Tuli & Co
Solicitors and Advocates

**Information and Cybersecurity Guidelines 2023**

13 June 2023

***Introduction***

The insurance sector, both in India and worldwide, has long been a potential target for cyber-attacks, due to the vast amount of sensitive data held by Insurers and insurance intermediaries pertaining to their prospects and policyholders, including personal and financial data. Driven by advancements in IT infrastructure over the past decade, popularisation of cloud infrastructure and internet tools, and remote work arrangements necessitated due to the COVID-19 pandemic, the insurance sector in India has also seen shifts towards digitalisation in order to streamline their operations, increase business efficiencies and enhance the related customer experience. However, the shift is also recognised to have made the insurance sector more vulnerable to cyber threats.

Recognizing the need to safeguard the sector from such threats and address security threats, the IRDAI as the regulatory body has also been continually issuing and updating the norms applicable to Insurers and various stakeholders in relation to their organisation-wide information and cyber security. Prior to 2017, the norms on data protection and confidentiality applicable to Insurers[1] and insurance intermediaries[2] were spread across various regulations and circulars issued by the IRDAI[3]. Further, Insurers were also required to store their policy and claims records in servers/data centres located in India[4].

Thereafter, on 9 March 2017, the IRDAI issued its "*Guidelines on Insurance e-commerce*" ("**Ecommerce Guidelines**") which recognised websites and mobile applications set up by Insurers and insurance intermediaries for undertaking insurance e-commerce activities ("**ISNP**"), including any sales and servicing of insurance products on such ISNP. The Ecommerce Guidelines briefly set out norms on data security and localisation to be followed on their respective ISNPs[5].

Shortly after, on 7 April 2017 the IRDAI issued the "*Guidelines on Information and Cyber Security*

1 As an illustration, please see R3(3)(b) of the IRDAI (Maintenance of Insurance Records) Regulations 2015, R12 of the IRDAI (Outsourcing of Activities by Indian Insurers) Regulations 2017 and R35(c) of the IRDAI (Health Insurance Regulations) 2016.

2 Please refer to code of conduct as specified in the IRDAI (Registration of Corporate Agents) Regulations 2015, the IRDAI (Insurance Brokers) Regulations 2018, the IRDAI (Insurance Surveyors and Loss Assessors) Regulations 2015 and the IRDAI (Insurance Services by Common Public Service Centres) Regulations 2019.

3 ¶14(a)(x) of the IRDAI's "*Guidelines on Insurance e-commerce*" of 9 March 2017.

4 R3(9) of the IRDAI (Maintenance of Insurance Records) Regulations 2015.

5 ¶10 and ¶14(a)(x) of the IRDAI's "*Guidelines on Insurance e-commerce*" of 9 March 2017.

Article

*for Insurers*" ("**2017 Guidelines**") for Insurers (including FRBs[6]) which not only required Insurers to maintain confidentiality and security of the data but also set out an internal governance mechanism and a framework for information and cyber-security within an Insurer's database and systems. These guidelines were also amended in 2020 by way of the IRDAI's circular of 29 December 2020, which prescribed certain norms in relation to Vulnerability Assessment and Penetration Testing ("**VA&PT**") and closure of audit gaps. On 2 September 2022, the IRDAI extended the applicability of the above norms, in entirety, to insurance intermediaries[7] and certain other regulated entities[8] requiring them to comply with the norms, irrespective of their access to the Insurer's database. Simultaneously, the IRDAI also proceeded to constitute a committee to review the 2017 Guidelines, *inter alia*, in relation to the extent of its applicability to various entities (both regulated and unregulated), depending upon the extent of their access to the Insurers' IT systems.

Accordingly, the IRDAI has now issued the "*Information and Cyber Security Guidelines 2023*" on 24 April 2023 ("**Cybersecurity Guidelines**") for "*ensuring the security of all organization's information assets[9] through implementation of up-to-date security mechanisms for prevention and monitoring of threats; governance of information security related activities and awareness of all employees*."

The Cybersecurity Guidelines supersede the 2017 Guidelines and the various circulars issued on this subject earlier.

