PAKISTAN STOCK EXCHANGE LIMITED
(Formerly Karachi Stock Exchange limited)
Stock Exchange Building, Stock Exchange Road, Karachi-74000
Phones: **111-001-122**

PSX/N-1502 Dated: **March 03, 2017**

NOTICE FOR SOLICITATION OF PUBLIC COMMENTS

BROKER BACK-OFFICE SYSTEM (*REVISED*)

This is in continuation to PSX notice number PSX/N-1266 dated February 27, 2017, wherein, the office of the Exchange had developed bare minimum standards and specifications for the Broker Back-Office Application, in accordance to Clause 4.26.1 (a) of PSX Rule Book.

The said guidelines, procedures and standards for the Broker Back-Office Application have now been revised in the following annexures, enclosed herewith, for public comments:

- Annexure A - Bare minimum standards and specification for Broker Back-Office Application (*Revised*)
- Annexure B - Application Security Standards Specifications, Requirements (*Revised*)

All TREC Holders / other entities interested are requested to kindly send in their comments for the above mentioned revised guidelines, procedures and Vendor eligibility criteria for Broker Back Office System to the undersigned latest by **Friday, March 10, 2017**.

SANI-E-MEHMOOD KHAN
General Manager
PAKISTAN STOCK EXCHANGE

Copy to:
Securities Market Division of SECP
MD and Acting CRO of PSX
HODs of PSX
CEO, Central Depository Company of Pakistan Ltd
CEO, National Clearing Company of Pakistan Limited
Regional Heads, PSX
PSX website

Annexure A

Working Copy

BROKER BACK OFFICE SYSTEM

BASIC GUIDELINES

PAKISTAN STOCK EXCHANGE

This document is released by the Exchange in consideration of Clause 4.26.1 (a) of PSX Rule Book and caters to only Broker Back-Office Application while prescribing bare minimum standards and specification.

The Exchange does not warrant that this document to be complete, as it only covers certain necessary elements which are required to be complied with in the context of above stated Regulation.

Table of Contents

Section 1
EXECUTIVE SUMMARY

This document presents bare minimal standard for Broker Back Office (BBO) Applications and eligibility criteria for the vendors of Broker Back Office Application. The Broker Back Office Vendors may use this document as a guideline to ensure that their BBO Application meets the bare minimal standards and specifications required by the Exchange in order for their Back Office Application to comply with clause 4.26 of PSX Regulations.

The section 2 of this document prescribes the eligibility criteria and the list of eligible back-office-vendors. The objective of prescribing the bare minimal criteria for eligible vendors is to ensure that only qualified vendors, having impeccable financial integrity, proven knowledge about application software of Capital Market Industry, adequate staff and corporate structure are allowed to act as service providers to the brokers.

The section 3 of this document covers the bare-minimal requirements for holding/retention of key information relating to account-opening, trading, risk management, settlement and compliance. The purpose of identifying the key-information-areas is to ensure that reliable information is available to Exchange for efficient thematic reviews, audits, inspections, and settlement of claims in the event of default of a broker.

The last section of this document contains the list and formats of the reports which must be generated through the BBO system.

Section 2
BROKER BACK OFFICE VENDORS

This section defines the eligibility criteria for selection of Broker Back-Office Vendors by the Exchange and contains the list of eligible vendors permitted by the Exchange to provide services to the Brokers.

2.1 Eligibility Criteria for Broker Back Office Application

Detailed below is the Eligibility criterion for a Vendor of Broker Back Office Application to apply for and continue to stay as PSX-authorized vendor for Broker Back Office Application:

2.1.1 Company Registration

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

2.1.2 Relevant Experience

Vendor must have at least 5 Years of experience in the area of application development/support in the Financial Industry. New Vendors without prior experience shall be required to present credentials and their application shall undergo a thorough and rigorous evaluation process by the Exchange.

2.1.3 Profitability

The Company should be profit making for at least last three years.

2.1.4 Skilled Resources

Vendor should have sufficient pool of qualified and skilled technical resources having business and IT graduates or Certified with at least 2-3 years of application development or system support experience in the Capital Market Industry.

Sufficient pool of qualified resource is defined as a group having two professionals as per above stated stature for each group of 20 brokers so as to ensure that adequate services are provided in a timely manner by the Broker Back Office Vendor to the Brokers.

