PAKISTAN STOCK EXCHANGE

NOTICE

PSX/N-670 **June 27, 2023**

NOTICE FOR ALL TRE CERTIFICATE HOLDERS

MINIMUM INFORMATION SECURITY STANDARDS FOR COMPLIANCE BY THE SECURITIES BROKERS

This is further to the Pakistan Stock Exchange Limited (PSX) Notice No. PSX/N-260 dated March 16, 2023 whereby PSX notified Minimum Information Security Standards **(Standards)** for seeking comments and feedback of the securities brokers.

After consultation with the relevant stakeholders, PSX is pleased to notify the Standards attached herewith as **Annexure-A**.

Accordingly, all securities brokers are hereby advised to make necessary arrangements to ensure meticulous compliance with these Standards.

AJEET KUMAR
Chief Regulatory Officer

ABBAS H. ZAIDI
Chief Risk Management Officer

Cc:

1. *The Director/HoD, PRDD, (SMD), SECP*
2. *Add. Director, Supervision Division, Offsite-I Dept., SECP*
3. *Director, Supervision Division-Onsite Dept., SECP*
4. *The Chief Executive Officer, PSX*
5. *The Chief Executive Officer, CDC*
6. *The Chief Executive Officer, NCCPL*
7. *The Chief Executive Officer, PMEX*
8. *The Chief Executive Officer, E-Clear*
9. *The Chief Executive Officer, IFMP*
10. *All Heads of Departments, PSX*
11. *The Regional Heads-ISB & LHR, PSX*
12. *Pakistan Stock Broker Association*
13. *PSX Website*

Annexure A

PAKISTAN
STOCK EXCHANGE
LIMITED

MINIMUM INFORMATION SECURITY STANDARDS FOR SECURITIES BROKERS

EFFECTIVE DATE: JUNE 27, 2023

This document contains the minimum information security standards prescribed by the Pakistan Stock Exchange Limited (PSX) for adoption and compliance by the Securities Brokers.

PSX reserves the right to amend any part of this document and notify the same for information and compliance.

PAKISTAN STOCK EXCHANGE LIMITED

TABLE OF CONTENT

PREAMBLE: 3

SCOPE: 3

REVIEW 4

SHARED RESPONSIBILITIES 4

CONTROLS APPLICABILITY 5

INFORMATION SECURITY STANDARDS 5

1. RESPONSIBILITIES OF BOARD OF DIRECTORS 5
2. HUMAN RESOURCE SECURITY STANDARDS 5
3. ASSET MANAGEMENT STANDARDS 6
4. ACCESS CONTROLS STANDARDS 6
5. DATA SECURITY STANDARDS 8
6. PHYSICAL AND ENVIRONMENTAL SECURITY STANDARDS 8
7. OPERATIONS SECURITY STANDARDS 9
8. NETWORK AND COMMUNICATIONS SECURITY STANDARDS 10
9. REMOTE CONNECTIVITY STANDARDS 10
10. PATCH MANAGEMENT STANDARDS 11
11. SUPPLIER MANAGEMENT STANDARDS 11
12. APPLICATION SECURITY STANDARDS 12
13. TESTING & CERTIFICATION STANDARDS 15
14. INCIDENT MANAGEMENT STANDARDS 15
15. BUSINESS CONTINUITY PLAN (BCP) AND DISASTER RECOVERY (DR) STANDARDS 15
16. INFORMATION SECURITY POSTURE REVIEW & ASSESSMENT STANDARDS 16
17. COMPLIANCE AND AUDIT STANDARDS 16
18. ANNEXURES 17

A. SoA Template 17

B. Asset Inventory Template 17

C. Cyber/Information Security Incident Reporting Format 17

19. GLOSSARY 18

PREAMBLE:

The technological advancement has been playing an instrumental role in driving organizations to unprecedented levels of growth and success. However, as technologies advance, the cybercrimes increase and may result in corporate security breaches. This has led to companies adopting various measures, techniques and tools to curb the cybersecurity threats.

The securities brokerage industry of Pakistan has also gone through the significant digital transformation over time in the shape of introduction of automated trading system, shift towards digital marketing and onboarding of customers, online trading, cloud computing, electronic front and back end applications etc. These changes coupled with the proliferation of access points/ mechanisms and the consolidation of information repositories, have resulted in securities brokers facing increasingly complex challenges in maintaining the confidentiality, integrity and availability of its information, which is critical for the efficient and seamless capital market operations filled with customer trust and confidence.

In view of the above, it is imperative for PSX to consolidate and redefine the minimum information security standards for securities brokers in line with international best practices of regional and global stock exchanges.

SCOPE:

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 incident management in case of any security breach.

In order to ensure consistent application of security standards across the brokerage market, these Standards shall be applicable on all the brokers, their employees and suppliers/vendors and the software or applications used directly or indirectly for the aforementioned purposes. The securities brokers may put in place additional security measures as deemed appropriate over and above the minimum standards prescribed in these Standards.

