NOTICE TO THE PUBLIC

Subject: SECOND EXPOSURE DRAFT OF MEMORANDUM CIRCULAR ON THE GUIDANCE FOR REGULATED ENTITIES ON ESTABLISHING AND MAINTAINING A CYBER RESILIENCE FRAMEWORK

The public is advised that the Commission *En Banc,* in its meeting held on 22 February 2024 resolve to expose the draft Memorandum Circular on the *Guidance for Regulated Entities on Establishing and Maintaining a Cyber Resilience Framework* for another round of comments.

The Commission hereby requests for comments, suggestions and/or inputs from all concerned on the proposed draft Memorandum Circular by submitting written comments on or before 6 March 2024 through email to msrdsubmission@sec.gov.ph, gclagonoy@sec.gov.ph and ggjarugay@sec.gov.ph with our proposed subject of **"COMMENTS ON THE GUIDANCE FOR REGULATED ENTITIES ON ESTABLISHING AND MAINTAINING A CYBER RESILIENCE FRAMEWORK"**

Issued on 23 February 2024.

The SEC Headquarters, 7907 Makati Avenue
Salcedo Village, Bel-air, Makati City
(+63 2) 8818 0921
www.sec.gov.ph | imessagemo@sec.gov.ph

SEC Memorandum Circular No. ___
Series of 2024

TO : **ALL SEC REGULATED ENTITIES**

SUBJECT : **GUIDANCE FOR REGULATED ENTITIES ON ESTABLISHING AND MAINTAINING A CYBER RESILIENCE FRAMEWORK**

DATE :

WHEREAS, the Philippine government has recognized the importance of information and the vital role of information and communications technology as one of the enablers for nation building.[1]

WHEREAS, the Securities and Exchange Commission (the "Commission") acknowledges that the rapid growth and sophistication of cybercrimes and cyber attacks have increased the vulnerability of data, people, and structures.[2] Further, the dynamic and fluid changes in the cyber environment make the challenges, risks, and threats more complex; therefore, information residing within computer systems, network systems, or applications systems is considered as a critical asset that must be protected and secured from being compromised or breached.[3]

WHEREAS, the Philippine Government promotes to pursue and advance Informational and Cybersecurity as one of its 12-point National Security Agenda, endeavoring to shield the country from computer-generated/cyber-attacks that could cause massive crises in our economy, banking and financial institutions, communications and other critical infrastructures.[4]

WHEREAS, the Commission acknowledges the importance of establishing comprehensive cybersecurity regulations to protect investors, promote market stability and foster trust in the Philippine capital market.

WHEREAS, the Commission recognizes the importance of collaboration and information sharing among financial institutions, regulators and stakeholders to enhance cyber resilience and create greater awareness of the global and local cybersecurity context.[5]

WHEREAS, Section 5 (b) of the Securities Regulation Code (SRC) provides that the Commission has the power to formulate policies and recommendations on issues concerning the capital markets;

[1] National Cybersecurity Plan 2022, p. 6
[2] Philippine Development Plan 2023-2028, p. 302
[3] National Cybersecurity Plan 2022, p. 12
[4] National Security Plan 2017-2022, p. 25
[5] Philippine Development Plan (PDP) 2023-2028, p 171

WHEREAS, in implementing these Guidelines, the Commission recognizes that regulatory approaches tend to be high-level and allow for flexibility, recognizing that there is no "one size fits all" approach that market participants should adopt.

WHEREFORE, IN VIEW OF THE FOREGOING, the Commission shall require all securities markets participants to comply with the following guidelines:

SEC. 1. Objectives and Scope - These guidelines aim to provide guidance to securities markets participants in enhancing their respective cyber resilience. In doing so, covered entities should consider up to what extent the specific provisions of these guidelines might be appropriate given their own cyber security objectives and risk tolerance. A risk-based approach shall be adopted by covered entities in applying these guidelines, and prioritize its risk mitigation efforts such that risk mitigating measures implemented are commensurate with the various levels of cyber risk it faces.

