GOVERNMENT OF PAKISTAN
SECURITIES AND EXCHANGE COMMISSION OF PAKISTAN
-.-.-.-

NOTIFICATION

DIRECTIVE

Islamabad, 8th January, 2019

S.R.O. 31 (I)/2019.- Whereas with the increasing reliance on technology for business operations and expansion of financial technology, the probable impact of cyber risk in recent times can be greater than ever before. The cyber risk means "any risks that emanate from the use of electronic data and its transmission, including technology tools such as the internet and telecommunications networks. It also encompasses physical damage that can be caused by cybersecurity incidents, fraud committed by misuse of data, any liability arising from data storage, and the availability, integrity, and confidentiality of electronic information be it related to individuals, companies, or governments."

AND Whereas "Cyber risk presents an evolving challenge for the insurance sector and overall financial sector due to growing interconnectedness. Insurers gather, store, and maintain substantial volumes of confidential personal and organizational information. Because of these reservoirs of data, insurers are potential targets for cyber criminals who seek information that later can be used for financial gain through extortion, identity theft, or other illegal activities. In addition, because insurers are significant contributors to the national financial sector, interruptions of insurers' systems due to cybersecurity incidents may have far-reaching implication."

AND Whereas the increasing reliance of the insurance sector of Pakistan on the technology, in distribution and in offering other innovative products through usage of technology, makes it imperative that adequate measures must be taken to make its information technology systems, and of its intermediaries, secure and resilient.

Now therefore, in exercise of the powers conferred under Section 12 of the Insurance Ordinance, 2000 and Section 40B of the Securities and Exchange Commission of Pakistan read with clause (t), (u), (w) and clause (y) of sub-section (4) of section 20 thereof, the Securities and Exchange Commission of Pakistan hereby publishes the proposed directive for information of all persons likely to be affected and notice is hereby given that objections or suggestions, if any, received from any person within fourteen days of the publication of this notification in the official Gazette, shall be taken into consideration, prior to directing all the insurance companies and takaful operators regulated by the Commission to comply with following requirements, namely:-

1. Applicability

This Directive will apply to all life and non-life insurers including family and general takaful operators. In this Directive, the word "takaful" may be used interchangeably with the word 'insurance', 'family takaful' with 'life insurance', 'general takaful' with 'general insurance', 'contribution' with 'premium', and 'insurer' with 'takaful operator'. Similarly, other terms used in the Takaful Rules, 2012 associated with the takaful business may be used interchangeably with their conventional counterpart words/ terms. This Directive will become effective from March 1, 2019.

2. Definitions

In this directive unless there is anything repugnant in the subject or context-

i. "**Act**" means "the Securities and Exchange Commission of Pakistan Act, 1997 (XLII of 1997)";

ii. "**Commission**" means the Securities and Exchange Commission of Pakistan established under section 3 of the Securities and Exchange Commission of Pakistan Act, 1997 (XLII of 1997);

iii. "**Cyber**" Refers to the interconnected information infrastructure of interactions among persons, processes, data, and information and communications technologies, along with the environment and conditions that influence those interactions.

iv. **"Cybersecurity Incidence"** means An incidence (or event or problem) resulting in unauthorized access to, disruption or extortion of electronic data and its transmission in relation with an information technology system or the information stored on such information technology system;

v. **"Cyber Risk"** means any risks that emanate from the use of electronic data and its transmission, including technology tools such as the internet and telecommunications networks. It includes physical damage that can be caused by cybersecurity incidents, fraud committed by unauthorized use of data, any financial implications arising from data storage, availability, integrity, and confidentiality of electronic information related to individuals, public or private organizations and government authorities;

vi. **"Cybersecurity"** means strategies, policies, processes, practices and standards encompassing the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resilience, and recovery activities, and policies regarding the security of an insurer's operations;

vii. **"Insurer"** means an insurer registered under the Ordinance to carry on insurance business;

viii. **"Ordinance"** means the Insurance Ordinance, 2000 (XXXIX of 2000);

ix. **"Privacy Wrongful Act"** means any error, misstatement, act, neglect, breach of duty, or Personal Injury offense actually or allegedly committed or attempted by covered party, resulting in the failure by covered party, or by an independent contractor for which covered party is responsible, to handle, manage, store, destroy or otherwise control, personal data, third party corporate

information in any format and specifically identified as confidential and protected under a nondisclosure agreement or similar contract, or an unintentional violation of privacy policy that results in the violation of any Privacy Regulation including but not limited to the unintentional wrongful collection of Personal Data;

x. **"Network Security Wrongful Act"** means any error, misstatement, misleading statement, act, omission, neglect, breach of duty, or Personal Injury offense actually or allegedly committed or attempted by covered party, in capacity as such, resulting in a failure of Network Security, including the failure to deter, inhibit, defend against or detect any Computer Malicious Act, including malware, hacking, denial of service attacks; or unauthorized use or access;

xi. **"Cyber Extortion Event"** means any credible threat or connected series of threats made by a third party against insurer expressing intent to misuse, corrupt, damage information stored on computer, or impede, corrupt, or inhibit the system access for the purpose of demanding monies from covered party;

xii. **"Data Asset loss"** means loss arising out of data asset Incident which means entry to, corruption of or destruction of Data caused by computer malicious acts, malware, hacking, unauthorised Use or Access, denial of service attack, human Error, programming Error; or power failure, surge or diminution of an electrical system controlled by insurer affecting insurer Computer System;

xiii. **"Business Interruption Loss"** means reduction in net profit which occurs as a result of a business interruption incident, which means inability to access, disruption of, or disturbance to computer system or data caused solely and directly by computer malicious acts, malware, hacking, unauthorized use or access, denial of service attack, human error, programming error or power failure, surge or diminution of an electrical system controlled by insurer affecting insurer computer system;

3. Developing cybersecurity framework and mechanisms

i. Insures, as starting point shall consider existing core technical standards on cybersecurity such as the National Institute of Standards and Technology (**NIST**)[1] **Cybersecurity Framework**, and Information Systems Audit and Control Association (**ISACA**)'s COBIT ("Control Objectives for Information and Related Technologies"), and the International Organisation for Standardisation (**ISO**)[2] **27000 series**, which consist of a set of standards and best practices to manage cyber risks. In 2017, the FSB had also published a **Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices** to discuss cybersecurity in the financial sector[3].