These Standards are being prepared and notified in accordance with requirements of Clause 4.25 and Chapter 9 of PSX Regulations:

> ***4.25. IT AND INFORMATION SECURITY REQUIREMENTS FOR THE SELECTION OF SOFTWARE VENDORS AND USAGE OF SOFTWARE BY THE TRE CERTIFICATE HOLDERS:***
>
> *4.25.1. The TRE Certificate Holders shall:*
>
> *(a) Ensure that the software or application, which means electronic data processing system; excluding network or communications equipment; for the purpose of this clause, used directly or indirectly for the purpose of trading, risk management, clearing and settlement, and preparation and maintenance of books and accounts etc. meet the bare minimum standards/specifications, regular testing including vulnerability assessment and penetration testing and certification requirements prescribed by the Exchange from time to time.*

(b) *Comply with information technology and information security requirements as prescribed by the Exchange.*

(c) *Use the software either procured from the eligible vendors or provided by the Exchange or developed in-house by the software development team of the TRE Certificate Holder.*

The Exchange shall make available the eligibility criteria and the list of eligible vendors on its website.

(d) *Ensure that the Exchange provided endpoint security and antivirus solution remain installed and operational at all times on all trading terminals.*

(e) *Ensure that only Exchange certified ancillary software are installed on the trading terminals.*

(f) *Ensure that multi-factor authentication is in place to use Exchange applications.*

4.25.2. The Exchange may conduct verification, review or inspection of Securities Brokers in accordance with a risk-based plan duly approved by the RAC to ensure their compliance with the requirements of clause 4.25.1 in such manner as specified by the Exchange from time to time.

4.25.3. The Exchange may require Securities Broker(s) to submit audit report on compliance with the requirements of clause 4.25.1 within such time and in such manner as specified by the Exchange.

4.25.4. The Exchange shall take disciplinary action(s) against a TRE Certificate Holder which fails to comply with requirement of this clause.

9.7 INFORMATION AND INFRASTRUCTURAL SECURITY MEASURES:

The Securities Broker providing IBTS shall ensure that:

(a) *The internet trading system is in compliance with the Information Security policy of the Exchange and the service provider and the Securities Broker.*

REVIEW

These Standards can be amended by the Information Security Office of PSX as per the established process as and when deemed appropriate in accordance with capital market's overall strategy and need.

SHARED RESPONSIBILITIES

Responsibilities for effective implementation of the information security standards rests with multiple stakeholders of the Capital Market, important of them include:

(a) PSX is responsible for the development, updating, dissemination and monitoring compliance of these Standards.
(b) PSX is responsible for awareness of stakeholders concerning these Standards.
(c) The brokers must ensure compliance with these Standards at all times.

(d) The brokers must extend full support and cooperation to SECP, PSX and/or the audit firm staff during inspection, review or monitoring and verification process for ascertaining compliance.
(e) The vendors/suppliers engaged by the brokers must develop the applications in line with these Standards.

CONTROLS APPLICABILITY

All controls specified in the information security standards are mandatory, wherever technically feasible. However, there may be cases where certain controls may not be applicable to the software being developed due to the technological or other reasons, in which case the brokers or/and software vendor shall provide sufficient details of those controls that are or cannot be implemented along with the justification. Brokers or/and software vendor shall maintain an up-to-date Statement-of-Applicability (SoA) (*refer to Annexure "A")* with rational explaining why a specific control is not applicable at their environment.

INFORMATION SECURITY STANDARDS

1. RESPONSIBILITIES OF BOARD OF DIRECTORS

(a) Ensure that a comprehensive information technology and security policy [**"Policy"**] encompassing the standards prescribed in these Standards at a minimum is formulated and communicated to all employees.
(b) Review, approve and ensure implementation of the aforesaid policy.
(c) Review and approve the criteria and procedures for engagement of suppliers for outsourcing activities clearly defining roles and responsibilities of the staff to be involved in the engagement process.
(d) Ensure adequate and timely allocation of resources to effectively implement the information security measures as per the approved policy.
(e) Ensure that an effective technology risk management is implemented and periodically reviewed and the same includes the risk identification, assessment, mitigation, monitoring and reporting on timely basis.
(f) Ensure that an adequate oversight mechanism is implemented to ensure strict adherence with the Policy.
(g) Review and approve all important decisions on critical issues related to information security.
(h) Ensure periodic awareness and training sessions are provided to employees at all levels.

2. HUMAN RESOURCE SECURITY STANDARDS

(a) All employees must sign a contract of employment establishing their responsibilities for protecting the confidentiality and integrity of the data and information.
(b) All employees who are given access to confidential information should sign a confidentiality or non-disclosure agreement prior to being given access to confidential information.
(c) All employees must have relevant knowledge and understanding so that they are aware of any security threats and prepare to adopt security measures in their routine activities.
(d) Ensure that duties of all employees are segregated in order to prevent any single person from performing a malicious or illegal activity undetected.
(e) All employees must receive ongoing, updated security awareness training to ensure their understanding of current threats and corresponding security practices to mitigate such threat.
(f) A formal disciplinary process must be in place to take action against employees involved in breach of information security standards.
(g) Management must have an arrangement to promptly notify to relevant departments such as administration, security, IT, business development etc. regarding removal/resignation/transfer of employee and prompt action is taken to revoke or amend his/her access rights and assets are taken back.

3. ASSET MANAGEMENT STANDARDS

(a) Maintain list of inventory of all assets associated with information and information processing facilities.
(b) Identify owners of all the assets, define classification of the assets based on confidentiality, integrity, availability and relevant interested party requirements and keep their classification up to date.