2.2 Application and Vendor Evaluation Process

Software Service Vendors intending to apply and become Exchange approved “Back-Office-System-Vendors” shall apply to Exchange in writing along with their credentials, relevant documents, list of their “Skilled-worked-force” along with a certificate from an Auditor regarding appropriateness and compliance of their application software with Exchange prescribed IT and Information Security Standards.

2.2.1 Term and Duration of Vendor Eligibility

The Exchange shall authorize the vendor for a period of three years and Vendors shall be required to attain renewal after successful completion of term. Vendors once approved by the Exchange shall ensure that provisioning should be made in their system with regard to regulatory changes that takes place after the approval and before the expiry date.

2.2.2 List of Eligible Vendor(s)

Given below is the list of PSX approved Vendors authorized to act as Vendors of Broker-back-office:

S#	VENDOR NAME	VALIDITY*
01	Catalyst Solutions	31-DEC-2016
02	Microlinks Pvt. Ltd.	31-DEC-2016
03	Softman	31-DEC-2016
04	Softech Systems	31-DEC-2016
05	LSE Financial Services	31-DEC-2016
06	V. Boss/Venturechest	31-DEC-2016
07	Vision Technologies	31-DEC-2016

**This is neither approved nor a final list of back-office-vendors*

Section 3
THE BARE MINIMAL STANDARDS

The Exchange Regulations require that the Software or application which TREC Holders use for trade-facilitation of their client and the Software that they use for risk-management and record-keeping shall meet some bare-minimal standards and specifications.

The general controls for Broker Back Office (BBO) System must entail in the following manner:

1. There shall be only single back office software and single book of accounts at any given time.
2. Each application shall be connected with single database.
3. The remote access to applications and database shall be controlled. The on-demand access for the vendor shall be enabled for support purposes only via access request approval process only for the duration required. Remote access users should be separately defined and clearly identified. For remote access by the vendor, only remote access users should be used and their activity should be fully logged and maintained.
4. Formal change management procedures should be employed to document the nature of change, justification, authorization, and other related business or technical level details.
5. The Trade Log shall be updated online in the BBO System.
6. The manual process to update the BBO system with trade log shall be discontinued.

In regards to the above, the areas of Account Opening, Trading, Clearing, Settlement and Custody shall comply with Information and Application Security Standards specified by the Exchange along with the standards and specifications prescribed in this document.

3.1 Account Opening

3.1.1 Client Account Management

Client information stored in the system at the time of opening of the account shall not be allowed to be deleted once a client account is operational. However, modification with regard to client details shall be controlled and the system should be capable of storing the original information that has been modified. This may be noted that there no provisions in law which could allow the change of title of account of Client name. The system shall also have the provision to upload the client information from CDS – client setup report.

3.1.1.1 KYC Principles

The system should comply with KYC principles and standards and should have provision to electronically store the scanned documents leading to the identity of the Client.

3.1.1.2 Client / Account Classification

The system should have provision to classify clients into various categories on the basis of most recent payment trends in relation to the information obtained through KYC, so as to help identify high, low and medium risk clients.

3.1.1.3 Reassignment of Client Code

Further, the system shall ensure that client codes once assigned to any client shall not be reassigned to another client of the brokers even after the closure of account so as to ensure the compliance of PSX rule book clause 8.6.1 as reproduced hereunder:

> *"Every Broker while inserting a bid and offer through KATS for each of his clients, shall insert unique Client Codes for those clients which are maintained by them in their back office system and registered with NCCPL. These Client Codes are linked/mapped to UIN through the interface of NCCPL.* **These Client Codes should not be re-assigned to another client of the Brokers even after the closure of the account"**

3.1.1.4 Web access for Clients

The system should be provided a secure access through a URL for enquiring and viewing account statements on real-time basis or EOD basis.

3.2 Trading

Apart from complying with relevant regulations and storing information relating to trading of the client, the system should have provisions to have trade-time and trade-confirmation-SMS sent time stored in the system.

3.3 Maker and Checker functionality

In order to facilitate role based permissions and auditing, the system should have provisions of maker and checker functionality for each and every transactions/account entry which is substantial and material.

The principle of maker and checker means that in order to have proper segregation of duties for each transaction (wherever required), there must be at least two individuals necessary for its completion. While one individual may create a transaction, the other individual should be involved in confirmation/authorization of the same.