[1] https://www.nist.gov/cyberframework
[2] https://www.iso.org/isoiec-27001-information-security.html
[3] http://www.fsb.org/wp-content/uploads/P131017-2.pdf

ii. Further, International Association of Insurance Supervisors (IAIS) has published draft **Application Paper on Supervision of Insurer Cybersecurity**. This paper focuses on supervision of insurers' cybersecurity.

4. Alignment of Cybersecurity Framework with overall Risk Management Framework

i. The insurer need to take into account the underlying cyber risk at the time of formulation of risk management policy by the Board of insurer, as part of significant policy as required under the clause (xi) of the Code of Corporate Governance for Insurers, 2016 (the *"Code"*). The Chief Information Security Officer (CISO) will be consulted for taking input with regards to cyber risk and required cybersecurity strategy and framework to be put in place for mitigation of inherent cyber risk.

ii. The insurer need to take into account the considerations of cyber risk, while evaluating that its risk management system, required to be established under clause (Ixx) of the Code of Corporate Governance for Insurers, 2016, is suitable, effective and proportionate for the business and that it is implemented and monitored.

iii. The Risk Management Function/ Department which is required to assess, quantify, monitor and control the nature, significance and interdependencies of the risks (at individual level as well as at aggregate level i.e. at enterprise level) under the clause (xx) of the Code , will also adequately take into account the cyber risk to which the insurer may be exposed and will also manage them accordingly. The risk management function/ department will adequately take into account the cyber risk, to which the insurer may be exposed, in performing all its functions as envisaged under clause (xxi) of the Code.

iv. Wherever the risk management requirements have been prescribed by the Code , the same will *ipso facto* apply in respect of inclusion in cyber risk management.

5. Appointment of Chief Information Security Officer (CISO)

i. The insurers will appoint a senior executive as Chief Information Security Officer (CISO) having adequate qualification and experience, who will be responsible for implementation of overall cybersecurity framework within the organization.

ii. The Chief Information Security Officer should have sufficient authority, independence, resources, and should report to the Board of insurer at least twice a year. He should be able to perform the roles as envisaged in other sections of this Directive.

iii. The Head of Information & Technology Department of Insurer cannot be appointed as Chief Information Security Officer (CISO).

iv. CISO will be responsible for continuous learning and improvements in Information Security measures and policies prepared in accordance with the requirements of this directive.

6. Insurers to conduct cybersecurity framework and risk assessment

i. Insurers shall implement at least annual assessment programs to help the Board and senior management to evaluate and take necessary measures for the adequacy and effectiveness of the insurer's cybersecurity framework including, where appropriate, through independent compliance program and audit carried out by qualified individuals to assess the cybersecurity framework and measure implementation.

ii. In addition to the annual assessment, insurer should perform cybersecurity risk assessments when:

   a. significant changes are proposed to the information system; or
   b. significant changes occur to the information system; or
   c. from the time that a need for a new information system is identified till the time it is disposed of, including at planned intervals.

7. Regulatory Reporting

i. The insurers are required to submit to the Commission the cybersecurity framework assessment reports, formulated in compliance of the clause 6 (i) above, by April 30 of every year.

ii. The cybersecurity framework assessment reports are required to be signed by the Chief Information Security Officer (CISO) and the Chief Operations Officer (COO)/ Chief Executive Officer (CEO) of the Company and where such assessment has been conducted by the independent auditor, the report is required to be signed by that auditor in addition to the aforementioned officers of the insurer.

iii. The insurer shall make available to the Commission, when required through a direction in writing, the reports or findings made after conducting the cybersecurity risk assessment in compliance with the clause 6(ii) above.

8. Data Security and Confidentiality

i. The insurer's cybersecurity framework shall be able to protect the policyholder data in the wake of enhanced reliance on business process outsourcing (BPO), technology based agency arrangements and other strategic partnerships for offering technology based innovative insurance products and services.

ii. The primary onus for safety and confidentiality of policyholder data lies on the insurer irrespective of its business arrangements with its agents, vendors, strategic partners, or any other parties. The insurers will adopt and act upon the applicable provisions of the "Prevention of Electronic Crimes Act, 2016" in all its business, agency, or service level agreements with the aforementioned parties while emphasizing on the fair usage of information to which they might get access by virtue of that agreement.

iii. The insurers will make utmost efforts to ensure safety and confidentiality of data of policyholder. In instances where policyholder data is inevitably shared with or collected by external parties, the privacy and fair usage of data clause will necessarily form part of the business agreement between the insurer and the counterparty. The clause will include, among other statements, that the policyholder or beneficiary data will only be used for the purpose of provision of insurance services to the policyholders and the data will not be shared with any other party except in instances where the applicable regulatory requirements so require.

iv. The insurers and all persons associated with the business of insurance in any manner, will collect only that information which is necessary to provide insurance services to the policyholder or potential policyholder through the technology based platforms and not any additional information without the express consent of the policyholder or potential policyholder. Express consent would mean the affirmation to collection of data while having complete knowledge about contents of data which will be collected, the frequency of collection of such contents, the purpose for which that data will be used and whether or not that data will be passed on to any other party any further.

