भारतीय बीमा विनियामक और विकास प्राधिकरण
INSURANCE REGULATORY AND
DEVELOPMENT AUTHORITY OF INDIA

Ref No: IRDAI/GA&HR/CIR/MISC/49/03/2025 24th Mar, 2025

To,

All Regulated Entities, IIB and Training Institutes

Sub: - Regarding Cyber Incident or Crisis Preparedness

1. In today's digital age, any cyber incident and / or crisis pose significant threats to organizations and therefore it is crucial to be prepared to respond effectively to prevent or minimize damage to information assets, including customer data and ensure business continuity.

2. In this connection, attention is invited to various provisions of IRDAI Information and Cyber Security Guidelines, 2023, with respect to the captioned subject:

   a) Para 3.5 under Policy no. 2.10 and IRDAI circular ref: Ref: IRDAI/GA&HR/CIR/MISC/128/06/2023 dated 13/06/2023 i.e. Regulated Entities (REs) to **report any cyber incidents to IRDAI in prescribed format within 6 hours of noticing or being brought to notice** about such incidents;

   b) Para 3.3 under Policy no. 2.16 i.e. Monitoring, Logging and Assessment Para:

      I. all ICT infrastructure and application logs are to be **maintained and monitored for a rolling period of 180 days**;

      II. the clocks of all relevant information processing systems within Organization or security domain shall be synchronized with Network Time Protocol (NTP) Server of National Informatics Centre (NIC) or National Physical Laboratory (NPL) or with NTP Servers traceable to these NTP Servers.

   c) Para 3.3 under Policy no. 2.18 i.e. Situational Awareness provides for **Cyber Crisis Management Plan (CCMP)** as a part of organisations response for cyber-attacks;

d) Para 3.4 under Policy no. 2.20 i.e. Cyber Resilience provides for **performing forensic investigation** for severe information security incidents. One of the functions of CISO also provides engagement of external forensic experts who are certified as well as competent for the job as and when required.

(e) Para 1.10 under General Guidelines provided that Regulated Entities shall adhere to directions issued by Cert-In from time to time including relating to Incident Reporting to the CERT-In as per CERT-In direction dated 28th April 2022 on information security practices, procedure, prevention, response and reporting of cyber incidents for Safe & Trusted Internet.

3. It is once again re-iterated that all Regulated Entities **must strictly adhere** to the above provisions on cyber incident/crisis preparedness to ensure effective readiness.

4. In addition to the above, all Regulated Entities are required to **establish a well-defined procedure / practice to ensure that the forensic auditor/s are empanelled in advance and can be onboarded to conduct** forensics and root cause analysis of cyber incident/s **without any delay.**

5. Furthermore, it must be ensured that the vendor handling Security Operation Centre (SOC), attack surface monitoring, Red teaming, or conducting the annual assurance audit or any cyber security aspect of Regulated Entity is not engaged as the forensic auditor for the incident to **avoid a conflict of interest**.

6. All Regulated Entities, including insurance intermediaries are advised to place compliance to the above provisions to their Board in the ensuing Board Meeting and submit the minutes of the meeting to the Authority for information.

Yours faithfully,

24/3/25

(A.R. Nithiyanantham)
Executive Director (IT & Legal)