These guidelines shall apply to all securities markets participants, which shall refer to a broad range of participants, entities, and securities and derivatives markets that include trading venues, Trading Participants such as broker-dealers, asset managers, Transfer Agents, Self-Regulatory Organizations, and such other regulated entities with a secondary license issued by the Commission.

SEC. 2. Definition of terms – When used in this circular, the following terms are defined as follows:

2.1. ***Capability/ies*** **-** refers to the people, processes and technologies that entities use to identify, mitigate and manage its cyber risks and to support its objectives.

2.2. ***Cyber-attacks*** **–** the use of an exploit by an adversary to take advantage of a weakness(es) with the intent of achieving an adverse effect on the information and communications technology environment.

2.3. ***Cyber incident*** **-** A cyber event that:

2.3.1. jeopardises the cybersecurity of an information system or the information the system processes, stores or transmits; or

2.3.2. violates the security policies, security procedures or acceptable use policies, whether resulting from malicious activity or not.

2.4. ***Cyber resilience*** **-** an entity's ability to anticipate, withstand, contain and rapidly recover from a cyber attack.

2.5. ***Cyber resilience framework*** **-** Consists of the policies, procedures and controls an FMI has established to identify, protect, detect, respond to and recover from the plausible sources of cyber risks it faces.

2.6. ***Cyber resilience strategy*** **-** An entity's high level principles and medium term plans to achieve its objective of managing cyber risks.

2.7. ***Cyber risk*** **–** The combination of the probability of an event occurring within the realm of an organization's information assets, computer and

communication resources and the consequences of that event for an organization.

2.8. ***Cybersecurity*** – the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber environment and organization and user's assets.

2.9. ***Enterprise Risk Management*** **-** Managing risks at an enterprise level and calls for understanding the core risks that an enterprise faces, determining how best to address those risks, and ensuring that the necessary actions are taken. An enterprise is an organization that exists at the top level of a hierarchy with unique risk management responsibilities.

2.10. ***Incident Response Plan*** **–** the documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber attacks against an organization's information systems(s).

2.11. ***Insider trading*** **–** refers to the act of an insider in selling or buying a security of the issuer, while in possession of material information in respect to the issuer or the security that is not generally available to the public. The definition provided under Sec. 27 of the SRC shall be adopted for purposes of implementing this Guidelines.

2.12. ***Market Participants*** **–** refers to a broad range of participants, entities, and securities and derivatives markets that include trading venues, market intermediaries such as broker-dealers, and asset managers. For the purpose of implementing these Guidelines, Market Participants likewise refer to Transfer Agents, Self-Regulatory Organizations, and such other similar regulated entities with a secondary license issued by the Commission.

2.13. ***Securities Depository*** **-** refers to entities that hold securities accounts, provides central safekeeping and asset services, which may include the administration of corporate actions and redemptions, and plays an important role in helping to ensure the integrity of securities issues (that is, securities are not accidentally or fraudulently created or destroyed or their details changed).

2.14. ***Self-Regulatory Organization (SRO)*** **-** means an organized Exchange, registered clearing agency, organization or association registered as an SRO under Section 39 of the Securities Regulation Code, and which has been authorized by the Securities and Exchange Commission to: (1) enforce compliance with relevant provisions of the Code and rules and regulations adopted thereunder; (2) promulgate and enforce its own rules which have been approved by the Commission, by their members and/or participants, and; (3) enforce fair, ethical and efficient practices in the securities and commodity futures industries including securities and commodities exchanges.

SEC. 3. Establishing a cyber resilience framework - Each Market Participant must adopt a cyber resilience framework that articulates its cyber resilience objectives and cyber risk tolerance, as well as how such Market Participant effectively identifies, mitigates, and manages its cyber risks to support its objectives. Each cyber resilience framework must be considered as continuously developing and Market Participants shall make further efforts to adapt, evolve and improve their cyber resilience capabilities.