9. Insurers to obtain cyber risk insurance

i. All life and non-life insurers including the family and general takaful operators (hereinafter to be referred as *"insurers"*) should consider obtaining the cyber risk insurance to cover their own cyber risks, to which they are exposed. The purpose of cyber risk insurance is to mitigate losses or damages from a variety of cyber incidents, including data breaches, business interruption, and network damage.

ii. The cyber risk insurance shall preferably, protect the insurers against the claims arising out of at least privacy wrongful act and network security wrongful act.

iii. The claims arising out of privacy wrongful act and network security wrongful act would include the following;

(a) written demand against the insurer for monetary and non-monetary damages for committing a Privacy Wrongful Act or network security wrongful act;
(b) a civil proceeding against the insurer seeking monetary damages or non-monetary or injunctive relief, commenced by the service of a complaint or similar pleading for committing a Privacy Wrongful Act or network security wrongful act; and
(c) an arbitration proceeding against the insurer seeking monetary damages or non-monetary or injunctive relief committing a Privacy Wrongful Act or network security wrongful act;

vi. The cyber risk insurance shall also ideally cover the insurer against the following risks:

(a) Cyber extortion;
(b) Data asset loss; and
(c) Business interruption.

v. Cyber insurance coverage options vary greatly and may be offered on a stand-alone basis or as additional coverage endorsed to existing insurance policies, such as general liability, business interruption, errors and omissions, or directors' and officers' policies. Further, cyber insurance coverage options may be structured as first-party or third-party coverage. First-party coverage insures against direct expenses incurred by the insured party and may address costs related to customer notification, event management, business interruption, and cyber extortion. Third-party coverage protects against the claims made by financial institutions' customers, partners, or vendors as a result of cyber incidents at financial institutions. Understanding the scope of coverage is critical for making an informed risk management decision.

vi. Purchasing cyber insurance i.e. transferring risk does not remove the need for a sound control environment. Rather, cyber insurance may be a component of a broader risk management strategy that includes identifying, measuring, mitigating, and monitoring cyber risk exposure. An effective system of controls remains the primary defense against cyber threats.

vii. The insurer while considering the benefits and costs of cyber insurance to purchase may take following into consideration:

a. Involving multiple stakeholders in the cyber insurance decision

i. Include appropriate departments across the institution such as legal, enterprise risk management (i.e. operational risk management, financial risk management, I&T risk management, information & cybersecurity risk management etc.).

ii. Assess the sufficiency of existing control environments to address the potential impact of cyber risk exposures and attestation requirements for the insurance policy.

iii. Communicate the cyber insurance decision-making process, including the assessment of cyber insurance options, to the appropriate level of management.

b. Performing proper due diligence to understand available cyber insurance coverage

i. Review the scope of existing or proposed insurance coverage to identify gaps.

ii. Understand insurance policy terms, coverage, exclusions, and costs for cyber events.

iii. Consider the potential benefits and costs to assess the insurance coverage appropriateness.

iv. Avoid overreliance on insurance coverage as a substitute for sound operational risk management practices.

v. Recognize that policy terms and language may not be standardized. Coverage may be different among insurance providers and tailored for institutions.

vi. Consider how the coverage is triggered, if certain types of cyber incidents (e.g., cyber terrorism) are excluded from coverage, and the impact that sub-limits may have in the total coverage and claims process.

vii. Assess the financial strength (ratings) and claims paying history of insurance companies providing coverage and their ability to fulfill obligations under the policy if multiple institutions file claims.

10. Insurers to have adequate cybersecurity systems in place

i. **Network and system security**. – The insurers are required to have adequate network security and system security in place to safeguard their operating systems, software and databases against the cyber risks.

ii. **Configuration of data and encryption**. – The insurers will put in place secure configuration of hardware, operating systems, software, applications, databases and servers with all unnecessary services and programs disabled or removed. The insurers will ensure encryption at database level, storage level and during network transmission as per the classification and sensitivity of the data.

11. The Cybersecurity Framework for Insurance Sector

The insurer shall formulate a sound cybersecurity framework in order to anticipate, withstand, detect, prevent and respond to cyber-attacks in line with international standards and best practices. The insurer shall establish the cybersecurity framework while taking into account the nature, size and complexity of cyber risks to which it is exposed, within six months of coming into effect of this directive. Few principles in respect of formulation of cybersecurity framework are given in this section.

(A) Cybersecurity Strategy and Framework

The insurers shall establish and maintain a cybersecurity strategy and framework tailored to specific cyber risks and appropriately informed by international, national, and industry standards and guidelines. The insurers shall consider the following while establishing the strategy and framework for cybersecurity.

(i) **Articulate principles. –** Cybersecurity strategies shall clearly articulate principles regarding how the insurer intends to address cyber risks. The insurer's cybersecurity strategy should be closely aligned with, and complementary to, its cybersecurity framework, to ensure that the framework is capable of achieving its objectives.

(ii) **Framework Objectives.** – The insurer's cybersecurity framework should support and promote both its operational security and the protection of policyholder data. Therefore, framework objectives should aim to maintain and promote the insurer's ability to anticipate, detect, withstand, contain and recover from cybersecurity incidents, so as to limit the likelihood or impact of a cybersecurity incident, which could damage the insurer's operations, its reputation, and the data privacy of its policyholders and third parties

(iii) **Cyber Security Infrastructure**. – The insurer's framework should clearly define its cybersecurity objectives and horizon as well as the requirements for people, processes, and technology necessary for managing cyber risks and timely communication in order to enable

an insurer to collaborate with relevant stakeholders to effectively respond to and recover from cybersecurity incidents.

(iv) **Defined roles and responsibilities**. – To maximize its effectiveness, the framework must be supported by clearly defined roles and responsibilities of the insurer's Board and its management, and it is incumbent upon the Board and management to create a culture which recognizes that staff at all levels have important responsibilities in ensuring the insurer's cybersecurity.

(v) **Alignment with enterprise risk management**. – The insurer shall align its cybersecurity framework with its enterprise risk management (ERM) integrated framework. Such consistency is important, and recognizes that an insurer's cybersecurity framework is likely to overlap with the policies, procedures, and controls that it has established to manage other areas of risks. For example, cyber risk should also be a consideration in an insurer's physical security framework (e.g., to limit access to critical ICT infrastructure) and its human resource policies (e.g., to manage "insider" threats).

