PAKISTAN STOCK EXCHANGE LIMITED
Stock Exchange Building, Stock Exchange Road, Karachi-74000
Phone: 111-001-122 Fax: **32437560**

PSX/N – 488 **NOTICE** **January 26, 2017**

FOR ALL TRE CERTIFCTAE HOLDERS AND BACK OFFICE SOFTWARE VENDORS

Standardization of Back Office System, IT & Information Security Requirements and Back Office Software Vendor Eligibility Criteria

Attention of all TRE Certificate Holders and Back Office Software Vendors is drawn to Clause 4.26 of the PSX Regulations which is reproduced hereunder:

QUOTE

"4.26. IT AND INFORMATION SECURITY REQUIREMENTS FOR THE SELECTION OF SOFTWARE VENDORS AND USAGE OF SOFTWARE BY THE TRE CERTIFICATE HOLDERS:

4.26.1. 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) Submit to the Exchange an audit report/certificate of the auditor for appropriateness of necessary controls and safeguards put in place in relation to information security arrangements.

(d) 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.

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

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

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

UNQUOTE

As required under the above Clause, PSX has developed Guidelines and Standards on Back Office System of the TRE Certificate Holders which also contain Software Vendor Eligibility Criteria enclosed herewith as **Annexure A.** Further, PSX has developed Application Security Standards, Specifications & Requirements, which are enclosed herewith as **Annexure B.**

All TRE Certificate Holders are advised to read and understand the requirements of these specifications and standards and put in place necessary arrangements to ensure compliance with these requirements in letter and spirit. The TRE Certificate Holders are further advised to ensure that they procure Back Office Software only from the vendors, which meet the Software Vendor Eligibility Criteria set out in the aforesaid document.

NOTE: In compliance with the requirement of the above clause, the PSX shall soon make available the list of eligible Software Vendor on its website, which shall be intimated to the market participants through a separate notice.

The above must be noted for your information, record and compliance purposes.

SHAFQAT ALI
Chief Regulatory Officer

Encl: The above-mentioned **Annexures A & B** are available on PSX website.

Distribution: TREC Holders of PSX based at Karachi through Karachi Office
TREC Holders of PSX based at Lahore through Lahore Office
TREC Holders of PSX based at Islamabad through Islamabad Office

Cc:

1. The Director/HOD (SSED/SMD), SECP
2. The Executive Director (PRDD/SMD), SECP
3. The Managing Director, PSX
4. The Chief Executive Officer, CDC
5. The Chief Executive Officer, NCCPL
6. The Chief Executive Officer, PMEX
7. All Heads of Departments, PSX
8. All TRE Certificate Holders of PSX
9. Notice Board & Website of PSX

Annexure-A

PAKISTAN
STOCK EXCHANGE
LIMITED

GUIDELINES AND STANDARDS ON BROKER BACK OFFICE (BBO) FOR PAKISTAN STOCK EXCHANGE

DOCUMENT SIGN-OFF

The following persons have approved this document:

Name	Designation	Approval Date	Signature
Sani Khan	General Manager (PDRM)		

REVISION HISTORY

Revision	Date	Doc Version	Author
	Comment		
	06/06/2016	1.1	Naveed Akbar Raja
	Initial Draft for the concept paper submitted for the review.		
	28/06/2016	1.2	Naveed Akbar Raja
	Amendments proposed after various discussions with stake holders		
	30/06/2016	1.3	Naveed Akbar Raja
	Incorporate the comments provided by PSX IT and templates of reports		
	24/10/2016	1.4	Naveed Akbar Raja
	Addition of vendor eligibility criteria		

RELATED DOCUMENTS

Please refer to the following documents for additional information related to this project:

Document Title	File Name

TABLE OF CONTENTS

1.1 TITLE

Guidelines on **Broker Back Office (BBO)** for Pakistan Stock Exchange Trading Participants i.e. TREC Holders

1.2 APPLICATION

These guidelines apply to all Trading Participants “TREC” holder of Pakistan Stock Exchange.

1.3 DEFINITIONS

The terms used in these guidelines shall be taken to have the meaning as assigned to them in the glossary.

1.4 STATEMENT OF POLICY

1.4.1 PURPOSE

These guidelines outline the minimum Broker Back Office requirements that Trading Participants will need to ensure comprehensiveness/ adequacy of their broker back office system in providing services to their clients as they mitigate the associated risks.

1.4.2 SCOPE

These guidelines set the minimum requirements for a Broker Back Office System for existing and new Trading Participants.

1.4.3 RESPONSIBILITY

The responsibility for Broker Back Office ultimately rests with the board of directors and the Senior Management of the Trading Participant. The Trading Participants have to be able to show that they are guided by these guidelines and the standards.

1.4 SOFTWARE VENDOR ELIGIBLITY CRITERIA

In order to ensure that the Back Office application development is performed to an acceptable standard and by a qualified vendor, it is necessary to assess all prospective vendors before they can be selected as “eligible vendor”. The pre-qualification process uses a pre-established set of requirements against which prospective vendors are evaluated prior to being approved and listed on Exchange website.