3.4 Audit Logs and Privilege Roles

The system shall be capable of generating and storing audit logs for all users and information in respect of login, data entry, and trail of modification/deletion with date and time along with exceptional reporting at user and system level.

The Broker Back Office System should establish and maintain operational and systems in-built audit control to facilitate automatic reconciliations and perform **exceptional reporting:**

- ✓ Number of Order, their quantities and values entered
- ✓ Number of Client's, their quantities, volumes and executed values
- ✓ Number of Stocks, Markets and types of order and values processed
- ✓ Gross Settlement values versus totals at Client, Market and Stocks level

3.5 Reports to comply with regulatory requirements

The system should be capable of generating and processing reports in the manner to enable TREC holders to comply with the requirements of regulatory framework. At minimum, the system shall be capable of generating/processing the following reports;

1- Wash trade report (company level/branch level/agent level)

2- Blank sale report (company level/branch level/agent level)

3- Trade rectification report (company level/branch level/agent level)

4- Cross trade report (company level/branch level/agent level)

5- Back date voucher report

6- Client last activity report

7- Employees investment holding period report (as required under section 16(3)f of Securities Brokers (Licensing And Operations) Regulations 2016

8- Client assets segregation and reconciliation report

9- Order register in the manner prescribed under section 19(4) of Securities Brokers (Licensing And Operations) Regulations 2016

10- Contract notes in the manner prescribed under section 21 and 22 of Securities Brokers (Licensing And Operations) Regulations 2016 and section 4.19 of PSX Rule Book.

11- Aging analysis report in the manner prescribed under section 34(2)h of Securities Brokers (Licensing And Operations) Regulations 2016

12- Quarterly account statements of the clients in the manner prescribed under Section 4.22 of PSX Rule Book.

13- Monthly IBTS reports as in the manner prescribed under Section 9.11(a) and 9.11(b) of PSX Rule Book.

3.6 Other Key Areas

The system must also include the provision for setting-up of branches, catering to accounting needs of various markets, multiple settlement cycles, maintenance of General and Sub-General Ledger and mapping of client with a ledger account. The system shall contain provisions for recording and maintenance of the following details/records;

1- Fixed asset register report

2- Accounting ledgers

3- Client trial balance

4- Accounting trial balance

5- Income statement

6- Balance sheet

7- Bank reconciliation report

3.7 Reconciliations and Back Office Accounting System

The System should contain provisions for day-end-reconciliations of back-office systems custody with CDC and NCCPL. The system must also ensure the segregations of customer money and 'own funds' by the way of maintenance of proper books and account, recording of liabilities, ledgers reflecting cash and custody movement and day-end-reconciliations of clients funds with client bank accounts.

Section 4
ANNEXURE A —BARE MINIMUM SPECS

4.1 Application Security (Password Management)

Sr. No.	Details
1	Passwords are masked during data entry on screen.
2	Passwords are unreadable during the course transmission, display and storage in the database.
3	Passwords are never kept in application/session memory.
4	Passwords are expired after first login and enforce to change them immediately.
5	Disable account after configurable number of consecutive failed attempts.
6	Enforce password change at least once in configured number of days.
7	Conform to accepted principles of strong password.
8	Maintain Password history and do not allow repetition from last 10 passwords
9	User can change password anytime
10	While Changing, re-entry of password is mandatory
11	There is no default (or internal) password which cannot be changed.
12	In case of failed login, user ID, date, time and machine address should be stored in the system
13	All successful and failed login attempts are logged with timestamp and machine address.
14	System can only be accessed through valid user id/login.
15	Access to the various tasks is based on roles and privileges defined in the system (User Admin)
16	Every User Account/Password must have an expiry date
17	Expiry date can be attached with each account to deactivate the account on a specific date.
18	Maker and Checker functionality as per latest accepted industry standards is always followed.
19	User Admin module should be able to define access at screen level, authorization for save/post

4.2 Custody Related Data

Sr. No.	Details
1	System should have the ability to maintain list of possible activities
2	System should have the ability to categorize activities into groups.
3	System should have the ability to mark IN or OUT activity.
4	System should have the ability to define multi leg activities and ability to assign the other leg. They could be used for activities like pledge, verification, conversion etc.
5	System should have the ability to associate charges with transactions/activities.
6	System should have the ability to mark tradable and non-tradable activities.
7	System should have the ability to define expense types and whether they are chargeable to clients or not.
8	System should have the ability to maintain corporate announcements for each company.