(vi) **Plan to identify cyber risk**. – Cybersecurity framework documentation should clearly articulate how the insurer plans to effectively identify the cyber risks that it faces, determine its cybersecurity objectives and risk tolerance, and mitigate and manage its cyber risks. This adopted framework shall be capable for identifying the cybersecurity-risk-owners; and risks associated with the loss of confidentiality, integrity and availability of information within the scope of the cybersecurity strategy objectives. All risks identified should 'owned' by a single named individual with the understanding that it may take shared responsibility to mitigate the risks successfully

(vii) **Regular review and Monitoring**. – An insurer's cybersecurity framework shall consider how the insurer would regularly review and actively mitigate the cyber risks that it bears from and poses to its stakeholders such as policyholders, other insurers, third party service providers (including the services and products provided by those third party service providers), and other third parties (the insurer's cybersecurity ecosystem).

(viii) **Updation**. – Maintaining an effective approach to cyber risk management is particularly challenging. Because cyber risks may rapidly evolve, an insurer's cybersecurity strategy and framework should be reviewed and updated with sufficient frequency to ensure that they remain effective.

(B) Governance

The insurers need to define and facilitate performance of roles and responsibilities for officers implementing, managing, and overseeing effectiveness of cybersecurity strategy and framework to ensure accountability and to provide adequate resources, appropriate authority, and access to the governing authority e.g. board of directors.

(i) **Responsibility of Board of Directors. –** The insurer's Board is ultimately responsible for setting strategy and ensuring that cyber risk is effectively put in place and managed. The Board shall endorse the insurer's cybersecurity framework and set the insurer's cybersecurity Risk Acceptance Criteria (RAC) i.e. risk appetizer.

(ii) **Regular Reporting to Board of Directors.** – The Board shall be regularly apprised of the insurer's cyber risk profile to ensure that it remains consistent with the insurer's risk tolerance i.e. Acceptance Criteria (RAC) as well as the insurer's overall business objectives. As part of this responsibility, the Board shall consider whether changes to the insurer's products, services, policies or practices, and the threat landscape materially affect its cyber risk profile. In case, the insurer have to accept risks that do not meet normal Acceptance Criteria (RAC), it shall explicitly comment on the risks and include justification for the decision to override normal risk acceptance criteria.

(iii) **Senior management**. – Senior management shall closely oversee the insurer's implementation of its cybersecurity framework, and the policies procedures, and controls that support the framework.

(iv) **Awareness and commitment**. – An insurer's Board and senior management shall cultivate awareness of and commitment to cybersecurity. The Board and senior management shall include members with skills appropriate to their oversight and management roles with respect to the risks posed by cyber threats. In addition, the Board and senior management shall promote a culture that recognizes that staff at all levels have important responsibilities in ensuring the insurer's cybersecurity and lead by example.

(v) **Oversight of third party service providers**. – Insurers shall have in place information security policies, procedures and processes including definitions of roles and responsibilities across the organization. These policies, procedures and processes shall include oversight of third party service providers, as well as cyber risk management processes and determination of priorities, constraints, assumptions, and risk tolerance level.

(C) Risk and Control assessment

The insurers shall identify functions, activities, products, and services—including interconnections, dependencies, and third parties—prioritize their relative importance, and assess their respective cyber risks," and to "identify and implement controls—including systems, policies, procedures, and training—to protect against and manage those risks within the tolerance i.e. Acceptance Criteria (RAC) set by the Board of Directors.

(i) **Identification and classification of functions. –** Insurers shall identify and classify functions including information assets and data sensitivity, as well as their interconnectedness; proactive technology and processes; external dependency management; and situational awareness.

(ii) **Prioritization of protection, detection, response and recovery efforts of insurer. –** The insurer shall adequately account for cyber risks in its overall enterprise risk management (ERM) integrated system, identifying its business functions and supporting processes and conducting a risk assessment to ensure that it thoroughly understands the importance of each function and supporting processes, and their interdependencies, in performing its functions. Identified business functions and processes shall then be classified by insurers in terms of criticality, which in turn should guide the insurer's prioritization of its protection, detection, response, and recovery efforts.

(iii) **Inventory or mapping. –** To the extent practicable, the insurer shall identify and maintain a current inventory or mapping of its information assets and system configurations, including interconnections with other internal and external systems, in order to know at all times the assets that support its business functions and processes. Overall, there may be three broad categories of information that shall be evaluated: Information that is confidential or non-public relating to the insurer's functions; Information relating to the insurer's internal operations; and Information that is public or non-confidential that is stored, accessed or distributed through or by the insurer. The insurer shall carry out a risk assessment of those assets and classify them in terms of critical importance. Risks identified by a risk assessment, shall be managed i.e. risk reduction, risk acceptance, risk avoidance or risk transfer.

(iv) **Identify dependencies**. – As part of this mapping process, the insurer shall also identify dependencies in its information assets and system configurations, for example, from third party service providers. The inventory should encompass hardware, software platforms and applications, devices, systems, data, personnel, external information systems, critical processes, and documentation on expected data flows.

(v) **Individual and system access rights (Access Controls)**. – Insurers shall identify and maintain a current record of both individual and system access rights to know who has access to information assets and their supporting systems, and to use this information both to ensure that access rights are no broader than necessary, and to facilitate identification and investigation of anomalous activities.

(vi) **Integrate identification efforts**. – Insurers shall integrate identification efforts with other relevant processes, such as acquisition and change management, in order to facilitate a regular review of its list of critical business processes, functions, individual and system credentials, as well as its inventory of information assets to ensure that they remain current, accurate and complete.

(vii) **Business impact analysis**. – Similarly, insurers shall conduct business impact analysis for cyber risks (i.e., a determination of risks and prioritization of risk responses through identification of threats, vulnerabilities, likelihoods, and impacts).

Inclusion of Cyber Risk in Risk Profile

(viii) Insurers' risk profiles shall identify key operational areas exposed to cyber risk, arising from both internal and external sources.