(c) Information Confidentiality Classification Levels:
Level 1: Public – Disclosure causes no harm
Level 2: Internal – Disclosure causes minor embarrassment or minor operational inconvenience
Level 3: Confidential – Disclosure has a significant short-term impact on operations or tactical objectives
Level 4: Restricted – Disclosure has a serious impact on long term strategic objectives or puts the survival of the organization at risk

(d) Ensure the information and other associated assets are appropriately protected, used, handled and discarded.
(e) Formulate an internet access policy to monitor and regulate the use of internet and internet-based services such as social media & cloud-based internet storage sites, etc. within the broker's critical IT infrastructure.
(f) Identify critical assets based on their sensitivity and criticality for business operations and services. Moreover, identify relevant cyber risks (threats and vulnerabilities), along with the likelihood of such threats and its impact on the business in order to deploy appropriate controls considering criticality of these assets.

4. ACCESS CONTROLS STANDARDS

All computer systems must have a log-on authentication procedure including at-least unique user ID & password.

User Access Controls

(a) Unique user IDs, preferably identifiable such as user name, should be used to enable users to be linked to and held responsible for their actions.
(b) The application identifiers should not be displayed until log-on process has been successfully completed.
(c) Help message should not be provided during the log-on procedure to avoid aiding an unauthorized user.
(d) Log-on information should only be validated upon completion of all input data. If an error condition arises, application should not indicate which part of the data is correct or incorrect.
(e) The log-on procedure should protect against brute force log-on attempts, such as via restrictions on the number of consecutive incorrect log-in attempts for username and password-based authentication.
(f) Inactive sessions should be locked/terminated after a maximum of 15 minutes of inactivity (even shorter time period is encouraged), and the session lock should be retained until the user re-establishes access using the established identification and authentication procedure.
(g) All critical systems accessible over the internet should have Multi-Factor Authentication (MFA).
(h) The Application should force the user to change the password at the time of first login.
(i) No person by virtue of rank or position should have any intrinsic right to access confidential data, applications, system resources or facilities.
(j) All access must be provided on a need-to-know basis, i.e., a user should only be granted access to the information they need to perform their job responsibilities/tasks/role, to limit the exposure to user related risks. Such access should be for the period when the access is required and should be authorized using strong authentication mechanisms.
(k) Employees and outsourced staff such as employees of vendors or service providers, who may be given authorized access to the critical systems, networks and other computer resources, should be subject to stringent supervision, monitoring and access restrictions. Any Application offered by brokers to customers

containing sensitive, private, or critical data such as IBTS, Back office, RDA etc. referred to as "Application" hereafter over the Internet should only be accessed via password requirement for users.

Password Management

The application should provide capability to enforce password control including complexity, expiration, account lockout and re-use time.

(a) Users shall be authenticated to application using a minimum of user ID and password combination.
(b) The following password controls shall be enforced at a minimum,
    (i) Access to systems shall not be allowed until a password has been authenticated with unique username.
    (ii) A system-based confirmation procedure shall be in place to allow for input errors at the time of password selection.
    (iii) Passwords shall be at least 10 characters in length.
    (iv) Passwords shall include a mixture of the following,
        a. Uppercase characters (A, B, C ...);
        b. Lowercase characters (a, b, c ...);
        c. Numbers (0, 1, 2 ...); an
        d. Special Characters (!, @, # ...).
    (v) User passwords shall be changed at least every 120 days.
    (vi) Passwords shall be changed at least 3 times before re-use.
    (vii) After 5 failed login attempts, the account should be locked temporarily and the user should contact Administrator to reset the password or the account may automatically unlock after 30 minutes.
    (viii) In case of customer facing application, after 5 failed login attempts, the customer's account can be set to a "locked" state where further logins are not possible until a password and authentication reset is performed, for instance, a secure unique link that is sent to the customer's registered e-mail, a random OTP (One Time Password) that is sent as an SMS to the customer's registered mobile number, or manually by the broker after verification of the customer's identity etc.
    (ix) Initial passwords provided to users upon registration will be set to a unique value per user. The user shall be forced to change this initial password at the time of first login.
    (x) Passwords shall not be displayed on the screen in clear text, be printed in clear text or be cached.
    (xi) Passwords shall be transmitted encrypted over a network, to avoid being captured by a network 'sniffer' program.
    (xii) Passwords shall not be stored in clear text on systems, storage devices, configuration files, logs or similar files accessible by system administrators and/or developers. Memory used for deciphering and checking passwords shall be cleared once processing is complete.
    (xiii) Monitoring mechanism shall be in place to detect multiple failed attempts and/or login attempts outside office timings.
    (xiv) User access shall be reviewed at-least once annually.

User Administration

(a) Unique security administrator IDs (only identifiable named users) shall be used to enable administrators to be linked to and held responsible for their actions; the use of shared/group IDs should only be permitted where they are necessary for business or operational reasons and should be approved and documented.
(b) Segregation of duties shall be enforced for access management roles and responsibilities to ensure that no single individual can make changes to access rights without the explicit approval of authorized personnel. At a minimum, the following functions should be segregated,
    (i) Request for user access;
    (ii) Approval of request;
    (iii) Implementation of request; and

(iv) Monitoring of changes.

(c) The user access shall be configured at a granularity level that sufficiently caters business confidentiality, integrity and segregation of duty requirements.

(d) If the system architecture does not allow for the implementation of access control at the required granularity level, a compensating control should exist to mitigate risk.

(e) Privileged access rights shall be assigned to a user ID different from those used for regular business activities. Regular business activities shall not be performed from a privileged ID.

(f) In order to further support above mentioned aim, the application shall have user administration interface with maker/checker control in place.

(g) User Management must address deactivation of access of privileges of users who are leaving the organization or whose access privileges have been withdrawn on his/her last working day.