4.3 Risk Management Related Data

Sr. No.	Details
1	Pre trade and post trade client risk management.
2	System should have the ability to define securities groups
3	System should have the ability to define haircuts for securities & security groups
4	System should have the ability to define credit limits, maintenance margin percentage, cash requirement percentage and maximum exposure limits.

5	System should have the ability to define different maintenance margin, cash requirement and exposure limits percentages for different market types, clearings, securities, security groups and future periods.
6	System should have the ability to block or allow short trading
7	System should have the ability to generate detailed and summarized client wise account positions with margin requirements and available margins, which includes; • Cash balance • Holding value • Current exposure • Buying power • Margin required • Available marginable equity • Current margin percentage • Margin call on Intra-day and historic basis

4.4 Mandatory Complaince With SECP Report Formats

4.4.1 NET CAPITAL BALANCE Report

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

4.5 Client Registration Individual / Corporate Report

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.**

4.5.1 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**

4.6 Client Funds Deposited into Bank

Client Fund Deposits into banks

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

4.7 Payment to Client Report

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

4.8 Bank Interest on Clients' Bank Accounts Report

Interest on Clients Bank Accounts

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

4.9 Un-posted Trades Book Report

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

4.10 Client Ledgers- Ready & Futures Report

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

4.11 Client Ledgers- Leveraged Report

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

4.12 Client Securities Report

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

The system shall be able to generate the “Client Securities Report” at company level, branch level and agent/trader level.

4.13 Pre-Settlement Delivery Report

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

4.14 Pledging of Client Securities Report

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

4.15 Client Aging Report

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

4.16 Client Wise CDC/Back Office Matching Report

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

4.17 Risk Management Report

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

The system shall be able to generate the "Risk Management Report" at company level, branch level and agent/trader level.

4.18 Broker's Proprietary Trades/Investments Report

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

4.19 Complaint Handling Report

Complaint handling Database

Sr. No	Date	Client		Nature	Steps taken to Resolve	Current Status	Date of Resolution	Description of Resolution
		Code	Name					

4.20 List of Agents Report

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

4.21 Commission Report

Commission Report

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

4.22 Loan Report

<table>
<tr><td colspan="7">Broker Name</td></tr>
<tr><td colspan="7">Corporate Member Pakistan Stock Exchange Limited</td></tr>
<tr><td colspan="7">(Address) (Ph#)</td></tr>
<tr><td colspan="7">(Details of Loan) (Date ________)</td></tr>
<tr><td>Sr. No</td><td>Name of Bank</td><td>Account No</td><td>Branch</td><td>Bank Code (Back Office)</td><td>Financing Facility</td><td>Mark-up Charged</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td>Rs</td><td>% age</td></tr>
</table>

Section 5

ANNEXURE B — COMPLIANCE REGULATORY REQUIREMENTS REPORTS

5.1 Wash Trade Report

WASH TRADE STATEMENT							
Ticket Number	UIN/Client	Symbol	QTY	Rate	Market	Buy Terminal/Order	Sell Terminal / Order

5.2 Blank Sale Report

BLANK SALE STATEMENT				
Symbol	Tittle	Max Short	Available	Blank

5.3 Trade Rectification Report

TRADE RECTIFICATION REPORT									
Date	Ticket No.	Order No.	Symbol	Type	Qty	Rate	Clients	KATS Entry	Remarks

5.4 Back Date Voucher Report

Back Date Voucher Report					
S.No	**Date**	**Time**	**Action**	**User Id**	**Description**

5.5 Client Last Activity Report

Client Last Activity Report

Purchase

Scrip	Flag	Qty	Rate	Comm.	CDC	PSX Laga	SECP Laga	NCCPL	C.V.T	W.H.T.	Adv. Tax	SST	Amount

Sale

Scrip	Flag	Qty	Rate	Comm.	CDC	PSX Laga	SECP Laga	NCCPL	W.H.T.	Adv. Tax	SST	Amount

Summary	
Purchase Amount	
Sell Amount	
Net Amount	

TRANSACTION SUMMARY FOR (DATE)