***Key Changes***

A brief summary of the key changes introduced by way of the Cybersecurity Guidelines are as follows:

1. Scope and applicability: The scope of the Cybersecurity Guidelines is much wider as compared to 2017 Guidelines. The norms continue to be applicable to all Insurers, but also expressly include insurance intermediaries and other entities such as insurance repositories, IIB, corporate surveyors, ISNPs, MISPs and CSCs (collectively, "**Regulated Entities**"). However, they do not apply to insurance agents, micro insurance agents, POSPs and individual surveyors, and instead, Insurers are now required to ensure that these individuals/entities follow the minimum information security framework as defined under the Insurers' Board approved policy. The Cybersecurity Guidelines provide specific instructions on how these



6 While the 2017 Guidelines did refer to "*all insurers regulated*", the IRDAI's clarificatory circular of 12 October 2017 expressly extended their applicability to FRBs by stating "*… recently registered insurers and **Reinsurers** also must ensure that steps are taken for implementation of the Guidelines.*".

7 IRDAI's circular on "*Re: Guidelines on Information and Cyber Security*" of 2 September 2022.

8 Please note that the IRDAI's circular on "*Implementation of Information and Cyber Security Guidelines – Reg.*" of 11 October 2022 extended the applicability of the 2017 Guidelines to insurance repositories, Insurance Information Bureau ("**IIB")**, insurance agents, corporate surveyors, ISNP, Motor Dealers, Common Service Centres ("**CSC**") and Point of Sale Persons ("**POSP**").

9 ¶1.2 of the Cybersecurity Guidelines defines the term "*information assets*" to include information/data in any form and systems required for organisation's business or operation, in the following terms:

> "*Information Assets comprise data or information recorded in electronic, printed, written, facsimile or other systems as well as the 'system' itself, required for Organization's business purpose or operations. Information Assets include business data, system logs, servers, desktops, network equipment, network media, storage media, paper, people etc*."

Regulated Entities should protect their databases and systems, reduce or manage cybersecurity risks, and improve their overall organisation-wide information security.

2. Organisational Structure: In terms of governance structure, the Cybersecurity Guidelines prescribe a structure for "*governance, implementation and monitoring of information security*" which includes the Board of directors, the Risk Management Committee, the Information Security Risk Management Committee[10], and the Information Security Team. In addition, while the 2017 Guidelines specified broad functions for the organisation's function heads (such as the CISO, CTO, CRO, HR) and various internal committees/sub-committees (such as the IS Team, Risk Management Committee), the Cybersecurity Guidelines now expressly contain detailed roles and responsibilities for each such function head and committee/sub-committee:

    a. The Board has now been made "*ultimately responsible*" for the information security of the organization, and is required to review "*quarterly inputs*" on information security matters.

    b. In relation to the CISO, who is responsible for overall governance and monitoring of an organisation's information security, the Cybersecurity Guidelines specifically require the CISO to perform various organisation wide functions such as the setting up of various IS standards (including training standards, vendor classification, business continuity etc), conducting VA&PT, access management to the organisation's information and data, reviewing of various exceptions to the organisation's information and cyber security policy etc.

3. Policies: The Cybersecurity Guidelines continue to require every organisation to have a Board approved Information and Cyber Security Policy ("**IS Policy**") along with the various other related polices/guidelines/plans. The Cybersecurity Guidelines now also prescribe certain additional norms in relation to the IS Policy:

    a. In relation to the contents of the IS Policy specifically, we note as an illustration that the 2017 Guidelines only required classification of data into different risk categories. However, the new Cybersecurity Guidelines also require the organisation to set out norms in relation to the storage, transfer, movement tracking, labelling, and data disposal/deletion requirements for each such risk category of data.

    b. Similarly, while the 2017 Guidelines only required that the acceptable use policy of an organisation should cover "*social media*", the Cybersecurity Guidelines now provide specific norms on such acceptable use, including norms on how the employees of the organisation may use social media for their corporate/personal purposes.

    c. Further, the Cybersecurity Guidelines have prescribed certain structural changes in relation to the IS Policy. In this regard, other existing polices/guidelines/plans (such as HR security, mobile security, asset management etc) have now been made different subsections/subparts of the IS Policy itself.

    d. In addition, the Cybersecurity Guidelines require every organisation to also include additional protocols within its IS Policy, such as a BYOD Policy, Change Control Policy,

10 The Information Security Risk Management Committee comprises of CRO, CISO, CHRO, CTP, CITSO, and function heads of operations, finance, legal and compliance.

Third Party Service Provider Policy, Legal and Regulatory Compliance Policy, Email Security Policy, Work from Remote Location Policy, and Dealing Room Operations Policy, and also prescribe norms on the contents of each such policy.