(ix) Using the same precepts as in the development of an enterprise-wide risk profile, the insurer would aim to describe the overall cyber risk to which the enterprise is exposed. The risk profile may benefit from inclusion of assessment processes that encompass assessments of likelihood and impact of harm. At a more detailed level, the risk profile may also include and be informed by the result of insurers' vulnerability scanning and management process. A typical vulnerability management system includes enumeration of platforms, software flaws, and improper configurations as well as an assessment of the vulnerability impact.

(x) Insights from both processes may be organised, for example, within the following categories: (1) technologies and connection types; (2) delivery channels; (3) organizational characteristics; and (4) external threats.

1. ***Technologies and Connection Types***. Certain technologies and connection types may pose a higher cyber risk depending on the complexity and maturity, connections, and nature of the specific technology products or services of the insurer. For example, it may be appropriate for an insurer to assess the number of Internet service provider (ISP) and third-party connections, whether systems are hosted internally or outsourced, the presence and number of unsecured connections, the use of wireless access, volume of network devices, end-of-life systems, extent of cloud services, and use of personal devices by insurer personnel.

2. ***Delivery Channels.*** Insurers shall be aware that some delivery channels for products and services may pose a heightened cyber risk depending on the nature of the specific product or service offered. Cyber risk increases as the variety and number of delivery channels increases. For example, online and mobile delivery channels may present increased levels of risk to an insurer.

3. ***Organizational Characteristics.*** Those Characteristics to consider include past and planned mergers, demergers, acquisitions, and sales, the number of direct employees and cybersecurity contractors, changes in security staffing, the number of users with privileged access, changes in information & technology (I&T) environment, locations of business presence, locations of operations and data centers (including legacy systems), and reliance on third party service providers, including cloud service providers.

4. ***External Threats****.* External threats, particularly the volume and type of attacks (attempted or successful) reflect and affect an insurer's cyber risk exposure. An insurer should consider the volume and sophistication of the attacks targeting it and other similarly situated organizations.

Implementation of Proactive Technology and Processes

(xi) Insurers shall protect data both when at-rest, in-transit and in-storage commensurate with the criticality of the information held and associated classification, extending to backup systems and offline data stores as well.

Management of External Dependencies

(xii) Insurers shall actively manage cyber risks presented by third parties. For example, many insurers' systems and processes are directly or indirectly interconnected with numerous third parties, including cloud service providers and providers of outsourced functions. The cybersecurity of those entities may significantly affect the cyber risk that an insurer faces.

(xiii) **Verification of third party service providers. –** Insurers shall verify that third-party service providers have implemented appropriate administrative, technical, and physical measures to protect and secure the data of an insurer and its customers to the same degree expected of the insurer.

(xiv) Insurers shall be aware that the significance of the risks the third parties may pose to the insurer is not necessarily proportionate to the criticality of their business relationship with the insurer. Therefore, an insurer shall identify the cyber risks that it bears from and poses to third parties and, to the extent practicable, coordinate with its relevant stakeholders, as these third parties design and implement their own resilience efforts with the objective of improving the overall resilience of the insurer and its stakeholders.

Enhancing Situational Awareness

(xv) **Proactive identification. –** An insurer shall have appropriate situational awareness of the cyber risks that it faces. An insurer shall seek to proactively identify cyber threats that could materially affect its ability to perform or to provide services as expected, or that could have a significant impact on its ability to meet its own obligations, including protection of confidential data. The insurer should regularly review and update this analysis.

(xvi) **Extreme but Plausible trigger.** – Cyber threats to be considered shall include those which could trigger extreme but plausible cyber events, even if they are considered unlikely to occur or have never occurred in the past. Insurers shall consider threats to the confidentiality, integrity, and availability of the insurer's business processes, policyholder data, and to its reputation. Threats arising from both internal and external sources, such as employees or third-party service providers, respectively, should be considered.

(D) Monitoring

The insurers shall establish systematic monitoring processes to rapidly detect cyber incidents and periodically evaluate the effectiveness of identified controls, including through network monitoring, testing, audits, and exercises. Effective monitoring helps entities adhere to established risk tolerances

and timely enhance or remediate weaknesses in existing controls," and testing and auditing protocols provide essential assurance mechanisms.

Continuous Monitoring

(i) **Protect network**. – Insurers shall protect network (hardware, firmware and software components) integrity including control of information flow, boundary protection, and network segregation if needed.

(ii) **Security Operations Centre**. – For example, an insurer shall establish real-time, or near real-time continuous monitoring capabilities to detect anomalous activities and events. One practice currently in use to accomplish this is commonly referred to as a Security Operations Centre (SOC). Insurers should consider establishing a SOC or developing similar capability to provide round the clock monitoring and such capabilities should be adaptively maintained and tested.

(iii) **Early Detection. –** The insurers shall be able to recognize signs of a potential cyber incident, or detect that an actual breach has taken place, which is essential to strong cybersecurity. Early detection provides an insurer with useful lead time to mount appropriate countermeasures against a potential breach, and allows proactive containment of actual breaches. In the latter case, early containment could effectively mitigate the impact of the attack – for example, by preventing an intruder from gaining access to confidential data or exfiltration of such data.

(iv) **Monitor for Anomalous activities**. – In view of the stealthy and sophisticated nature of cybersecurity incidents and the multiple entry points through which a compromise could take place, an insurer should maintain effective capabilities to extensively monitor for anomalous activities. An insurer shall implement, within relevant legal boundaries, measures to capture and analyse anomalous behavior by persons with access to the corporate network.

(v) **Behaviorally based detection mechanisms**. – The insurers shall monitor relevant internal and external activities and events, seeking to detect vulnerabilities through a combination of signature monitoring for known vulnerabilities and behaviorally-based detection mechanisms.

(vi) **Misuse of access**. – Insurers' detection capabilities shall also address misuse of access by third party service providers, policyholders, potential insider threats, and other advanced threat activity. These processes should be informed by and integrated with a strong cyber threat intelligence programme.

(vii) **Identities and Credentials**. – As part of the monitoring process, insurers shall manage the identities and credentials for physical, logical, and remote access to information assets, based on principles of least privilege and separation of duties.