A. Vendor must be a registered company of Pakistan/International Origin OR their authorized business partner with registered office in Karachi, Pakistan.

B. Vendor must have at least 5 Years of experience in application development and support. Please note that capital markets experience is not mandatory.

C. The Company should be profit making for atleast last three years.

D. Vendor should have sufficient pool of qualified and skilled technical resources. Exchange will assess the interested vendors and maintain a list of qualified vendors on its website.

1.5 SPECIFIC REQUIREMENTS

1.5.1 CLIENT MANAGEMENT

1 The system (Broker Back Office) should have all the necessary fields for static data that are required for identification and future processing. It must comply with Know Your Customer (KYC) principles and standards.

2 Amendment of client details should be controlled and the system must be able to support this process.

3 The system should have the capability to set up the different service charge type for different clients. These should be parameterized fields for interest rate and any other client related charges.

4 The system should have the ability to enquire and view account statements on line through a secure connection.

5 The system should have the ability to create and maintain additional fields in the future. These may be fields that are required for future financial reporting or data analysis.

6 The system should have other functionalities that will improve the management of client information so as to facilitate a secure and efficient market.

7 The system should have the capability to receive funds from multiple sources. In the case of cheques, the value should indicate after a configurable cheque clearing timeframe.

8 The system should allow for various clients' sales settlement mode i.e. direct credit to appointed bank a/c, cheques, or current account. There should be EOD reconciliation between the brokers and the Bank account.

1.6 ORDER MANAGEMENT

1 The system should provide the capability for the broker to register trade a vast array of financial instruments in real-time. These include equities and debt instruments or any other securities such as derivatives, options or ETFs.

2 The system should have a single order entry process from the order taking desk, trade matching and client account update without any manual intervention.

3 Orders captured into the system should automatically affect the total client's position in the client's account.

4 The system should have the ability to perform automatic reconciliation of trades executed by KATS against order capture.

5 The system should have inbuilt authorization procedures for orders whose account balances are insufficient.

6 The system should have the ability to connect to multiple trading systems by the use of the FIX protocol and additionally provide for Direct Market Access.

7 The system should have the ability process in Real-time transactions and provide straight-through-processing, end-to-end, from trade to settlement.

8 The system should have provision for risk managers of the firm to exercise emergency powers, with suitable internal approval mechanisms — to disable some users, some clients, remove some orders etc. depending on the market situation.

9 The system should allow agents to manage transactions of their clients through a direct, but limited access to the system. Views restricted to only those clients under that agent and transactions restricted to only those allowed for agents.

10 The system should allow for configurable computation of brokerage commission and/or rebate and generate contract once the order confirmation info is received.

11 The system should have the capability to automatically update contract information to client's ledger and allow viewing of the same on-line.

12 The system should allow for manual key-in of contract details and amendment of selected contract details. An auto generated amendment/cancellation Letter will then be printed/emailed to show the reason of the amendment/cancellation.

1.7 CDC RELATED FUNCTIONS

1 The system should allow brokers to send/receive share transfer messages to/from CDC and update client's details and accounts accordingly.

2 The system should allow broker to mark pledged securities and update client's account.

3 The system should have the ability of handling different settlement periods for different markets (e.g. T+0, T+1, T+2...).

4 The system should have the capability to define and recognize trading and settlement time and days for different markets.

1.8 DEALING FUNCTIONS

1 The system should support for dealing on the broker's own account in compliance with regulations for dealing.

2 The system should support for real-time portfolio valuation through price-feed and automatic trigger of stop-loss alerts.

3 The system should provide the capability to apply Chinese wall between dealing and stock broking.

1.9 ACCOUNTING FUNCTIONS

1 The system should have a complete accounting module that allows GL interfacing with other existing accounting applications a firm may have.

2 The system should allow for sub ledgers for clients to be user defined and should then be linked to control accounts. All common accounting functionalities should be possible to be carried out using this module.

3 The system should have the capability to receive bank's notice on failed settlement i.e. returned cheque or insufficient Cash balance.

4 The system should be able to enable credit control section to reverse the receipt (auto journal) and update client ledger on real time basis.

1.10 IPO FUNCTIONS

1 The system should provide an automated process for managing broker related IPO activities.

2 The system should have the capability to download IPO returns from receiving banks and registrars to perform auto reconciliation i.e. the auto matching of payments and applications.

3 The system should have the capability to process refunds and be able to perform auto reconciliation with the bank accounts.

1.11 RISK, SURVEILLANCE AND COMPLIANCE REQUIREMENTS

1 The system should have an inbuilt Support for stronger KYC, and scanning of all important identification documents.

2 The system should be able to validate all buy orders against cash available and any trading limits granted, and to validate all sell orders against security available at CDC including employee trading.

3 The system should have the capability to classify clients depending on their standing- Good standing, doubtful debt, bad debt etc. and to grant graded privileges for these accounts.

4 The system should minimize frauds through high security environment with maker-checker, approvals, audit trails and Role based permissions. This include notifying clients of major transactions in their accounts and making brokerage accounts transparent to clients — they can view their accounts, orders and holdings at any time over the internet.