(h) The application shall create detailed logs for each of the above activities.

(i) Privileged users' access shall be reviewed at-least on a quarterly basis.

(j) Monitoring mechanism shall be in place to detect all login attempts outside office timings.

(k) The application shall have the functionality available to create following on-demand reports:

(i) Report 1 – User Access Summary Report

(ii) Report 2 – User Access Detailed Report

(iii) Report 3 – Information Security Administrator Detailed Report

5. DATA SECURITY STANDARDS

(a) Critical data shall be stored encrypted at all times. This is an all-encompassing requirement that applies to data stored in any medium, through any mechanism, in any format.

(b) Critical data shall be transmitted encrypted at all times. This is an all-encompassing requirement that applies to data transmitted between any two nodes on the wire, through any mechanism, and in any format.

(c) The information security policy should also cover use of devices such as mobile phones, faxes, photocopiers, scanners, etc., within their critical IT infrastructure, that can be used for capturing and transmission of sensitive data. For instance, defining access policies for personnel, and network connectivity for such devices etc.

(d) Implement strict data access controls amongst personnel, irrespective of their responsibilities, technical or otherwise. It is not feasible for certain personnel such as System Administrators and developers to not have privileged access to databases. For such cases, take strict measures to limit the number of personnel with direct access, and monitor, log, and audit their activities. Take measures to ensure that the confidentiality of data is not compromised under any of these scenarios.

(e) Ensure that all critical and sensitive data is adequately backed up as per its data retention policy and that the backup locations are adequately secured.

6. PHYSICAL AND ENVIRONMENTAL SECURITY STANDARDS

(a) Develop security perimeters to protect areas that contain information systems to prevent unauthorized physical access, damage, and interference.

(b) Monitor physical access to the information systems to detect and respond to physical security incidents.

(c) Protect information systems from power failure and disruptions caused by a failure in supporting utilities.

(d) Restrict physical access to the critical systems to minimum or only to authorized officials. Physical access of outsourced staff/visitors should be properly supervised by ensuring at the minimum that outsourced staff/visitors are accompanied at all times by authorized employees.

(e) Physical access to the critical systems should be revoked immediately if the same is no longer required.

(f) Ensure that the perimeter of the critical equipment room, if any, is physically secured and monitored by employing physical, human and procedural controls such as the use of CCTVs and card access systems, etc. where appropriate.

(g) **Removable Storage Media:** Access to removable storage media must be restricted only to authorized personnel and adequately protected from physical and environmental damage, equipment should not be taken off-site without prior authorization data on removable storage media must be password protected and encrypted (where feasible) and movement of the assets should be recorded accordingly. All items of equipment containing storage media must be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

(h) **Secure disposal or re-use of equipment:** Authorized persons are allowed to dispose the equipment containing storage media. The equipment containing storage must be formatted, destroyed, deleted or overwritten using techniques that ensure the original information is non-retrievable before disposal. Records for the disposed equipment should be maintained. The brokers shall formulate a data-disposal and data-retention standards to identify the value and lifetime of any record.

(i) **Emergency Procedures:** Emergency and evacuation procedures must be documented and made available to all personnel. The emergency procedures must be tested at least once a year.

7. OPERATIONS SECURITY STANDARDS

(a) Document procedures for operational activities such as system start-up and close-down, backups, media handling, equipment maintenance, and computer room.

(b) Specify the operational instructions, including the installation and configuration of systems; processing and handling of information both automated and manual; backup; support and escalation contacts including third party support; media handling instructions; system restart and recovery procedures; and management of audit-trail and system log information.

(c) Maintain and regularly update the documents in relation to Operations Security in order to ensure information is up-to-date, complete and accurate.

(d) A change management procedure should be established. This should include documentation of all changes to the systems including information processing. Further, any change should be assessed to consider its potential impacts, should be duly approved by relevant authorized authorities and tested prior to its implementation. All changes made must be logged and the audit log containing all relevant information must be retained.

(e) Establish capacity management plan for mission critical systems.

(f) Mitigate the risks of accidental change and unauthorized access to operational software and business data, the process should include: a) Development; b) Test; and c) Production.

(g) Testing environment should be consistent with the production environment to ensure adequate levels of confidence in the testing.

(h) Record all backup media, uniquely identified, stored securely and subjected to secure disposal procedures.

(i) Protect backups by means of encryption where confidentiality is of importance. All storage media must be uniquely labelled to identify the contents. Periodically test restoration of backup data. Event logs, including the operator console activity, where applicable, must be maintained as an audit trail and reviewed.

(j) Place controls to ensure information and processing facilities are protected against malware.

(k) Establish and Implement controls that prevent or detect the use of unauthorized software.

(l) Implement controls that prevent or detect the use of known or suspicious malicious websites.

(m) Implement controls that prevent or detect the misuse of corporate email.

(n) Establish data leakage prevention or detection controls.

(o) Place mechanism to detect, analyze, and respond to security threats before they harm business operations.

(p) Review of the software and data content of systems supporting critical business processes must be conducted regularly and the presence of any unapproved applications or files or unauthorized amendments must be formally investigated.

(q) Install and regularly update malware detection software.

(r) Business continuity plans must include recovering from malware attacks and any other cyber threats covering all necessary data and software backup and recovery arrangements, and isolating environments when there are catastrophic impacts.