SEC. 4. Defining levels of expectation - Market Participants are expected to exercise their sound judgment in defining their respective level of expectation in structuring their cyber resilience capability, taking into consideration their organizational structure, set-up, operations, cross-border presence, their role within the securities market, and the size, volume and value of their transactions, among others. The following levels of expectation shall serve as a guide for Market Participants:

4.1. **Evolving** - Essential capabilities are established, evolved and are sustained across the Market Participant to identify, manage and mitigate cyber risks, in alignment with the cyber resilience strategy and framework approved by the Board. Performance of practices is monitored and managed.

4.2. **Advancing** - Practices involve implementing more advanced tools (e.g. advanced technology and risk management tools) that are integrated across the Market Participant's business lines and have been improved over time to proactively manage cyber risks posed to the Market Participant.

4.3. **Innovating** - This level involves driving innovation in people, processes and technology for the Market Participant and the wider ecosystem to manage cyber risks and enhance cyber resilience. This may call for new controls and tools to be developed or new information-sharing groups to be created.

Established Self-Regulatory Organization and Securities Depository are required to reach the advancing level, as a minimum, with active steps to be taken over time to attain an innovating level, where deemed appropriate.

SEC. 5. Components of the cyber resilience framework - At the minimum, a cyber resilience framework of a Market Participant must be consistent with its enterprise risk management framework and shall integrate the following:

5.1. A cyber resilience strategy that meets the following standards:

5.1.1. Establishment of an internal, cross-disciplinary steering committee comprised of senior management and appropriate staff from multiple business units to collectively develop a cyber resilience strategy and framework.

5.1.2. Must be aligned to the Market Participant's corporate strategy and other relevant strategies.

5.1.3. Approved by the Board of the Market Participant and regularly reviewed and updated according to the Market Participant's threat landscape.

5.2. Procedure on how the Market Participant determines its cyber resilience objectives and risk tolerance, as well as how it effectively identifies, mitigates, and manages its cyber risks to support its objectives.

5.3. Incorporation of the requirements related to governance, identification, protection, detection, response and recover, testing, situational awareness, and learning and evolving. The foregoing requirements are further discussed in these Guidelines.

5.4. Leading international, national and industry-level standards, guidelines or recommendations, reflecting current industry best practices in managing cyber threats, as a benchmark for designing its cyber resilience framework and incorporating the most effective cyber resilience solutions.

5.5. Clear definition of the roles and responsibilities, including accountability for decision-making within the organization, for identifying, mitigating and managing cyber risks.

The cyber resilience framework shall be endorsed by the Market Participant's Board and must be reviewed at least annually and updated when needed to ensure its relevance.

SEC. 6. Role of the Board and Senior Management - A Market Participant's Board shall be primarily responsible for approving its cyber resilience framework and ensuring that cyber risk is effectively managed. In so doing, the Board must ensure the following:

6.1. That it collectively possesses the appropriate balance of skills, knowledge and experience to understand and assess the cyber risks.

6.2. A Chief Information Security Officer (CISO) shall have oversight function on, and shall be primarily responsible and accountable for implementing the cyber resilience framework. A detailed outline of the CISO's responsibilities is discussed in Section 11.

6.3. There is adequate, skilled, knowledgeable, and experienced staff responsible for cyber activities.

SEC. 7. Fundamental principles of risk management to be adopted in the cyber resilience framework - – Market Participants shall integrate their cyber resilience framework in its enterprise risk management program and shall observe the following fundamental principles in its risk management:

7.1. **Identification** – Market Participants should be able to identify its information assets and system configurations, including processes that are dependent on third-party service providers, in order to know at all times the assets that support its business functions and processes. A Market Participant should carry out a risk assessment of assets and

classify them in terms of criticality. It should identify and maintain a comprehensive inventory of both individual and system credentials to know the access rights to information assets and their supporting systems. The Market Participant shall review and update this inventory on a regular basis.