1.12 REPORTS

The system must provide the following reports besides the standard inbuilt reports.

1. Net Capital Balance Report
2. Client Registration Corporate Report
3. Client Funds Receipts Report
4. Client Fund Deposits into Banks Report
5. Payments to Client Report
6. Bank Interest on Clients Accounts report
7. Un-posted Trade Book Report

8. Client Ledgers – Ready & Futures Report
9. Client Ledgers – Leveraged Report
10. Client Securities Report
11. Pre Settlement Delivery Report
12. Pledging of Client Securities report
13. Client Aging Report
14. Client wise CDC/Back Office Matching Report
15. Risk Management Report
16. Broker's Proprietary Trades/Investments Report
17. Complaint Handling Report
18. List of Agents Report
19. Commission Report
20. Loan Schedule Report

The formats of the aforesaid reports are attached as Annexure.
Further, the TREC Holders would be required to maintain following details, as part of their back office record

1. Fixed Asset Register Report
2. Accounting Ledger Report
3. Client Trial Balance Report
4. Accounting Trial Balance Report
5. Income Statement Report
6. Balance Sheet

1.13 USER MANAGEMENT AND WORKFLOWS

The system should provide for the following;

a) Support for maker-checker for key entry into the system.
b) Flexible approval workflow process with escalation support.
c) Hierarchical role based access permission for various functionalities of the system.
d) Ability to flag sensitive transactions and to highlight such transactions.
e) Complete audit trail of all input, changes and deletes.
f) Ability to automatically raise alerts on exceptional events.
g) Ability to raise alerts for pre-defined events on appropriate dates

1.14 TECHNICAL REQUIREMENTS

REQUIREMENT SPECIFICATIONS

1.14.1 GENERAL

1 User -friendly front-end interface that is customizable with mostly drop down menus.
2 Interfacing capabilities with industry standard interfaces — API's and FIX
3 Centralized repository for distributing each broker's database. This is to minimize inconsistencies across front and back-office operations. This database shall be kept secure and access shall be restricted to authorized personnel only.
4 Graphical user interface suitable for the various business users to perform analysis
5 Web client interface
6 Three tier architecture (presentation tier controlling what users see, application tier where business rules reside and data tier containing customer, product and business data).
7 Technical controls shall be in place to:
   - Restrict Presentation of incorrect Data, intentionally or malevolently
   - Restrict use of incomplete information for transactions
   - Restrict manipulation of any data
   - Restrict Multi-logins into the application
   - Lock out system in case of bad login attempts

8 The application should provide capability to enforce password control including complexity, expiration, account lockout and re-use time.
9 Users shall be authenticated to application using a minimum of user ID and password combination. Where strong authentication and identity verification is required, authentication methods alternative to or complementing passwords, such as tokens (hard or soft), cryptography (symmetric or asymmetric encryption) or biometric should be used.
10 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.
11 System should provide the disaster recover site capabilities.
12 System should provide mechanism for updating disaster recovery site in reasonable real-time mode
13 System must maintain the audit trail of all control functions performed by the user of the System
14 Documentation, SOPs, Guidelines, User Manual shall be developed and shall be made available in the system
15 A proper Technical Support Section shall be developed with enough number of trained and skilled personnel to facilitate and support the end users.
16 The system shall implement Data Preview, Export and Transfer Controls. This includes:
   - The application should not provide facility to preview, export or transfer unauthorized data e.g. in any case the data of other members should not be displayed or transferred using the application.
   - The practices pertaining to due diligence and due care should be followed while previewing, exporting or transferring data before transferring between applications.

- 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.
- The application should require approval or maker/checker control for initiating data preview, export or transfer.
- The application should follow best practices to maintain the confidentiality of data in preview, exports or transfer processes.
- The 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 data should remain visible to the authorized individual in the process.
- The transfer of data between applications should comply the contractual and legal requirements.

17 System shall incorporate the following high level requirements:

- All input is validated to be correct and fit for the intended purpose.
- Data from an external entity or client should never be trusted and should be handled accordingly.

18 The following controls are sufficiently in place within the application:

- The runtime environment is not susceptible to buffer overflows, or that security controls prevent buffer overflows.
- Server side input validation failures result in request rejection and are logged.
- Input validation routines are enforced on the server side.
- A single input validation control is used by the application for each type of data that is accepted.
- 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.
- Application is not susceptible to LDAP Injection, or that security controls prevent LDAP Injection.
- Application is not susceptible to OS Command Injection, or that security controls prevent OS Command Injection.
- Application is not susceptible to Remote File Inclusion (RFI) or Local File Inclusion (LFI) when content is used that is a path to a file.
- Application is not susceptible to common XML attacks, such as XPath query tampering, XML External Entity attacks, and XML injection attacks.
- All string variables placed into HTML or other web client 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.
- 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 “Account Balance ”, “role ” or “password ” are protected from malicious automatic binding.
- 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.).
- Client side validation is used as a second line of defense, in addition to server side validation.
- 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).
- Unstructured data is sanitized to enforce generic safety measures such as allowed characters and length, and characters potentially harmful in given context should be escaped (e.g. natural names with Unicode or apostrophes, such as ねこ or O'Conner).

