PAKISTAN STOCK BROKERS ASSOCIATION

(A company setup under section 42 of the Companies Act 2017)

Regd Office: Mezzanine Floor, Trading Hall, Stock Exchange Building, Stock Exchange Road, Off I.I Chundrigar Road, Karachi.

Tel: 021-32401278, E-mail: secretariat@psba.pk, Web: www.psba.pk, Fax: 021-32401279

PSBA/Notice-170 August 7, 2024

NOTICE FOR MEMBERS

SOURCE CODE REVIEW, AND VULNERABILITY & PENETRATION TESTING CERTIFICATION STANDARDS

Respected Members,

This is in continuation of our letter dated April 1, 2024, addressed to the Securities and Exchange Commission of Pakistan (SECP), and the subsequent meetings held with the Pakistan Stock Exchange (PSX) and SECP.

Kindly note that the agreed-upon procedure, duly finalized by the SECP, is attached for your kind perusal.

We would like to summarize the conclusion as follows:

Following the completion of the Review & Testing, the vendor will provide a formal confirmation to their respective broker client, certifying that the System follows the Minimum Standards. Subsequently, each relevant securities broker will forward this confirmation with its Covering Letter to the Exchange.

We trust that this information will be helpful for your ongoing compliance and operational requirements.

Should you have any questions or need further clarification, please do not hesitate to contact us.

Thank you,

_____sd_____
BILAL FAROOQ ZARDI
Secretary General

Copy to:

1. PSBA Website

Enclosed:

1. Procedure as discussed above.

BACKGROUND:

Pakistan Stock Brokers Association (**PSBA**) vide email dated April 22, 2024 informed PSX that SECP in its recent meeting held with PSBA advised PSBA to engage with the PSX team to explore alternative solutions in order to address the issues relating to the "Source Code Review, and Vulnerability & Penetration Testing Certification" of the systems procured by the brokers or developed in-house.

Consequently, PSBA approached PSX to deliberate the matter in detail and devise an alternate arrangement. As a result of the deliberations held among relevant departments of PSX and after obtaining feedback from SECP, the following procedures are agreed to be implemented:

- Since PSX has prescribed minimum Information Security Standards as well as the Back-Office Standards for securities brokers (collectively referred to as "**Minimum Standards**"), which mandate that the Back-Office System, Order Management System or Applications (collectively referred to as "**System**"), providing services to securities brokers should be meeting the Minimum Standards prescribed by PSX. Therefore, the standard version of the System/Software shall mandatorily undergo the source code review, and vulnerability & penetration testing ("**Review & Testing"**) every two years to ensure compliance with the Minimum Standards.

- The cost of such Review & Testing of the System shall be mutually decided by the vendors and the respective securities brokers in consultation with PSBA.

- If a securities broker has developed its own System in-house, it shall also ensure that the same meets the Minimum Standards and undergoes the required Review & Testing.

- In case, any securities broker desires to obtain enhanced features/ services of the System procured from the vendor, the additional features/services shall be subject to Review & Testing at a cost to be mutually decided by the vendors and respective securities broker in consultation with PSBA.

- To give effect to the above, Service Level Agreement signed by the vendor and the securities broker must cover the below aspects.

MANNER OF SUBMITTING COMPLIANCE REPORT OF SYSTEM REVIEW & TESTING:

- The independent audit firm to be engaged by the securities brokers/ PSBA will perform the Review & Testing of respective Systems either procured from vendors **OR** developed in-house.

  Following the completion of the Review & Testing, the vendor will provide a formal confirmation to their respective broker client, certifying that the System follows the Minimum Standards. Subsequently, each relevant securities broker will forward this confirmation with its Covering Letter to the Exchange.

- The independent audit firm should have the relevant expertise and experience in cyber security/ specialized IT-related audits preferably in the financial sector and must also comply with additional criteria to be prescribed by the securities brokers in consultation with PSBA.

- Any new securities broker or an existing securities broker deciding to procure the System from the vendor in the future, shall also be required to submit above above-referenced confirmation to the Exchange accompanied with its own Covering Letter.

AGREED-UPON PROCEDURES FOR REVIEW & TESTING OF BACK OFFICE SYSTEM & OMS DEVELOPED OR PROCURED BY THE BROKERS

- The Covering Letter shall contain an undertaking of the securities brokers that the Systems in use, either developed in-house or procured from the vendor, follow the Minimum Standards/ standards version. In case of any customization/ enhancement or any difference in the source code between the standard System and the installed System, the changes should also be subject to Review & Testing.

- The existing securities brokers shall be required to submit the Covering Letter accompanied with the undertaking and the confirmation certificate from the vendor, <u>within 60 days from the date of circulation of this document to all securities brokers.</u>

- In all other cases including procurement of System, customization/ enhancement of existing System or change of System, securities brokers shall be required to submit the Covering Letter accompanied with the undertaking and the confirmation certificate from the vendor, <u>within 15 days from the date of occurrence of such event.</u>

- The securities brokers shall be required to submit the following additional information to the Exchange for preservation of records:

  a. Details and number of Systems installed;
  b. Details of compatibility connections in case of a heterogeneous system.
  c. Details of updates/ changes in the System as and when such event occurs.

  Note: The information mentioned above shall be submitted to the PSX within the Covering letter as required above.

NOTE:

It is pertinent to mention that the "Minimum Information Security Standards for Security Brokers" notified by PSX vide Notice No. N-670 dated June 27, 2023, or as amended from time to time, are applicable to all securities brokers on their IT/IS infrastructure and Systems which include Back-Office System, OMS and any other applications installed. The relevant section of the aforementioned information security standards is reproduced below for ready reference:

> *"These Standards have been established to prescribe minimum standards to be complied with by the brokers pertaining to their software or applications which include order management system, front office, back office and internet-based trading systems and/or other related software used by brokers directly or indirectly or outsourced to suppliers for the purpose of customer onboarding, trading, risk management, clearing and settlement, and preparation and maintenance of books and accounts etc. or related activities. These Standards also prescribes requirements regarding regular testing & certification, standards, requirements relating to supplier management, clouding services and incidence management in case of any security breach."*

PSX reserves the right to inspect any securities broker(s) in respect of their compliance with the above-mentioned requirements in such manner as prescribed under the relevant Regulations of PSX and SECP.