7.2. **Protection** – Market Participants should implement a comprehensive and appropriate set of security controls that will allow it to achieve the security objectives needed to meet its business requirements. The Market Participant should implement these controls based on the identification of its critical functions, key roles, processes, information assets, third-party service providers and interconnections, as per the risk assessment in the identification phase. The security controls should be monitored and audited regularly to ensure that they remain effective and have been applied to all assets where they might be needed.

7.3. **Detection** – Market Participants should define, consider and document the baseline profile of system activities to help detect deviation from the baseline. Appropriate capabilities, including the people, processes and technology should be developed to monitor and detect anomalous activities and events, by setting appropriate criteria, parameters and triggers to enable alerts. The detection capabilities of a Market Participant shall be periodically reviewed, tested, and updated appropriately, in a controlled and authorized manner.

7.4. **Response and Recovery** – Market Participants must develop an incident response plan for those types of incidents to which the organization is most likely to be subject. In line with this, market participants must have a recovery plan to manage cybersecurity events or incidents in a way that limits damage and prioritizes resumption and recovery actions in order to facilitate the processing of critical transactions, increases the confidence of external stakeholders, and reduces recovery time and costs. In line with this, members of the Market Participant's incident response team must have the requisite skills and training to address cyber incidents.

7.4.1. **Resumption within two hours to complete settlement by end of day** - When applicable to its operations, a Market Participant shall design and test its systems and processes to enable the safe resumption of critical operations within two hours of a disruption and to enable itself to complete settlement by the end of the day of the disruption, even in the case of extreme but plausible scenarios. This notwithstanding, a Market Participant should exercise judgment in effecting resumption so that the attendant risks do not thereby escalate.

SEC. 8. Testing - Market Participants shall establish and maintain a comprehensive testing programme as an integral part of its cyber resilience framework, which shall be subject to periodic review and updated on a regular basis. Critical systems, applications and data recovery plans, including governance and coordination, and crisis communication arrangements and practices shall be tested at least annually.

SEC. 9. Situational Awareness - Market Participants shall have capabilities in place to gather cyber threat information from internal and external sources. Gathered information shall be analyzed and continuously used to assess and manage security threats and vulnerabilities to implement appropriate cybersecurity controls and in regularly enhancing the cyber resilience framework.

Market Participants shall define the goals and objectives of information sharing which shall include collecting and exchanging information in a timely manner that could facilitate the detection, response, resumption and recovery of its own systems and those of other sector participants during and following a cyber-attack. Trusted and safe channels of communication with direct stakeholders must be adopted by each market participant for exchanging information.

SEC. 10. Learning and evolving - Market Participants shall aim to instill a culture of cyber risk awareness whereby its resilience posture, at every level, is regularly and frequently re-evaluated.

Senior management should ensure that a programme for continuing cyber resilience training and skills development is established for all staff. The training programme should include the Board members and senior management and should be conducted at least annually. The annual cyber resilience training should include incident response, current cyber threats and emerging issues. The Market Participant shall ensure that the training programme equips staff to deal with cyber incidents, including how to report unusual activity.

SEC. 11. Appointment of a Senior Executive - A Market Participant shall appoint a senior executive, normally a Chief Information Security Officer (CISO), who is responsible for all cyber resilience issues within the Market Participant and with regard to third parties. The Senior Executive ensures that the cyber resilience objectives and measures defined in the Market Participant's cyber strategy, cyber resilience policies and guidelines are properly communicated both internally and, when relevant, to third parties, and that compliance with them is reviewed, monitored and ensured. The following are the minimum measures to be implemented by Market Participants in appointing its CISO:

11.1. Each Market Participant shall have its own senior executive or in-house CISO, depending on the specific structure and organizational set-up. In case of group entities, a group-wide CISO may be appointed.