- Verify that data transferred from one DOM context to another, uses safe JavaScript methods, such as using .innerText and .val.
- That authenticated data is cleared from client storage, such as the browser DOM, after the session is terminated.

1.14.2 SECURITY & ADMINISTRATION

The Security & Administrative manual for Broker Back Office System is attached as Annexure.

1.14.3 INTEGRATION

1. Allow Integration of Microsoft Outlook (or any other mailing tool) for emails and attachments.
2. Integrate to internal and external systems using pre-built interfaces and standard XML/SOAP web services APIs, ISO, XML and FIX.
3. Documented web services based API for completing custom integration with other applications.

1.14.4 DATA MIGRATION

1. Enhanced data synchronization (online/offline) for full access to sales and customer service information.
2. Seamless data migration routines --using easy to use online wizards
3. Test validation process (3rd party, documentation, test results) & ability to define data validation.

1.14.5 INFRASTRUCTURE

1. Robust and standard Hardware, Network, Operating System and Database Management System shall be used for hosting the application.
2. Light bandwidth consumption and maximum users load.
3. Scalable database for optimal performance and growth.
4. Ability to support concurrency processing.
5. Easy administration of the system.

1.15.6 OTHER FEATURES

1. Support for good integration speed and performance.
2. Capable of switching to other servers/systems when the primary/running server/system fails.
3. Well and documented Backup/Restore Policy

Annexure A: Formats of the Reports

1. Net Capital Balance Report

The format of the report is illustrated below:

Net Capital Balance
Particulars
Current Assets
Cash In Hand or In Bank
Cash In Hand
Bank Balances
Trade Receivables
Book Value
Less: Overdue for more than 14 days
Investment In Listed Securities In the name of Broker
Securities on the exposure list marked to market
Less: 15% Discount
Securities held for client
Total Current Assets
Current Liabilities
Trade Payable
Book Value
Less: Overdue For More Than 30 Days
Other Liabilities
Total Current Liabilities
Net Capital Balance

2. Client Registration Individual/Corporate Report

The format of the report is illustrated below:

Client Registration

Individual												
Client Code	Name	S/0, D/O, W/O	NIC No.	Current Address	Mailing Address	Email	Cell No.	Landline Phone No.	Details of occupation	Source of income	Average Trading limit	Risk profile - i.e. Political exposed person, off shore etc.

Corporate													
Client Code	Name	Incorporation No.	Incorporation Date	Country of Incorporation	Contact Person	Status of contact person in the client	Email	Cell No.	Landline Phone No.	Details of occupation	Source of income	Average Trading limit	Risk profile - i.e. Political exposed person, off shore etc.

3. Client Funds Receipts Report

The format of the report is illustrated below:

Client Funds Receipts

							In case of cash following	
System Generated Receipt No (Primary Key)	Client Name	Client Code	Date of receiving	Slip No. / other Ref No.	Mode of receipts	Amount	Name of Person depositing	Date of reporting to NCHS

4. Client Funds Deposits into Banks Report

The format of the report is illustrated below:

Client Fund Deposits into banks

Bank Name	Account No.	System generated Primary Key	Client Name	Client Code	Date of Deposit	Amount

5. Payments to Client Report

The format of the report is illustrated below:

Payments to Client

							Payment to others on instruction of client		
Client Name	Client Code	Date of Payment	Cheque No.	Bank and Account No.	Amount	Mode of delivery	Details of evidence	Signatures verified	Details of Payee

6. Bank Interest on Clients' Bank Accounts Report

The format of the report is illustrated below:

Interest on Clients Bank Accounts

Date of accrual	Rate	Amount	Client code getting credits	Management Fee charged	Rate

7. Un-posted Trades Book Report

The format of the report is illustrated below:

Un-posted Trades Book

Voucher Type	Market Type	Trade Date	Settlement Date	Order No.	Ticket No	Bill No	Bill Date	Scrip	Qty	Price	Commission	Taxes/duties/levies

8. Client Ledgers- Ready & Futures Report

The format of the report is illustrated below:

Trade Related - Ready and Futures														
Voucher Type	Market Type	Trade Date	Settlement Date	Ticket No.	Bill No.	Bill Date	Scrip	Qty	Price	Commission	Taxes/duties /levies	Payment - Primary Key Number	Receipt - Primary Key Number	Balance outstanding Dr/Cr

9. Client Ledgers- Leveraged Report

The format of the report is illustrated below:

Trade Related - Leveraged													
Voucher Type	Market Type	Trade Type - Marked/Released	Trade Date	Settlement Date	Ticket No	Bill Number	Bill Date	Scrip	Qty	Price	Commission	Taxes/duties/levies	Interest charged

10. Client Securities Report

The format of the report is illustrated below:

Client Securities										
Symbol	**Scrip**	**Position owned**	**Available**	**Transferred under Pre Settlement Delivery**	**Pledged**	**Freezed**	**Blocked**	**Pending in**	**Pending out**	**Market Value**

11. Pre-Settlement Delivery Report

The format of the report is illustrated below:

Pre Settlement Delivery Report						
Date of Marking	**Market Type**	**Trade Date**	**Settlement Date**	**Client Code**	**Symbol**	**Qty**

12. Pledging of Client Securities Report

The format of the report is illustrated below:

Pledging of Client Securities							
Primary Key - Pledge transaction	**Date Marked**	**Date Released**	**Symbol**	**Qty**	**Pledgee**	**Pledgor**	**Purpose**

13. Client Aging Report

The format of the report is illustrated below:

Clients Aging					
Client Code	**Client Name**	**Balance Outstanding**	**Aged for 14 days**	**Aged for 30 days**	**Market Value of Securities held in back office**

14. Client Wise CDC/Back Office Matching Report

The format of the report is illustrated below:

CDC/Back Office Matching Report					
Client Code	**Name**	**Symbol**	**Balance as per BO**	**Balance as per CDC**	**Difference**

15. Risk Management Report

The format of the report is illustrated below:

Risk Management														
Client Code	Client Name	Balance of ledger	Balance of Un-posted Trade Balance	Securities	Qty	Market Rate	Value	Haircut	Accepted Value	Securities Transferred Under PSD	Value of open position in leveraged/ Future markets	Margin Allowed	Margin Utilized	Margin Remaining

16. Broker’s Proprietary Trades/Investments Report

The format of the report is illustrated below:

Broker's Propriety Trades/investments		Trade Related - All								
Voucher Type	Market Type	Trade Date	Settlement Date	Ticket No	Scrip	Qty	Price	Taxes/duties/levies	Symbol Wise Avg. Cost Till date	Market Value

Trade Related - Leveraged										
Voucher Type	Market Type	Trade Type - Marked/Released	Trade Date	Settlement Date	Ticket No	Scrip	Qty	Price	Taxes/duties/levies	Interest charged

17. Complaint Handling Report

The format of the report is illustrated below:

Complaint handling Database							
Sr. No	Date	Name	Nature	Steps taken to Resolve	Current Status	Date of Resolution	Description of Resolution

18. List of Agents Report

The format of the report is illustrated below:

List of Agents							
Name of Agent	UIN	Date of obtaining Agent Status	Location of Branch Office	Qualification	Experience	Amount of Security Deposit	Date of quieting the Agent Ship

19. Commission Report

The format of the report is illustrated below:

Commission Report								
				Introducer				
Date	Name of Client	Type (Slab)	Description	Name	Relationship	Commission Gross	Commission Shared with Introducer	Commission Net
						Rs.		

20. Loan Report

The format of the report is illustrated below:

Broker Name						
Corporate Member Pakistan Stock Exchange Limited						
(Address) (Ph#)						
(Details of Loan) (Date _______)						
Sr. No	Name of Bank	Account No	Branch	Bank Code (Back Office)	Financing Facility	Mark-up Charged
					Rs	% age

Annexure-B

Application Security Standards, Specifications and Requirements

Information Security Office (ISO)
Pakistan Stock Exchange Limited

Version 0.5

EFFECTIVE DATE:

Public
This document and the information it contains shall be made available to the public as well as to the Pakistan Stock Exchange (PSX) Brokers for their understanding and compliance, where applicable. PSX reserves the right to amend or repeal a part or complete document, with the permission of the regulatory authority.

History of Changes

This section records the history of significant changes to this document.

Version	Date	Author / Owner	Reviewer	Approver	Description of change
0.1	29/01/2016	Mr. Arif Rehman (CISO)	--	--	Initial version
0.2	12/04/2016	Mr. Arif Rehman (CISO)	Mr. Shafqat Ali Khan (CRO)	--	PSX RAD Review
0.3	19/04/2016	Mr. Arif Rehman (CISO)	Mr. Iftikhar Ahmed (CIO)	--	PSX IT Review
0.4	09/09/2016	Mr. Arif Rehman (CISO)	TREC Holders Review	--	TREC Holders Review & Feedback sought via Notice PSX/N-5049
0.5	30/09/2016	Mr. Arif Rehman (CISO)	--	Mr. Nadeem Naqvi (MD) Mr. Shafqat Ali Khan (CRO) Mr. Haroon Askari (DMD) Mr. Iftikhar Ahmed (CIO)	Specifications approval ISO-201608-009 - Application Security
0.6	TBC	Mr. Arif Rehman (CISO)	PSX IT & Information Security Steering Committee	--	
1.0	TBC	Mr. Arif Rehman (CISO)	--	PSX BOD	

Where significant changes are made to this document, the version number is incremented by 1.0.

Where changes are made for clarity and reading ease only and no change is made to the meaning or intention of this document, the version number is increased by 0.1.

TABLE OF CONTENTS

1 INTRODUCTION

The advancement of technology has helped to drive organizations to unprecedented levels of growth and reach. However, this advancement has also resulted in a large increase in new threats to the confidentiality, integrity and availability of the organizations' information.