(s) Establish appropriate security monitoring systems and processes to facilitate continuous monitoring of security events / alerts and timely detection of unauthorized or malicious activities, unauthorized changes, unauthorized access and unauthorized copying or transmission of data / information held in contractual or fiduciary capacity, by internal and external parties. The security logs of systems, applications and network devices exposed to the internet should also be monitored for anomalies.

8. NETWORK AND COMMUNICATIONS SECURITY STANDARDS

(a) Documented and approved Network Architecture must be available.

(b) Ensure information in networks and its supporting information processing facilities are adequately protected from unauthorized access.

(c) Ensure network switches and routers (including firewalls, content switches, IDS etc.) have well defined access controls.

(d) Establish controls to safeguard the confidentiality and integrity of data that are transmitting over public networks or wireless networks.

(e) Segregate the group of information services, users and information based on different network domain.

(f) Use cryptographic techniques to protect the confidentiality, integrity and authenticity of information transmitted through mobile or removable media.

(g) Develop procedures to control the flow of information and access control between the internal and external network should be established.

(h) Install network security devices, such as firewalls, proxy servers, intrusion detection and prevention system (IDS/IPS) to protect broker IT Infrastructure which is exposed to internet, from security exposures originating from internal and external sources. Firewalls should be configured to block all services not required and disable unused ports, hide and prevent direct accessing of trusted network addresses from non-trusted networks, and maintain comprehensive audit trails.

(i) Deploy adequate controls to address virus/ malware/ ransomware attacks. These controls may include host/network/application-based IDS systems, customized kernels for Linux, anti-virus and anti-malware software etc.

(j) Install the most up-to-date anti-virus software of corporate standard on all critical servers and workstations.

(k) Ensure that PSX provided antivirus solution always remain installed & operational on all trading terminals.

(l) Ensure that only PSX certified ancillary software are installed on the trading terminals.

(m) For brokers Back Office System, adequate measures should be taken to isolate and secure the perimeter and connectivity to the servers running back office trading applications.

9. REMOTE CONNECTIVITY STANDARDS

(a) Maintain detailed access log.

(b) Put in place appropriate security controls for remote access services.

(c) Protect critical data in-transit (e.g., encryption).

(d) It is the responsibility of connecting parties with VPN privileges to ensure that unauthorized users are not allowed to access internal networks.

(e) Remote connectivity shall be authenticated, preferably by using one-time password such as a token device.

(f) When actively connected to the corporate network, VPN shall force all traffic directed to and from the customer PC (or network) over the VPN tunnel, mainly includes business applications only. All other traffic shall be dropped to enter in this tunnel.

(g) Any software for VPN probes or other such tools shall not be used for any reason.

(h) Any user found to have violated these Standards may be subject to disconnection in the form of service unavailability for an unspecified time frame.

10. PATCH MANAGEMENT STANDARDS

(a) Patch management procedures should include the identification, categorization and prioritization of security patches and updates. An implementation timeframe for each category of security patches should be established to implement security patches in a timely manner.
(b) Perform rigorous testing of security patches and updates, where possible, before deployment into the production environment so as to ensure that the application of patches do not impact other systems.
(c) Strictly follow Change Management Process and document every change that will occur when the patch is applied. This helps identify devices that don't respond correctly to the patch or show an anomaly.
(d) Where feasible, with properly recorded justification, enable the automatic patching and update the features of operating systems and other software to help firms maintain the latest security controls.

11. SUPPLIER MANAGEMENT STANDARDS

(a) Establish a policy and procedures to address the information security risks for its outsourcing activities such as data center operations, network administration, disaster recovery site, application hosting and cloud computing services.
(b) Clearly define and communicate procedures for identifying, selecting and engaging a supplier including authorities responsible for granting approvals.
(c) The details of the supplier engaged and the corresponding SLA should be reported to the Board.
(d) Put in place controls to ensure the integrity of the information processing provided by the suppliers.
(e) Put in place recovery and contingency arrangements to ensure the availability of information processing by the suppliers within the required recovery time objective.
(f) Review the background of suppliers before being engaged. When evaluating the feasibility of outsourcing to a Cloud Service Provider (CSP), broker(s) shall keep in view the National, legal, regulatory & compliance risks, cost effectiveness and quality of services etc. Further, broker(s) shall carry out due-diligence of the prospective CSPs including their competence, business structure, experience, track record, financial strength, regulatory compliances with applicable laws, physical security/internal controls placed by the CSP.
(g) Execute a legally vetted Service Level Agreement [**SLA**] with supplier which may include the following terms:
    (i) an agreed set of controls of each party to be implemented including access control, performance review, monitoring, reporting and auditing;
    (ii) incident management & handling procedures including escalation and reporting procedures;
    (iii) Business continuity & back-up arrangements in case of any mishap/disaster causing service disruptions.
    (iii) suppliers' obligations to comply with the business security requirements.
(h) Avoid inclusion of lock-in clause or exclusivity arrangements in the SLA.
(i) Ensure that the Securities broker has right to terminate the SLA in the severe circumstances which may compromise the information security or its arrangements.
(j) Sign a statement of confidentiality and Non-Disclosure Agreement prior to execution of SLA.
(k) Monitor and review regularly the service performance levels of the supplier to verify adherence to the terms defined in the suppliers' agreements.
(l) Obtain prior approval of PSX before entering into Cloud arrangement.
(m) Core trading applications/services/operations and business processes used to process and store investor/trading data/information shall not be placed under cloud-based outsourcing arrangements.
(n) PSX may prescribe eligibility criteria for vendors of brokers' back office system or for any other purpose as deemed appropriate.