(viii) **Multi-layered detection controls. –** The insurers shall have the ability to detect an intrusion early, as this capability is critical for swift containment and recovery. Insurers should take a defence-in-depth approach by instituting multi-layered detection controls covering people, processes, and technology, with each layer serving as a safety net for preceding layers.

(ix) **Effective intrusion detection capability**. – In addition, an effective intrusion detection capability could assist insurers in identifying deficiencies in their protective measures for early remediation. These capabilities would include data loss/leaks prevention and detection, the recording and documentation of audit logs, event data aggregation, correlation, analysis and communication, as well as network, personnel and external dependency activity monitoring.

(x) **Incident Response and Forensic Investigation**. – The insurer shall employ monitoring and detection capabilities to facilitate its incident response process and support information collection for the forensic investigation process.

Testing

(xi) Testing is an integral component of any effective cybersecurity framework. Sound testing regimes produce findings that are used to identify gaps in stated resilience objectives and provide credible and meaningful inputs to the insurer's cyber risk management process. Analysis of testing results provides direction on how to correct weaknesses or deficiencies in the cybersecurity posture and reduce or eliminate identified gaps. Such testing could include vulnerability assessments, scenario-based testing, penetration tests, and tests using red teams.

(xii) Insurers shall rigorously tests all elements of their cybersecurity framework to determine their overall effectiveness before being employed within an insurer, and regularly thereafter. Such testing should encompass the extent to which the framework is implemented correctly, operating as intended, and producing desired outcomes.

(xiii) Insurers shall tests their cybersecurity framework and communicate the results within their organisation. For example, insurers should establish an appropriately comprehensive testing programme to validate the effectiveness of all elements of their cybersecurity framework, employing appropriate available cyber threat intelligence to inform its testing methods – such as by designing tests to simulate advanced threat agent capabilities and extreme but plausible scenarios.

(xiv) The results of the testing programme shall be used by the insurer to support the ongoing improvement of its cybersecurity. Where applicable and practicable, these tests should include other stakeholders and functions within the organization, such as business line management including business continuity, incident and crisis response teams, and relevant external stakeholders. An insurer should have proper procedures in place to ensure that its Board and Senior Management are appropriately involved (e.g., as part of crisis management teams) and informed of test results.

(xv) The insurers shall consider using a combination of the available state-of-the-art testing methodologies and practices. Currently, such state-of-the-art testing methodologies and practices, include the following elements (which partly overlap and can be combined):

(xvi) **Vulnerability Assessment .** – Insurers shall regularly perform vulnerability assessments to identify and assess security vulnerabilities in their systems and processes. Insurers should establish a process to prioritize and remedy issues identified in VAs and perform subsequent validation to assess whether gaps have been fully addressed in a timely manner.

(xvii) **Scenario-Based Testing**. – An insurer's response, resumption, and recovery plans shall be subject to periodic review and testing. Tests shall address an appropriately broad scope of scenarios, including simulation of extreme but plausible cybersecurity incidents, and should be designed to challenge the assumptions of response, resumption, and recovery practices, including governance arrangements and communication plans. Insurers should use cyber threat intelligence and cyber threat modelling to the extent possible to imitate the unique characteristics of cyber threats. They shall also conduct exercises to test the ability of their staff and processes to respond to unfamiliar scenarios, with a view to achieving stronger operational resilience.

(xviii) **Penetration Tests**. – Insurers shall carry out penetration tests to identify vulnerabilities that may affect their systems, networks, people or processes. To provide an in-depth evaluation of the security of insurers' systems, those tests shall simulate actual attacks on the systems. Penetration tests on internet-facing systems should be conducted regularly and before updated systems are deployed. Where applicable and practicable, the tests could include wider business stakeholders, such as those involved in business continuity, incident and crisis response teams, as well as third parties, such as service providers.

(xix) **Red Team Tests**. – Insurers shall consider challenging their own organizations and external dependencies through the use of so-called red teams to introduce an adversary perspective in a controlled setting. Red teams serve to test for possible vulnerabilities and the effectiveness of an insurer's mitigating controls. A red team may consist of insurer's own employees and/or outside experts, who are in either case independent of the function being tested.

(xx) **Response Testing**. – An insurer shall, to the extent practicable/possible, promote, design, organize, and manage exercises designed to test its response, resumption, and recovery plans and processes. Such exercises should include the insurer as well as critical service providers, and linked insurers (such as affiliates within an insurance group). Where appropriate, insurers should participate in exercises organized by relevant authorities and in industrywide tests.

(xxi) **Integrated or Dynamic Testing**. – Insurers shall take note that traditional isolated testing implicitly assumes that all other players operate as usual, which may be an unrealistic limitation. Removing that hypothesis helps an insurer to identify plausible complexities,

dependencies and weaknesses that may have been overlooked in its recovery plans. Accordingly, testing should include scenarios that cover breaches affecting external dependencies.

(E) Response

The insurers shall, in a timely manner,

(a) assess the nature, scope, and impact of a cyber incident;
(b) contain the incident and mitigate its impact;
(c) notify internal and external stakeholders (such as law enforcement, regulators, and any other authorities, as well as shareholders, third-party service providers, and customers as appropriate); and
(d) coordinate joint response activities as needed."

The insurers shall be able to implement incident response policies and other controls to facilitate effective incident response," and among other things, these controls should clearly address decision-making responsibilities, define escalation procedures, and establish processes for communicating with internal and external stakeholders."

(i) **Awareness and Training.** – In advance of a cybersecurity incident, insurers shall raise awareness among all its stakeholders by providing training for employees and others with access to its systems. Insurers shall also develop response plans (Incident Response and Business Continuity) and communication plans regarding cyber incidents. These plans shall be subject to review and improvement as appropriate.

(ii) **Investigation**. – Upon detection of a cybersecurity incident (or an attempt), it is good practice for an insurer to perform a thorough investigation to determine its nature and extent as well as the damage inflicted. While the investigation is ongoing, the insurer shall also take immediate actions to contain the situation to prevent further damage, and commence recovery efforts to restore operations based on its response planning.