The situation for the Brokerage Houses associated with Pakistan Stock Exchange (PSX) is no different, as over time, since the introduction of Karachi Automated Trading System (KATS) in 2002, the majority of Brokerage Houses operations began to be supported by and heavily reliant on technology in one form or another.

These changes, including the proliferation of access points/mechanisms and the consolidation of information repositories, have resulted in Brokerage Houses facing increasingly complex challenges in maintaining the confidentiality, integrity and availability of its information, which is critical for the on-going effective functioning and good governance of the capital market.

In addition to the inherent complexity of the capital market, the nature and pace of the change necessitates that critical requirements pertaining to application security and risk management are not overlooked.

It is therefore imperative that PSX have a coherent strategy for achieving the above mentioned objectives. In-line with these requirements, these application security standards, specifications, and requirements have been developed to provide for consistent application of security principles throughout the capital market and to serve as a definitive reference guide when matters of security arise.

2 PURPOSE

The purpose of this document is to provide necessary guidance to the Brokerage Houses in order to ensure that the order management system, front office system, back office system and the ancillary software used by Brokers which directly or indirectly supports trading or related activities meet the minimum standards and requirements prescribed by the frontline regulator.

These requirements would assist in protecting the confidentiality of data, uniformity in the manner of maintenance of records and facilitate inspection of Brokers by ensuring availability of necessary records in a timely and transparent manner.

Further, the vendor providing the related software to the Brokers will also be subject to suitable criteria thereby ensuring the quality of the software and create accountability.

3 SCOPE

The document prescribes application security standards, specifications, benchmarks, confidentiality and control standards to be met by the application or software, regular testing and certification requirements, as well as eligibility criteria for the vendor who may provide application or software to Brokers of the Pakistan Stock Exchange (PSX), and matters considered necessary thereto.

The document is intended for PSX Brokerage Houses and the personnel responsible for developing and supporting applications.

The section 4.26 of PSX Rule Book (regulations) states that;

4.26. IT AND INFORMATION SECURITY REQUIREMENTS FOR THE SELECTION OF SOFTWARE VENDORS AND USAGE OF SOFTWARE BY THE TRE CERTIFICATE HOLDERS:

4.26.1. 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) Submit to the Exchange an audit report/certificate of the auditor for appropriateness of necessary controls and safeguards put in place in relation to information security arrangements.

d) 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.

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

f) Ensure that only Exchange certified ancillary software are installed on the trading terminals.

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

4 REVIEW

This document shall be reviewed on need basis by the PSX's Information Security Office, and updates made to keep it in accord with capital market's overall strategy and risk appetite. Any material changes to the document shall be incorporated as per the established process.

5 RESPONSIBILITY

Responsibilities for effective implementation of the application security standards, specifications, and requirements rests with multiple stakeholders of the Capital Market. Additional responsibilities for specific stakeholders of the capital market include;

- Securities and Exchange Commission of Pakistan (SECP) is responsible for reviewing, approving, enforcing, and empowering Exchange to assure the compliance of these standards and requirements both on and off premises of the Brokerage Houses.
- The Exchange is responsible for the development, updatation, and dissemination of these standards and requirements to all concerned stakeholders. The Exchange is also responsible for socialisation, education, and awareness of stakeholders concerning these standards, specifications, requirements, and assuring its compliance through regular system audits.
- The Brokerage Houses shall ensure the compliance with these standards, specifications, and requirements at all times as well as extending full support and cooperation with the Exchange staff in the assurance of its compliance.
- The application/software vendors hired by Brokerage Houses must develop the applications in line with these standards, specifications, and requirements.

6 CONTROLS APPLICABILITY

All controls specified in the application security standards, specifications, and requirements 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 software vendor will provide sufficient details of those controls that are not implemented along with the justification.

7 TESTING & CERTIFICATION

The penetration testing or vulnerability assessment of all applications which store or process market sensitive data shall be completed independently atleast once in every two years or whenever there is any major change in application/system. The critical and high risk observations identified as a result of the testing must be rectified within 6 months of identification.

The testing must be performed by the Exchange approved vendor listed on Exchange website.

8 CONTROL DEFINITIONS

8.1 Access Controls

All computer systems should have a logon authentication procedure that includes at least a unique user ID and password (some systems may potentially require additional verification, such as RSA tokens).

User Access Controls –

a) Unique user IDs 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 the 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) The 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 defined period of activity, and the session lock should be retained until the user re-establishes access using the established identification and authentication procedure.

g) The application should force the user to change the password at the time of first login.

h) 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.

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) Where strong authentication and identity verification is required, such as systems which store or process market sensitive information, authentication methods alternative to or complementing passwords, such as tokens (hard or soft), cryptography (symmetric or asymmetric encryption) or biometric shall be used.

c) The following password controls shall be enforced at a minimum,

- Access to systems shall not be allowed until a password has been authenticated with a unique username.
- A system based confirmation procedure shall be in place to allow for input errors at the time of password selection.
- Passwords shall be at least 8 characters in length.