12. APPLICATION SECURITY STANDARDS

Encryption

Algorithm Requirements

(a) Encryption should be achieved using secure algorithms, such as AES, 3DES, RSA or comparable algorithm.
(b) Minimum cryptographic key length should be 128 bits.
(c) Self-signed Digital Certificates, if required, shall be created by applying recognized standards (e.g., X.509v3).

Key Management

(a) Encryption keys shall be unique and known to brokers authorized staff only.
(b) Keys stored in the system or configuration files shall be stored encrypted.
(c) Keys exchanged over communication lines / emails shall be sent in encrypted form.
(d) Encryption keys that are compromised should be revoked/replaced. Key re-assignments should require re-encryption of data.
(e) Where symmetric encryption is used, master keys should be changed at least once a year.

Note: *When asymmetric encryption is used, the operational period of asymmetric keys associated with a public key certificate are defined by the encryption key management plan of the issuing certificate authority.*

Data Preview, Export and Transfer Controls

(a) Application should follow best practices to maintain the confidentiality of data in preview, exports or transfer processes. Application shall not provide facility to preview, export or transfer unauthorized data e.g. in any case the data of other TREC Holders shall not be displayed or transferred using the application.
(b) Application should prompt a warning message while previewing, exporting or transferring the data. The warning should intimate the appropriate measures to be taken while transferring data. The process should remain visible to the authorized individual in the process.
(c) All kinds of application errors while previewing, exporting or transferring the data should be handled properly. The application should intimate with appropriate error message relevant to the issue. In case of an error the application should be able to resume the transmission of data from the point it was broken.
(d) When an Application transmitting sensitive data communicates over the Internet with the broker's system, it should be over a secure, encrypted channel to prevent Man-In-The-Middle (MITM) attacks, for instance, an IBTS or a Back office communicating from a customer's web browser or Desktop with the brokers' systems over the internet, or intra or inter organizational communications. Strong transport encryption mechanisms such as TLS (Transport Layer Security, also referred to as SSL) should be used.
(e) Applications carrying sensitive data that are served as web pages over the internet, a valid, properly configured TLS (SSL) certificate on the web server is mandatory, making the transport channel HTTP(S).
(f) Avoid using insecure protocols such as FTP (File Transfer Protocol) that can be easily compromised with MITM attacks. Instead, adopt secure protocols such as FTP(S), SSH and VPN tunnels, RDP (with TLS) etc.

Logging

(a) Application shall maintain log of every activity performed within the application.
(b) Successful and failed logins with user ID, date, timestamp, source & destination IP addresses, and other relevant elements shall be logged. Such logs should be maintained and stored in a secure location for a time period not less than two (2) years.
(c) Log shall contain sufficient details, for example, date & time, user ID, event ID, concise description of activity etc., to track an activity.

(d) Logging facilities and log information shall only be accessible as and when needed by authorized personnel.
(e) Logging system time shall be synchronized (e.g., via NTP service etc.) to maintain consistent timestamps.
(f) Log entries shall be created for user access provision, modification in user roles / profiles and user revocation by administrator.
(g) Application shall generate record in log file whenever user password is reset or account unlocked by administrator.
(h) Log data shall not record any sensitive information, including authentication or market sensitive data. Any encryption keys must also not be logged.
(i) Logging facilities and log information should be protected against, tampering/unauthorized changes to log information, including unauthorized log deletion.
(j) Application should also restrict administrator to modify, erase or de-activate logs of their own activities.
(k) Application shall store logs within database and maintain provision to make logs available as and when needed in structured human readable format.
(l) Review the logs to maintain accountability for the privileged users.

Input Handling

(a) The most common application security weakness is the failure to properly validate input entered by the user using application customer or automatically made by the system. This weakness is the cause of some major vulnerabilities in the applications, such as cross site scripting, SQL injection, interpreter injection, file system attacks, and buffer overflows.
(b) All input is validated to be correct and fit for the intended purpose.
(c) Server-side validation shall be used as a second line of defense, in addition to customer-side validation.
(d) Server-side input validation failures result in request rejection and are logged.
(e) Input validation routines are enforced on the server side.
(f) A single input validation control is used by the application for each type of data that is accepted.
(g) All SQL queries, HQL, OSQL, NOSQL and stored procedures, calling of stored procedures are protected by the use of prepared statements or query parameterization, and thus not susceptible to SQL injection.
(h) Application shall not be susceptible to LDAP, OS Command, Remote File Inclusion (RFI) injections, as applicable.
(i) Application is not susceptible to common XML attacks, such as XPath query tampering, XML External Entity attacks, and XML injection attacks.
(j) All string variables placed into HTML or other web customer code is either properly contextually encoded manually, or utilize templates that automatically encode contextually to ensure the application is not susceptible to reflected, stored and DOM Cross-Site Scripting (XSS) attacks.
(k) Application framework allows automatic mass parameter assignment (also called automatic variable binding) from the inbound request to a model, verify that security sensitive fields such as "UIN", "role" or "password" are protected from malicious automatic binding.
(l) Application has defenses against HTTP parameter pollution attacks, particularly if the application framework makes no distinction about the source of request parameters (GET, POST, cookies, headers, environment, etc.).
(m) All input data is validated, not only HTML form fields but all sources of input such as REST calls, query parameters, HTTP headers, cookies, batch files, RSS feeds, etc.; using positive validation (whitelisting), then lesser forms of validation such as grey listing (eliminating known bad strings), or rejecting bad inputs (blacklisting).
(n) Structured data is strongly typed and validated against a defined schema including allowed characters, length and pattern (e.g. credit card numbers or telephone, or validating that two related fields are reasonable, such as validating suburbs and zip or post codes match).
(o) Untrusted HTML from WYSIWYG editors or similar are properly sanitized with an HTML sanitizer and handled it appropriately according to the input validation task and encoding task.