(iii) **Systems back up**. – Insurers shall also be cognizant not to bring systems back up too quickly and risk another attack or expansion of the cybersecurity incident.

(iv) **Plan to resume critical operations**. – While an insurer shall plan to resume critical operations as soon as is safely possible after a cybersecurity incident, it should analyse critical functions, transactions, and interdependencies to prioritize resumption and recovery actions while remediation efforts continue. Insurers should also plan for situations where critical people, processes, or systems may be unavailable for significant periods – for example, by potentially reverting, where feasible and practicable, to manual processing if automated systems are unavailable.

(v) **Access to external experts**. – Insurers shall plan to have access to external experts, recognizing that a large-scale or industry wide event may reduce the availability of such key resources on short notice.

(vi) **Develop and test response, resumption, and recovery plans**. – Insurers shall develop and test response, resumption, and recovery plans. These plans should support objectives to protect the confidentiality, integrity, and availability of its assets, including policyholder data. Plans should be actively updated based on current cyber threat intelligence, information-sharing, and lessons learned from previous events, as well as analysis of operationally and technically plausible scenarios that have not yet occurred. An insurer should consult and coordinate with relevant internal and external stakeholders during the establishment of its response, resumption, and recovery plans, including supervisors and other relevant authorities.

(vii) **System and process to support incident response. –** System and process design and controls for critical functions and operations shall support incident response activities to the extent possible. Insurers should design systems and processes to limit the impact of any cyber incident and protect the privacy of policyholder data. An insurer's incident response, resumption, and recovery processes shall be closely integrated with crisis management, business continuity, and disaster recovery planning and recovery operations, and coordinated with relevant internal and external stakeholders.

(viii) **Specific Team**. – Insurers should have a specific team in place for all stakeholder communications – inclusive of policyholders, business partners, and appropriate authorities, to ensure adequate preparation and consistency of message.

(ix) **Responsible disclosure of potential vulnerabilities**. – As part of its overall governance framework and in compliance with relevant laws, insurers shall have a policy and procedure to enable the responsible disclosure of potential vulnerabilities following a risk-based approach. In particular, insurers should prioritize disclosures that could facilitate early response and risk mitigation by stakeholders for the benefit of the cyber ecosystem and broader financial stability.

(x) **Policy and procedure to meet the disclosure obligations**. – In the event of an exposure of policyholder data, an insurer shall have a policy and procedure to meet the disclosure obligations set forth in the laws and regulations of all relevant jurisdictions.

(xi) **Forensic investigations**. – Insurers shall have the capability to assist in or conduct forensic investigations of cyber incidents and engineer protective and detective controls to facilitate the investigative process. In this regard, insurers should establish relevant system logging policies that include the types of logs to be maintained and their retention periods. While forensic analysis may need to be postponed and I&T resources may be focused on recovering critical systems, insurers should ensure that investigations can still be performed post-event to the extent possible, e.g., through preservation of necessary system logs and evidence.

(F) Recovery

The insurers shall be able to resume operations responsibly, while allowing for continued remediation, including by

(a) eliminating harmful remnants of the incident;
(b) restoring systems and data to normal and confirming normal state;
(c) identifying and mitigating all vulnerabilities that were exploited;
(d) remediating vulnerabilities to prevent similar incidents; and
(e) communicating appropriately internally and externally."

They shall consider the following while adopting recovery practices.

(i) **Validated plans and procedures**. – Insurers shall have in place validated plans and procedures to recover from a cybersecurity incident. Cyber incident recovery arrangements should be designed to enable insurers to resume operations safely with a minimum of disruptions to policyholders and business operations.

(ii) **Timely recovery**. – Insurers shall design and test their systems and processes to enable timely recovery of accurate data following a breach. As an example, insurers' systems and processes could be designed to maintain an uncorrupted "golden copy" of critical data (including, to the extent possible, application source code), to be used in the restoration of impacted systems and data. Data instances should be safeguarded by stringent protective and detective controls. In addition, the insurer's cybersecurity framework should include data recovery measures, such as keeping a backup copy of all policyholder data in the event such data is corrupted.

(iii) **Review and improvement**. – Insurers' recovery plans (Incident Recovery and Disaster Recovery) shall be subject to review and improvement as appropriate.

(iv) **Contagion risk**. – Because an insurer's systems and processes are often interconnected with the systems and processes of third parties, in the event of a large-scale cyber incident it is possible for an insurer to pose contagion risk (i.e., propagation of malware or corrupted data) to, or be exposed to contagion risk from, its third party service providers or other interconnected systems. An insurer should work with these third parties to resume operations in a safe manner.

(v) **Formal plans for communicating with all stakeholders. –** Insurers shall have formal plans for communicating with policyholders, internal and external stakeholders (such as law enforcement, regulators, and other public authorities, as well as shareholders and third-party service providers as appropriate) likely to sustain harm due to a major cybersecurity incident. Communication plans in accordance with governing law should be developed through an adaptive process informed by scenario-based planning and analysis as well as prior experience. Because rapid escalation of cybersecurity incidents may be necessary, insurers should determine decision-making responsibilities for incident response and recovery in advance, and implement clearly defined escalation and decision-making procedures.

(G) Information Sharing

The insurer shall engage in the timely sharing of reliable, actionable cybersecurity information with internal and external stakeholders (including entities and public authorities within and outside the financial sector) on threats, vulnerabilities, incidents, and responses to enhance defenses, limit damage, increase situational awareness, and broaden learning.

Sharing technical information, such as threat indicators or details on how vulnerabilities were exploited, allows entities to remain up-to-date in their defences and learn about emerging methods used by attackers. Sharing broader insights among entities, between entities and public authorities, and among public authorities deepens collective understanding of how attackers may exploit sector-wide vulnerabilities that could potentially disrupt critical economic functions and endanger financial stability.

The insurers may consider the following in respect of information sharing regarding cybersecurity.