- Passwords shall include a mixture of at least three of the following,
  - Uppercase characters (A, B, C …);
  - Lowercase characters (a, b, c …);
  - Numbers (0, 1, 2 …); and
  - Special Characters (!, @, # …).
- User passwords shall be changed at least every 120 days.
- Passwords shall be changed at least 3 times before re-use.
- After 5 failed login attempts the account should be locked out temporarily and the user should be required to contact the Administrator to reset the password or the account may automatically unlock after 30 mins.
- 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.
- Passwords shall not be displayed on the screen in clear text, be printed in clear text or be cached.
- Passwords should not be transmitted in clear text over a network, to avoid being captured by a network 'sniffer' program.
- 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.

User Administration –

a) Unique security administrator IDs should 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,

- Request for user access;
- Approval of request;
- Implementation of request; and
- Monitoring of changes.

c) The user access should 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 should be assigned to a user ID different from those used for regular business activities. Regular business activities should not be performed from a privileged ID.

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

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

h) The application shall have the functionality available to create on-demand reports in below format. The reports should be available in excel format.

Report 1 – User Access Summary Report

S. No.	Application Name	User Id	User ID / Access Status	User id creation date	User id deletion date	User access last modification date	User access last enablement date

Report 2 – User Access Detailed Report

S. No.	Application	User Id	User Profile / Rights

Report 3 – Information Security Administrator Detailed Report

S. No.	Application Name	Maker Id	Checker ID	Activity	Date	Time

8.2 Encryption

Encryption Requirements –

a) Sensitive data should 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) Sensitive data should 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) In order to support above mentioned aims, following mechanisms can be employed:

- Sensitive data can be transmitted via encrypted communication channel to ensure that it does not traverse the network in plain-text; or
- The data can be encrypted to facilitate the secure transport of individual files, data feeds, email attachments and mobile SMS messages through the application over network where encryption on wire is not feasible; or
- In web-based application, end-to-end encryption i.e. between user's browser and the web server of communicated data can be secured through the use of secure protocols e.g., (HTTPS, TLS/SSL etc.).

d) Hashing of the data/information shall be used, where technically feasible, to ensure that the data received at receiver end is original and not tempered through man-in-the-middle attack.

Algorithm Requirements –

a) The encryption should be achieved using secure algorithms, such as AES, DES3, RSA or comparable algorithm.

b) Cryptographic hash values should be derived using secure algorithms: SHA-2, SHA-3, or Whirlpool or comparable algorithm.

c) The minimum cryptographic key length should be 128 bits.

d) Self-signed Digital Certificates, if required, shall be created by applying recognized standards (e.g., X.509v3) and shall at least,

- Identify the issuing certificate authority;
- Identify its subscriber;
- Provide the subscriber's public key;
- Identify its operational period; and
- Be digitally signed by the issuing certificate authority.

Key Management –

a) Encryption keys used to protect organization's sensitive information shall be classified at the highest classification / sensitivity level, i.e. 'Restricted'.

b) The access to encryption keys should be restricted to authorised users only based on need-to-know principle.

c) The key exchange between two parties to agree on a session key must be done through: Diffie-Hellman or comparable algorithm etc.

d) If keys are exchanged over communication lines / emails, they themselves should be sent in encrypted form.
e) Encryption keys that are compromised should be revoked/replaced. Key re-assignments should require re-encryption of data.
f) 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.)

8.3 Logging

General Controls –

a) Application should generate logging data in normalized data format such as log record entry starts with [date & time, user ID, event ID, concise description of exhibit] etc.
b) Application should have a provision to make logs available as and when needed in structured human readable format.
c) The logging facilities and log information should only be accessible as and when needed by authorized personnel.
d) Files containing encrypted or hashed passwords which are required for systems to authenticate users should be readable only with super-user privileges.
e) All remote access to a network, whether to the DMZ or the internal network (i.e., VPN, dial-up, or other mechanism), should be logged verbosely.
f) Logging system time shall be synchronized with open source or organization's (i.e., Network Time Protocol or NTP) so that timestamps in logs are consistent.
g) Logging data shall contain user activities that includes, but not limited to:

    - Successful and failed logins with source IP address, user ID, date, timestamp, source addresses, destination addresses, protocols and various other useful elements of each packet and/or transaction;
    - On any change in application regarding business process creation / modification like Alert Management, log record must be generated;
    - Edit account settings i.e. password change etc. (but no password itself should be saved);
    - Generating and exporting reports by logged in user;
    - Printing reports through the application by logged in user;

Application Administration –

a) Log entries shall be created for user access provision, modification in user roles / profiles and user revocation by administrator.
b) Application shall generate record in log file whenever user password is reset or account unlocked by administrator.
c) Log data shall not record any sensitive information, including authentication or market sensitive data. Any encryption keys must also not be logged.

Maintaining Log Data Security and Integrity –

a) The logging facilities and log information should be protected against, tampering/unauthorized changes to log information, including unauthorized log deletion;
b) The application should also restrict administrator to modify, erase or de-activate logs of their own activities;
c) Application logging data should be in the application's installation directory preferably in separate directory named as "Log".

