establish the roles and responsibilities of the Oversight Body, the Designated Officer, the employees and other stakeholders, including clear communication lines to be adhered to, during a cyber incident.
    vi. be reviewed and updated periodically to ensure that the framework stays relevant.

8. The Oversight Body shall ensure that the aforementioned framework is in accordance with the RE's overall risk management framework.

9. The REs shall formulate an Information Security (IS) Policy as part of their cyber security and cyber resilience framework with the following basic principles.

    a) <u>Identification and Classification of IT Assets</u>

        i. The REs shall maintain a detailed inventory of IT assets, including both logical (data, software) and physical (hardware) components, including system configurations, their interconnections with internal and external systems, with distinct and clear identification of the assets.

        ii. The REs shall carry out a risk assessment of those assets and classify the assets based on their business criticality, sensitivity of data they hold, and potential impact on other systems if compromised.

        iii. The REs shall identify and classify their business functions and supporting processes based on their criticality to overall operations and potential impact on performance. This classification shall guide the prioritization of security measures across protective, detective, response, and recovery efforts, focusing on mitigating risks associated with the most critical functions and processes.

    b) <u>Protection</u>

        The REs shall implement appropriate security controls, aligned with international best practices and cyber security and cyber resilience standards like NIST, ISO 27000, etc, to minimize the likelihood and impact of cyber-attacks on critical business functions, IT assets, and data. These controls must be

proportional to the RE's threat landscape and risk appetite. These controls shall be selected after taking into account the potential threat of compromise of technology, people and processes.

This may, inter alia, include measures pertaining to hardening of devices, network security, data security, patch management, disposal of systems and any other policies that aid in protection of the RE's IT assets.

c) Access Control

i. The REs shall manage access rights to IT assets and their supporting systems on a 'need-to-know' basis, following the principle of 'least privilege' (i.e., prevent unjustified access to a large set of data) and principle of 'segregation of duties' (i.e., to prevent the allocation of combinations of access rights that may be used to circumvent controls).

ii. The REs shall enforce authentication methods that are sufficiently robust to adequately and effectively ensure that access control policies and procedures are complied with.

d) Physical Security

The Confidentiality, Integrity and Availability of information can be impaired through physical access and damage or destruction to physical components. The REs need to ensure adequate physical security of their IT assets, using measures such as secure location of critical data, restricted access to data centers, server rooms etc.

e) Vulnerability Assessment and Penetration Testing (VAPT)

The REs shall conduct Vulnerability Assessment and Penetration Testing (VAPT) to detect vulnerabilities in the IT environment for all critical systems,

infrastructure components and other IT systems. The VAPT shall be conducted at least once a year.

f) Recovery

The REs shall have recovery policies and procedures to maximise their ability to provide services on an ongoing basis and to limit losses in the event of severe business disruption.

g) Incident Management

The IS Policy of the REs shall clearly define the term "cyber incident". The REs shall develop and implement processes for preventing, detecting, analysing and responding to cyber incidents. REs shall also establish mechanisms to fulfil the disclosure and reporting requirements, as specified by IFSCA, during and after a cyber incident.

h) Audit trail

The REs shall ensure that audit trail exists for IT assets, such that it:

a. satisfies the entity's business continuity and recovery needs,
b. satisfies the entity's regulatory and legal obligations,
c. facilitates audit and serves as forensic evidence when required, and
d. assists in dispute resolution.

III. Third Party Risk Management

10. The REs shall adopt a collaborative security approach with their third-party vendors/external partners, by clearly outlining shared expectations for data security, incident reporting and adherence to relevant security standards.

11. The REs shall adopt a risk-based approach for periodic review of third-party vendors/external partners. The REs shall identify the third-party service providers which it is dependent on for its core operations or to whom it has granted access to

its critical systems. For all such third-party service providers, the REs shall carry out an assessment for detecting vulnerabilities or compliance gaps through audit, review or feedback every six months. For other third-parties, the REs shall have the flexibility to determine the appropriate frequency for periodic review.

