Ref: IRDA/IT/CIR/MISC/301/12/2020 Dt: 29/12/2020

To

All insurers,

**Re: Amendments to the Guidelines on Information and Cyber Security for Insurers dated 07.04.2017**

IRDAI vide its Ref. No: IRDA/IT/GDL/MISC/ 082/04/2017 dated 07-4-2017 had issued Information and Cyber Security Guidelines containing comprehensive cyber security framework for Insurance sector for the purpose of implementing appropriate mechanism to mitigate cyber risks

Based on the review of the compliance process for cyber security by insurers and their subsequent feedback, the following sections of guidelines are amended as below.

**14. PLATFORM/INFRASTRUCTURE SECURITY.**

As per the action point 14.1 of the Guidelines, the Vulnerability Assessment and Penetration Testing (VAPT) on the entire ICT infrastructure should be conducted by the insurers on a periodic basis. Also, VA & PT has to be conducted on the software applications whenever there are changes in the configurations / applications.

In order to streamline the security assessment process, the following sub sections are added to Section 14.

**14.3 Procedure for conducting VA&PT**

(a) VA&PT of the entire ICT infrastructure components should be conducted annually in every financial year.

(b) Every VA&PT shall have two test cycles one at the beginning of VA&PT for identification of gaps and to check for known vulnerabilities, and a retesting post closure of vulnerabilities identified.

(c) VA&PT of critical applications should be conducted annually in every financial year. The remaining applications should be conducted once in a two-year cycle.

(d) VA&PT of all internet facing applications and Infrastructure components should be conducted at least once in a six months.

(e) An assessment of the need for security testing should be conducted whenever any change is made to any internet facing application or to any infrastructure component irrespective of the magnitude of change.

(f) Mandatory security testing should be conducted in case of all applications and related infrastructure components so as to check for known vulnerabilities once initially and again whenever major changes in internet facing applications and related infrastructure components take place. However, all Internet facing applications should be tested for all major and minor changes either through internal or external VA, and any gap found must be closed.

(g) The Cycle of the above security testings should be aligned with Annual assurance audit.

**14.4 Closure of VA&PT gaps**

(a) Closure of identified gaps in critical applications should be completed within one month. This includes confirmatory testing to ensure that the identified gaps have been successfully closed.

(b) Similarly, closure of identified gaps in other remaining applications should be completed within two months. Confirmatory testing should also be done to ensure closure of such identified gaps.

(c) For closure of identified gaps in all internet facing applications and Infrastructure components, External Black Box Penetration Testing should be done within one month, followed by confirmatory testing to ensure closure of such identified gaps.

(d) Closure of identified gaps in the entire ICT infrastructure components during internal vulnerability scan should be done immediately and without any loss of time.

(e) Insurers should classify the VA&PT gaps based on their risk assessment, Priority should be given to the high risk issues. In case any high risk issue is not resolved

within the prescribed timeline. The matter should be reported to the Risk Management Committee of the Board for deliberation and guidance.

## 23. INFORMATION SYSTEM AUDIT

### Section 23.3 Frequency of Conducting Assurance Audit is amended as follows

Assurance Audit shall be carried out annually for every financial year through a qualified external systems Auditor holding certifications like CISA/ DISA/Cert-in empanelled Auditors. Insurers shall indicate the specific quarter of the FY in which they would commence and complete their annual comprehensive assurance audit. Once the quarter is decided, the annual cyber security audit should be conducted during that quarter in every financial year.

**The following Sub-section is newly added to Section 23:**

### 23.7 Procedure for closure of audit gaps

(a) Closure of reported audit gaps should depend on the severity of the gaps and their impact on the overall service delivery, security, ensuring confidentiality of PII data, scope/coverage of implementation etc.

(b) Insurers should evaluate on the merits of issues based on the complexity of gaps and identify closure timelines as soon as possible, commit the same as a part of audit summary to be submitted to IRDAI.

(c) The major deficiencies/aberrations noticed during audit should be highlighted in a special note and given immediately to the Information Security Committee(ISC) and IT Department. Minor irregularities pointed out by the auditors are to be rectified immediately.

(d) Timelines for closure of audit gaps based on risk/impact of the reported gaps

including the controls implemented in the interim to reduce the level of risk exposure will be put-up to Risk Management Committee of the Board through Information Security Committee (ISC).

(e) The outer time limit for closure of audit gaps is two months. However, priority for closure of gaps should be decided based on risks associated with each gap.

(f) Insurer should submit the closure report to IRDAI on the identified audit gaps **within two months of completion of Annual Assurance Audit.**

(g) Insurer need not wait completion of assurance audit to close the audit gaps. As soon as any gap is noticed during the course of the audit, effort should be made to close the gaps.

**Member(Life)**