(i) **Information sharing**. – Insurers shall establish a process to gather and analyse relevant cyber threat information. Insurers should consider participating actively in information-sharing groups and collectives, within the country to gather, distribute and assess information about cyber practices, cyber threats, and early warning indicators relating to cyber threats. Insurers may participate in system-wide initiatives such as Incident Response Teams (IRT), if established through the joint efforts of insurers, or other financial institutions.

(ii) **Business-specific context**. – An insurer's analysis of cyber threat information shall be in conjunction with other sources of internal and external business and system information so as to provide business-specific context, turning the information into usable cyber threat intelligence that provides timely insights and informs enhanced decision-making by enabling the insurer to anticipate a cyber attacker's capabilities, intentions, and *modus operandi*.

(iii) **Ability to understand threats posed by external service provider.** – If practicable, an insurer's cyber threat intelligence operations shall include the capability to gather and interpret information about relevant cyber threats posed by the insurer's third-party service providers, as well as utility providers and other critical infrastructure resources. Additionally, cyber threat intelligence operations should interpret this information in ways that allow the insurer to identify, assess, and manage security threats and vulnerabilities for the purpose of implementing appropriate safeguards in its systems. In this context, relevant cyber threat intelligence could include information on geopolitical developments that may trigger cyber attacks on the insurer or any of its external dependencies.

(iv) **Mitigation of cyber risks at the strategic, tactical, and operational levels. –** When properly contextualized, cyber threat information enables an insurer to validate and inform the prioritization of resources, risk mitigation strategies, and training programmes. Therefore, an insurer should make cyber threat intelligence available to appropriate staff within the insurer with

the responsibility for the mitigation of cyber risks at the strategic, tactical, and operational levels. Cyber threat intelligence should be used to ensure that the implementation of any cybersecurity measures is threat-informed.

(v) **Sector-wide response**. – To facilitate sector-wide response to large-scale cybersecurity incidents, insurers shall plan for information-sharing through trusted channels, collecting and exchanging timely information that could facilitate the detection, response, resumption, and recovery of its own systems and those of other sector participants during and following a cybersecurity incident. Insurers should, as part of their response programmes, determine beforehand which types of information will be shared with whom and how information provided to the insurer will be acted upon. Reporting requirements and capabilities should be aligned with relevant laws and regulations as well as information-sharing arrangements within insurer communities and the financial sector.

(vi) **Exchanging information**. – An insurer shall consider exchanging information on its cybersecurity framework bilaterally with its third-party service providers to promote mutual understanding of each other's approach to securing systems that are linked or interfaced. Such information exchange would facilitate an insurer's and its stakeholders' efforts at dovetailing their respective security measures to achieve greater cybersecurity.

(H) Continuous Learning

The insurers shall review the cybersecurity strategy and framework regularly and when events warrant—including its governance, risk and control assessment, monitoring, response, recovery, and information sharing components—to address changes in cyber risks, allocate resources, identify and remediate gaps, and incorporate lessons learned.

The cyber threats and vulnerabilities evolve rapidly, as do best practices and technical standards to address them. Therefore, "entity-specific, as well as sector-wide, cybersecurity strategies and frameworks need regular review and update to adapt to changes in the threat and control environment, enhance user awareness, and to effectively deploy resources."

The following should be helpful for insurers keen to adopt continuous learning practices.

(i) **Continuous cybersecurity**. – Insurers shall adopt a cybersecurity framework premised on ensuring continuous cybersecurity amid a changing threat environment.

(ii) **Proactive protection**. – Insurers shall implement cyber risk management practices that go beyond reactive controls and include proactive protection against future cyber events.

(iii) **Predictive capabilities**. – Predictive capabilities and anticipation of future cyber events are based on analyzing activity that deviates from the baseline. Insurers should work towards achieving or acquiring predictive capabilities, capturing data from multiple internal and external sources, and defining a baseline for behavioural and system activity, including through outsourcing such expertise.

(iv) **Adaptive cybersecurity framework**. – To be effective in keeping pace with the rapid evolution of cyber threats, an insurer shall implement an adaptive cybersecurity framework that evolves with

the dynamic nature of cyber risks and allows the insurer to identify, assess, and manage security threats and vulnerabilities for the purpose of implementing appropriate safeguards into its systems. An insurer should aim to instill a culture of cyber risk awareness whereby its resilience posture, at every level, is regularly and frequently re-evaluated.

(v) **Distil key lessons**. – An insurer shall systematically identify and distil key lessons from cyber events that have occurred within and outside the organization in order to advance its resilience capabilities. Useful learning points can often be gleaned from successful cyber intrusions and near misses in terms of the methods used and vulnerabilities exploited by cyber attackers.

(vi) **Monitor technological developments**. – An insurer shall actively monitor technological developments and keep abreast of new cyber risk management processes that can more effectively counter existing and newly developed forms of cyber attack. An insurer should consider acquiring such technology and know-how to maintain its cybersecurity, including through outsourcing such expertise.

(vii) **Metrics to assess cybersecurity maturity**. – As methods for cyber risk quantification continue to develop, insurers may consider using metrics to assess cybersecurity maturity against a set of predefined criteria, such as operational reliability objectives. Benchmarking enables an insurer to analyze and correlate findings from audits, management reviews, incidents, near misses, tests and exercises, as well as external and internal intelligence.

12. Statement of Compliance with the Directive

The insurers shall submit to the Commission the statement of compliance to this Directive within six months of coming into effect of this Directive, and thereafter by April 30th of every year, along with submission of annual assessment report of cybersecurity framework as required under clause 7 of this Directive.

Any person to whom this directive applies and who contravenes or fails to comply with the requirements of this directive shall be liable to imposition of penalty under section 40A of the Securities and Exchange Commission of Pakistan Act, 1997 which may extend up to ten million rupees and where contravention is a continuing one, with a further penalty which may extend to one hundred thousand rupees for every day after the first during which such contravention continues.

[No.SY/SECP/8/13]

(Bilal Rasul)
Secretary to the Commission