8.4 Web Application Security Controls

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

a) **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.
b) **Injection** – 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.
c) **Broken Authentication and Session Management** – 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.
d) **Cross-Site Scripting (XSS)** – 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.
e) **Insecure Direct Object References** – 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.
f) **Security Misconfiguration** – 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.
g) **Sensitive Data Exposure** – Most web applications 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.
h) **Missing Function Level Access Control** – 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.

i) **Cross-Site Request Forgery (CSRF)** – 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 defences and enable a range of possible attacks and impacts.

j) **Using Components with Known Vulnerabilities** – 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.

8.5 Data Preview, Export and Transfer Controls

a) The application should not provide facility to preview, export or transfer unauthorized data e.g. in any case the data of other members should not be displayed or transferred using the application.

b) The practices pertaining to due diligence and due care should be followed while previewing, exporting or transferring data before transferring between applications.

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) The application should follow best practices to maintain the confidentiality of data in preview, exports or transfer processes.

e) The 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 data should remain visible to the authorized individual in the process.

f) The transfer of data between applications should comply the contractual and legal requirements.

8.6 Input Handling

The most common application security weakness is the failure to properly validate input coming from the client or from the environment before using it. This weakness leads to almost all of the major vulnerabilities in the applications, such as cross site scripting, SQL injection, interpreter injection, file system attacks, and buffer overflows. Ensure that a verified application satisfies the following high level requirements:

1. All input is validated to be correct and fit for the intended purpose.
2. Data received from an external entity should never be trusted and sufficient validation control should be in place to ensure protection from data corruption.

Ensure that the following controls are sufficiently in place within the application:

a) The runtime environment is not susceptible to buffer overflows, or that security controls prevent buffer overflows.

b) Server side input validation failures result in request rejection and are logged.

c) Input validation routines are enforced on the server side.

d) A single input validation control is used by the application for each type of data that is accepted.

e) 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.

f) Application is not susceptible to LDAP Injection, or that security controls prevent LDAP Injection.

g) Application is not susceptible to OS Command Injection, or that security controls prevent OS Command Injection.

h) Application is not susceptible to Remote File Inclusion (RFI) or Local File Inclusion (LFI) when content is used that is a path to a file.

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 client 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 defences 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) Client side validation is used as a second line of defence, in addition to server side validation.

n) 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)

o) 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).

p) Unstructured data is sanitized to enforce generic safety measures such as allowed characters and length, and characters potentially harmful in given context should be escaped (e.g. natural names with Unicode or apostrophes, such as ねこor O'Conner).

q) Untrusted HTML from WYSIWYG editors or similar are properly sanitized with an HTML sanitizer and handle it appropriately according to the input validation task and encoding task.

r) For auto-escaping template technology, if UI escaping is disabled, ensure that HTML sanitization is enabled instead.

s) Verify that data transferred from one DOM context to another, uses safe JavaScript methods, such as using .innerText and .val.

t) That authenticated data is cleared from client storage, such as the browser DOM, after the session is terminated.

9 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.

Address Space Layout Randomization (ASLR)
A technique to help protect against buffer overflow attacks.

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.

Application Security Verification
The technical assessment of an application against the OWASP ASVS.

Application Security Verification Report
A report that documents the overall results and supporting analysis produced by the verifier for a particular application.

Authentication
The verification of the claimed identity of an application user.

Automated Verification
The use of automated tools (either dynamic analysis tools, static analysis tools, or both) that use vulnerability signatures to find problems.

Back Doors
A type of malicious code that allows unauthorized access to an application.

Blacklist
A list of data or operations that are not permitted, for example a list of characters that are not allowed as input.

Cascading Style Sheets (CSS)
A style sheet language used for describing the presentation semantics of document written in a mark-up language, such as HTML.

Certificate Authority (CA)
An entity that issues digital certificates.

Communication Security
The protection of application data when it is transmitted between application components, between clients 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
A security vulnerability typically found in web applications allowing the

(XSS)	injection of client-side scripts into content.
Cryptographic module	Hardware, software, and/or firmware that implements cryptographic algorithms and/or generates cryptographic keys.
Denial of Service (DoS)	The flooding of an application with more requests than it can handle.
Design Verification	The technical assessment of the security architecture of an application.
Globally Unique Identifier (GUID)	A unique reference number used as an identifier in software.
External Systems	A server-side application or service that is not part of the application.
Hypertext Markup Language (HTML)	The main mark-upp 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.
Malicious Code	Code introduced into an application during its development unbeknownst to the application owner, which circumvents the application’s intended security policy. Not the same as malware such as a virus or worm!
Malware	Executable code that is introduced into an application during runtime without the knowledge of the application user or administrator.
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).
SQL Injection (SQLi)	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 markup 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.

PSX

PAKISTAN
STOCK EXCHANGE
LIMITED

PAKISTAN STOCK EXCHANGE

(FORMERLY KARACHI STOCK EXCHANGE LTD.)

Information Security Office (ISO)

Together Ahead