12. The REs should establish clear communication channels and escalation procedures for addressing any identified risks or non-compliance with partners, promptly and effectively.

13. The ultimate responsibility to mitigate the cyber risks arising from the third parties shall be on the REs.

IV. Communication & Awareness

14. The REs shall provide regular training to its employees on topics pertaining to cyber security, including but not limited to, phishing awareness, social engineering, password hygiene and incident reporting procedures.

15. The REs shall establish clear and accessible channels for employees to report suspicious activity, vulnerabilities, and potential cyber incidents.

V. Audit

16. The aim of the audit is to provide an independent assurance of the effectiveness of RE's measures to its Governing Board and the senior management. Towards this effect, the governance, systems and processes established by the REs for managing their cyber risks shall be audited on a periodic basis by either of the following:
    a. a CERT-In empanelled auditor,
    b. an independent auditor possessing the following certifications:
        i. Certified Information Security Auditor (CISA) or
        ii. Certified Information Security Manager (CISM) or
        iii. GIAC Systems and Network Auditor (GSNA) or
        iv. Certified Information Systems Security Professional (CISSP)

c. an auditor having prior experience in conducting cybersecurity audit of entities with similar business activity as that of the RE

The auditor shall also certify if the security controls implemented by the entity are aligned with the risks faced by the RE.

17. The auditor engaged by an RE shall not have any conflict of interest with the RE. The audit shall be conducted annually and a report in this regard shall be submitted to IFSCA by the REs within 90 days from the end of the financial year. The REs shall submit the audit report to the corresponding IFSCA Department/ Division in charge of the supervision of the RE.

    Though the minimum audit frequency prescribed is annual, REs may choose to adopt a higher frequency commensurate with their cyber risks and the criticality of their systems.

18. In case the RE is registered with IFSCA as a Broker Dealer/Bullion Trading Member, Clearing Member/Bullion Clearing Member or as a Depository Participant, and is required to submit cyber security audit report to a recognised Market Infrastructure Institution/Bullion Exchange, such REs may submit the same audit report to IFSCA within 7 days of submission of the audit report to the Market Infrastructure Institution/Bullion Exchange.

19. In case of occurrence of any cyber incident, the REs are required to report the particulars of the incident to the Authority on cyber-incidents@ifsca.gov.in with a copy to CISO, IFSCA, not later than six (6) hours from the detection of the incident.

20. Additionally, the REs shall submit the interim report within 3 days followed by a detailed root cause analysis report within 30 days. The REs shall take mitigation measures for the same within 7 days.

21. The following categories of REs are exempted from the requirements mentioned in these Guidelines:

    a. The REs operating in the form of a branch of a regulated Indian or foreign entity.
    b. The REs providing services to their group entities only e.g. Global In-House Centres (GICs).
    c. The REs which have less than 10 employees.
    d. Foreign universities set up in IFSCs.

22. The exemptions to the REs provided vide para 21, are subject to fulfilment of the following conditions:

    a. REs shall adopt the Cyber Security and Cyber Resilience framework and IS Policy of its parent entity.
    b. The CISO of the parent entity shall act as the Designated Officer for the REs in IFSC.
    c. The parent entity of REs, in India or overseas, shall be regulated by a financial-sector regulator in its home jurisdiction and cyber security and cyber resilience framework of the parent entity shall include within its scope, the REs in IFSC.

       The Designated Officer of the RE shall certify that all the necessary systems/processes have been put in place, which are in line with these Guidelines within 90 days of the end of each financial year. The said undertaking shall be submitted to the respective Department/ Division of IFSCA responsible for supervision of the RE.

These exemptions have been granted for a period of three years from the date of the issuance of these guidelines.

This Circular is issued in exercise of powers conferred by Section 12 and 13 of the International Financial Services Centres Authority Act, 2019 to develop and regulate the

financial products, financial services, and financial institutions in the International Financial Services Centres, and shall come into effect on April 1, 2025.

A copy of the circular is available on the website at www.ifsca.gov.in

Yours Faithfully,

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