(p) Verify that data transferred from one DOM context to another, uses safe JavaScript methods, such as using inner Text and val.

(q) That authenticated data is cleared from customer storage, such as browser DOM after session termination.

Web Application Security Controls

(a) Application security for customer facing applications offered over the Internet such as IBTS (Internet Based Trading applications), portals containing sensitive or private information and Back office applications (repository of financial and personal information offered by brokers to customers) are paramount as they carry significant attack surfaces by virtue of being available publicly over the Internet for mass use.

(b) Web Security Controls establish a baseline of security requirements for all TREC Holders' web services / websites, especially the ones that facilitate trading and related activities. The application should have protection against common threats, such as,

(i) **Injection flaws** – SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

(ii) **Broken Authentication & Session Management** – Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities.

(iii) **Cross-Site Scripting (XSS)** – XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

(iv) **Insecure Direct Object References** – A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.

(v) **Security Misconfiguration** – Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. Secure settings should be defined, implemented, and maintained, as defaults are often insecure. Additionally, software should be kept up to date.

(vi) **Sensitive Data Exposure** – Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data deserves extra protection such as encryption at rest or in transit, as well as special precautions when exchanged with the browser.

(vii) **Missing Function Level Access Control** – Most web applications verify function level access rights before making that functionality visible in the UI. However, applications need to perform the same access control checks on the server when each function is accessed. If requests are not verified, attackers will be able to forge requests in order to access functionality without proper authorization.

(viii) **Cross Site Request Forgery** – A CSRF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim's browser to generate requests the vulnerable application thinks are legitimate requests from the victim.

(ix) **Using Components with Known Vulnerabilities** – Components, such as libraries, frameworks, and other software modules, almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications using components with known vulnerabilities may undermine application defenses and enable a range of possible attacks and impacts.

(x) **Invalidated Redirects & Forwards** – Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages.

13. TESTING & CERTIFICATION STANDARDS

The vulnerability assessment and source code review of applications which store or process market sensitive data shall be completed independently at least once in every two years or whenever there is major change in application/system. The critical and high-risk observations identified as a result of the testing must be rectified at the earliest but not later than 2 weeks of identification.

The assessment carried out by the software vendor through an approved vulnerability assessment and source code review vendor shall be considered acceptable as long as brokers and/or software vendor are able to demonstrate that the same software which was assessed is being used by the concerned brokers.

14. INCIDENT MANAGEMENT STANDARDS

(a) Establish written policies and procedures specifying the manner in which a suspected or actual information security incident should be reported internally to the Board and Senior Management and externally to PSX and to the customers also if deemed appropriate.
(b) Ensure that all its employees and contractors are made aware of their responsibility to report any information security events.
(c) Maintain logs of all incidents at a central place accessible to authorized personnel only.
(d) Investigate alerts generated from monitoring and detection systems in order to determine activities that are to be performed to prevent expansion of such incident of cyber-attack or breach, mitigate its effect and eradicate the incident.
(e) The incident log must include:
    (I) The time of the incident logged;
    (ii) Description and nature of the incident;
    (iii) How the incident was identified;
    (iv) who reported the incident (i.e. name / department / designation);
    (v) the extent of the incident and its implications on other components of the system;
    (vi) the priority of the incident and details of diagnostic or attempted recovery actions taken.
(f) Report to PSX all security incidents and breaches as soon as possible. The report must include summary analysis of the incident and causes along with the steps taken to resolve the same.
(g) Ensure that log and data of identified and reported incident must be preserved for a period of 03 years or as may be prescribed by PSX from time to time.
(h) Analyze any incident of loss or destruction of data or systems and lessons learnt from such incident should be incorporated to strengthen the security mechanism and improve recovery planning and processes.

15. BUSINESS CONTINUITY PLAN (BCP) AND DISASTER RECOVERY (DR) STANDARDS

(a) Ensure compliance with the requirements of clause 4.27 and 8.3.2 of PSX Regulations in such manner as specified by PSX from time to time.
(b) Have in place BCP and DR so as to maintain data and transaction integrity.
(c) A BCP and DR should be undertaken with business impact analysis/ assessment to ensure that all key business activities, business support systems and operational functions are identified.
(d) A BCP and DR must clearly identify and document computing resources and office facilities needed to support critical business functions.

(e) Any services provided by third parties and their responsibilities must be formally defined and documented in a Supplier Agreement.
(f) Conduct/perform periodic drills to validate business continuity plan's effectiveness.
(g) Employees must be trained in the implementation of BCP/DR procedures. Backup personnel must also be identified and trained.
(h) A BCP and DR must be kept up-to-date and reviewed once a year and signed off by the management.
(i) Integrate the disaster recovery plan with the business continuity plan.