4. Independent Assurance Audit: The Cybersecurity Guidelines continue to require every organisation to conduct an Independent Assurance Audit ("**IA Audit**") annually. In this regard, the Cybersecurity Guidelines set out (i) the format of the Audit Report comprising of audit summary, overall findings, non-compliances, risk rating and audit checklist; (ii) the eligibility criteria of auditor(s)/audit firm to be engaged; and (iii) the format of audit certificate to be certified by the auditor(s)/audit firm. However, there have been certain changes in relation to the reporting thereof.

   a. Internally, the Audit Report is now required to be presented to the Audit Committee/Board of Directors/Principal Officer of the organisation, as applicable. Earlier, the requirement was for the report to be presented to the Risk Management Committee of the Board.

   b. Externally, as opposed to the previous requirement for an organisation (both Insurers and insurance intermediaries) to submit an executive summary of its Audit Report (along with an action taken report) to the IRDAI within 30 days of completing of the IA Audit, the Cybersecurity Guidelines now require (i) an Insurer to submit their Audit Report (including the comments by the Board) duly signed by the auditor(s)/audit firm to the IRDAI within 90 days from the end of the financial year or within 30 days of the completion of the Audit, whichever is earlier and (ii) an insurance intermediary to submit the Audit Report (including the comments by the Board) to the Insurer(s) annually. Further, in relation to insurance intermediaries that do not have access to the Insurer's information database/systems but only retain such information in a physical form, the Cybersecurity Guidelines require such insurance intermediaries to provide an annual "*self-certification*" to the Insurer(s) instead of the Audit Report.

   c. In relation to the controls now specified in the Audit Checklist, the Cybersecurity Guidelines classify such Regulated Entities (other than Insurers) on the basis of their access to the Insurer's database/system and gross insurance revenue, and accordingly make certain controls applicable based on whichever category the said entity falls under. As an illustration, Regulated Entities that connect to an Insurers' database/system through automated interfaces (such as API, EDI etc) and/or operate though an ISNP, are required to comply with all the controls specified in the Audit Checklist. However, Regulated Entities that have access to Insurer's internal system to only view certain data (but are not permitted to upload or edit such data), are only required to comply with controls pertaining to the protection of data and limiting the impact of cyber events.

5. Data Localisation: The Cybersecurity Guidelines appear to have removed the express requirement for the Insurers to host all their "*core business records*" on servers located in India. However, the Audit Checklist now requires all Regulated Entities (other than Insurers) to provide confirmation on whether the "*ICT infrastructure logs, critical and business data*" are stored in India. Notwithstanding the omission, the presence of the specific question in the Audit Checklist and various other provisions under the insurance statutory and regulatory framework[11] that continue to require Insurers to store specific forms of data/records in

[11] ¶14(a)(x) of the IRDAI's "*Guidelines on Insurance e-commerce*" of 9 March 2017, R3(9) of the IRDAI

India, indicate that the regulatory intent is to continue to require all Regulated Entities (including Insurers) to store their primary data in India.

***Concluding Remarks***

The Cybersecurity Guidelines represent a significant update from the 2017 Guidelines in strengthening the information and cyber security landscape within the insurance sector, surpassing the previous 2017 Guidelines by providing a more comprehensive approach and putting in place an adaptable framework.

Unlike the 2017 Guidelines, which were initially limited to Insurers and later extended to other Regulated entities, the new Cybersecurity Guidelines introduce specific norms for Regulated Entities based on their access to the Insurer's database/system and gross insurance revenue. This approach is expected to be a welcome development for smaller players in the industry as it allows them to adopt specific measures that are tailored to their specific needs and capabilities, without being burdened by extensive requirements.

While the Cybersecurity Guidelines are generally expected to enhance the sector's preparedness against both physical and cybersecurity risks, ongoing monitoring, regular assessments, and necessary updates will remain crucial to ensure the regulatory guidance continues to remain relevant in the times to come.

*The content of this article is intended to provide a general guide to the subject matter. Specialist advice should be sought about your specific circumstances.*

**For further information on this topic please contact Tuli & Co**

**Tel +91 120 693 4000, Fax +91 120 693 4001 or Email lawyers@tuli.co.in**

www.tuli.co.in

Author(s)

**Anuj Bahukhandi**

Managing Associate

**Priti Singh**

Associate

Article

(Maintenance of Insurance Records) Regulations 2015, and R24 of the IRDAI (Minimum Information Required for Investigation and Inspection) Regulations 2020.