11.2. The Senior Executive or CISO must be independent in order to avoid any potential conflicts of interest. In this regard, the CISO must be able to act independently from the IT/operations department and directly report to senior management and the Board and at any time.

11.3. The appointed senior executive or CISO shall not be involved in internal audit activities.

SEC. 12. Data privacy and disclosure of nonpublic personal information - It is the policy of the Commission that all Market Participants must protect its client's right to privacy. In this regard, Market Participants must comply with the requirements of Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012, its implementing rules and regulations, and other relevant rules that may be applicable to the protection of personal data, whether issued by the Commission or other government agencies.

Market Participants should establish suitable response measures to address any security breach that may occur involving the personal information of its clients, including matters such as timely notification to affected clients and relevant competent authorities.

SEC.13. Regular review of cyber resilience framework. – Market Participants should regularly review their cyber resilience framework to ensure they continue to be appropriate to manage adverse impacts of the cyber risks in their operations.

SEC. 14. Report to the Commission. – A regular review and audit by an independent firm must be conducted on the Market Participant's cyber resilience framework, including relevant documents and systems, such as its business continuity plan, disaster recovery and risk management systems, at least once every three years or as frequent as the Commission may deem necessary. Results of such review and audit shall be submitted to the Commission.

SEC. 15. Availability of documents and policies relating to cyber resilience - Policies and documents pertinent to the implementation of the cyber resilience framework shall be made available by each Market Participant to the Commission, in the event of audit or on-site examinations.

SEC. 16. Disclosures required – A cyber incident shall be reported by the Market Participant to the Commission, not later than four (4) days from the discovery of its occurrence, insofar as such incident is material event which shall include but not limited to the following:

16.1. It creates a risk on the investments on any of the securities of the Market Participant, or its investors, as the case may be,

16.2. Ten percent (10%) or more change in the financial condition or results of operation of the Market Participant.

16.3. Any similar event that would reasonably be expected to affect the decision of the Market Participant's investors.

16.4. Other material events analogous to the foregoing

In determining the materiality of a certain cyber incident, Market Participants must give weight on the importance of any compromised information and of the impact of the incident on its operations. These may include harm that such cyber incident may cause to the Market Participant's reputation, financial performance, customer and vendor relationships, as well as the possibility of litigation or regulatory investigations or actions.

When personal data has been compromised by a certain cyber incident, the concerned Market Participant shall disclose the said event to the Commission in accordance with the relevant rules and regulations issued by the National Privacy Commission.

SEC. 17. Insider Trading – Companies and their directors, officers, and other corporate insiders shall, in all cases, comply with the laws related to insider trading, in connection with trading the securities of any publicly listed company (PLC) while in possession of any material non-public information relating to cybersecurity risks and incidents, including vulnerabilities and breaches of such PLC.

SEC. 18. Supplemental Regulations – This circular may be supplemented by relevant regulations which the Commission may from time to time issue.

SEC. 19. Applicability of certain laws and regulations – The provisions of the SRC and its implementing rules and regulations, and other relevant laws and regulations insofar as they are applicable and not inconsistent herewith, shall apply suppletorily.

SEC. 20. Administrative Sanctions – The Commission shall impose sanctions provided under the SRC and its implementing rules and regulation in case of violation of this circular. Additional sanctions provided under relevant laws, rules and regulations shall also be imposed in so far as it may be applicable.

SEC. 21. Transitory Provision - Market Participants shall comply with the provisions of these Guidelines within at least one (1) year but not exceeding two (2) years from the date of effectivity, taking into account their respective levels of expectation and the complexities of their information technology structures.

SEC. 22. Effectivity – This circular shall take effect fifteen (15) days after its complete publication in the *Official Gazette* or in at least two (2) newspapers of general circulation in the Philippines.

Makati City, Metro Manila, _____ 2024.

EMILIO B. AQUINO
Chairperson