16. INFORMATION SECURITY POSTURE REVIEW & ASSESSMENT STANDARDS

(a) All systems must undergo an independent security review, technical security reviews i.e. Vulnerability Assessment and Penetration Testing and as determined by events (e.g. vulnerability notifications and security incident), system changes, and changes to the system sensitivity levels at least once in every two years.
(b) Ensure that the interconnected systems have commensurate levels of security. Brokers also need to review the design and architecture of such engagement to ensure technical feasibility and authorize the same.
(c) Apply security controls to their respective domains and ensure that the controls are properly integrated.

17. COMPLIANCE AND AUDIT STANDARDS

(a) All brokers are required to comply with the information security standards prescribed by PSX under Clause 4.25 and Chapter 9 of PSX Regulations and these Standards.
(b) The brokers providing IBTS shall ensure that their systems, controls and procedures are audited, vulnerability and penetration tested independently, once in every two years, by an audit firm.
(c) Submit an audit report to PSX within two months of the date of the close of its periodic vulnerability assessment along with a certificate of the auditor for appropriateness of necessary controls and safeguards put in place in relation to information security arrangements in relation to IBTS.
(d) Broker shall be liable to rectify the deficiencies or issues identified during the process of audit and furnish a compliance report to PSX from the auditor, within 30 days from the date of submission of IBTS audit report, certifying that the noncompliance(s)/vulnerability has been rectified/removed.
(e) IBTS systems may require periodic technical security reviews and pen-test as determined by events (e.g. vulnerability notifications and security incident), changes in system or system sensitivity levels.
(f) PSX may conduct verification, review or inspection of brokers to ensure their compliance with the requirements of clause 4.25.1in such manner as specified by PSX from time to time.
(g) PSX require broker(s) to submit audit report on compliance with the requirements of clause 4.25.1 within such time and in such manner as specified by PSX.

18. ANNEXURES

A. SoA Template

Section	Information Security Standard	Applicable (Yes /No)	Rational

B. Asset Inventory Template

Unit & Process Information			Information Asset Details									
Operating Unit / Function	Process name	Process owner	Name of Asset	Description of Asset	Type of Information Asset [Hard copy, Electronic File (specify type), removable media/ device (specify type)]	Personal Data (Y/N)	Personal Sensitive Data (Y/N)	Sensitive Customer Data (Y/N)	Classification	Integrity	Availability	Data Retention Period

C. Cyber/Information Security Incident Reporting Format

Sr. No.	Date of security breach discovery	Source of security breach discovery	Nature of security breach	Reasons for the occurrence of security breach (e.g. Breach of controls, Procedures were not followed, weaknesses in implemented security controls etc.)	Impact of security breach (e.g. on Securities Broker business, systems, customers, investor, market, finances etc.)	Action(s) taken to rectify the Security Breach	Remarks (further details, if any)

19. GLOSSARY

Sensitive Data	Trading data, Personable Identifiable Information (PII), or any other data whose disclosure may affect confidence of the customer on the capital market.
Access Control	A means of restricting access to files, referenced functions, URLs, and data based on the identity of users and/or groups to which they belong.
Application Security	Application-level security focuses on the analysis of components that comprise the application layer of the Open Systems Interconnection Reference Model (OSI Model), rather than focusing on for example the underlying operating system or connected networks.
Authentication	The verification of the claimed identity of an application user.
Blacklist	A list of data or operations that are not permitted, for example a list of characters that are not allowed as input.
Certificate Authority (CA)	An entity that issues digital certificates.
Communication Security	The protection of application data when it is transmitted between application components, between customers and servers, and between external systems and the application.
Component	A self-contained unit of code, with associated disk and network interfaces that communicates with other components.
Cross-Site Scripting (XSS)	A security vulnerability typically found in web applications allowing the injection of customer-side scripts into content.
Cryptographic module	Hardware, software, and/or firmware that implements cryptographic algorithms and/or generates cryptographic keys.
Design Verification	The technical assessment of the security architecture of an application.
Hypertext Mark-up Language (HTML)	The main mark-up language for the creation of web pages and other information displayed in a web browser.
Hyper Text Transfer Protocol (HTTP)	An application protocol for distributed, collaborative, hypermedia information systems. It is the foundation of data communication for the World Wide Web.
Input Validation	The canonicalization and validation of untrusted user input.
IBTS	"Internet Based Trading Services or IBTS" shall mean services associated with internet based trading for the purpose of routing orders to trading systems of the Exchange through an automated order routing system as provided for under these Regulations;
Malware	Executable code that is introduced into an application during runtime without the knowledge of the application user or administrator.
RDA	Roshan Digital Account application
Regulatory Affairs Committee (RAC)	means a committee constituted by the Board with prior approval of the Commission pursuant to Licensing Regulations.
Security Control	A function or component that performs a security check (e.g. an access control check) or when called results in a security effect (e.g. generating an audit record).
SoA	Statement of Applicability
SQL Injection (SQL)	A code injection technique used to attack data driven applications, in which malicious SQL statements are inserted into an entry point.

URI/URL/URL fragments	A Uniform Resource Identifier is a string of characters used to identify a name or a web resource. A Uniform Resource Locator is often used as a reference to a resource.
XML	A mark-up language that defines a set of rules for encoding documents.
User Acceptance Testing (UAT)	Traditionally a test environment that behaves like the production environment where all software testing is performed before going live.
TRE Certificate Holder	means any person who is issued a TRE Certificate by the Exchange upon Corporatization under Section 5 of the Act, or purchases or acquires such TRE Certificate under section 16 of the or is issued a fresh TRE Certificate in accordance with the provisions of the Act.