Symbol	Title	Flag	Buy	Sell	Net	AVG(G)	Gross AMT	COMM	CDC	OTC	CVT	SST	Net Amount	AVG(N)

Accounts Ledger from (Date) to (Date)

VOU/BILL #	Date	Paticulars	Symbol	QTY	Flag	Debit	Credit	Balance

Outstanding Trades

Symbol	Buy	Sell	Net	Trade Value	AVG.	MKT	Profit/(Loss)	Exposure	Demand

Portfolio/Deliveries

Status	Symbol	Scrip	Quantity	MKT	Market Value	MKT.VAL With H/C

Accounts/Ledger Balance	
Securities Value With H/C	
Outstanding Profit/(Loss)	
Net Equity/Floating	
Trading Limit @ 40%	
Current Exposure @ 0%	

Balance Trading Limit	
Excess/(Demand)	

5.6 Employees Investment Holding Period Report

Employee Investment Holding Report					
Scrip	**Symbol**	**Pending**	**Available**	**Closing**	**Market Value**

5.7 Client Assets Segregation and Reconciliation Report

"Client Asset Segregation Statement"

As on __________

Securities Segregation					
As per Back Office Record	Own Account	Client Account	As per CDC Record	Own Account	Client Account
Securities Held			Securities Available		
			Securities Pledges with PSX/NCCPL		
			Securities Pledged with Banks		
			Pre-Settlement Delivery		
			*Reconciling Entries:		
Total			Total		

Cash Segregation			
Trade Payable (Clients)		Cash at Bank (Client Account)	
		Reconciling Entries:	
Total		Total	

5.8 Order Register

Order Register										
Code	Client Title	KAT CD	Symbol	Scrip	QTY	Rate	TYPE	ORD#	Ticket Number	Time

5.9 Contract Notes

Contract Note

Purchase Confirmation - (Regular)

Scrip	QTY	Rate	Comm.	CDC	PSX Laga	SECP Laga	NCCPL	C.V.T	W.H.T	Adv.Tax	SST	Net Amount

Summary	
Purchase Amount	
Sale Amount	
Net Amount	

Purchase Confirmation - (Future)

Scrip	QTY	Rate	Comm.	CDC	PSX Laga	SECP Laga	NCCPL	C.V.T	W.H.T	Adv.Tax	SST	Net Amount

Sale Confirmation - (Future)

Scrip	Qty	Rate	Comm.	CDC	PSX Laga	SECP Laga	NCCPL	W.H.T	Adv.Tax	SST	Net Amount

5.10 Aging Analysis Report

Aging Analysis Report						
Client Code	**Title**	**Balance**	**1-14**	**Above -14**	**Sec. Values**	**Allowed**

5.11 Monthly IBTS Reports

Monthly IBTS Report	
Broker Name	
Internet Based Trading (I.T.S) Commenced From	
Total Active Clients	
No. of Clients Using I.T.S	
Total No. of Trades	
Total Volume Traded	
Security Value Traded	
Average Transactions Per Day	
Highest No. of Transaction / date	
Application Mode Provided to Clients	
Software Provider/Vendor	
No. of Clients Using I.T.S	
Non-Availability of % of Scheduled Time# of Incidences Reason (s) (if any)	
System Modification (If any)	

5.12 Cross Trade Report

Cross Trades Statement								
		Buyer Code			**Seller**			
Symbol	**Ticket No.**	**Buyer Code**	**Buyer**	**Qty**	**Seller Code**	**Seller**	**Qty**	**Rate**

PAKISTAN
STOCK EXCHANGE
LIMITED

Application Security Standards, Specifications and Requirements

Information Security Office (ISO)
Pakistan Stock Exchange Limited

Version 0.8

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) TREC Holders 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	16/12/2016	Mr. Arif Rehman (CISO)	PSX IT & Information Security Steering Committee	--	Committee Review & Feedback
0.7	30/12/2016	Mr. Arif Rehman (CISO)	TREC Holders Review	--	TREC Holders Review & Feedback sought via Notice PSX/N-7372
0.7	16/02/2017	Mr. Arif Rehman (CISO)	Software Vendors Review	--	Software Vendors Review & Feedback
0.7	16/02/2017	Mr. Arif Rehman (CISO)	TREC Holders Review	--	TREC Holders Feedback (Seminar) sought via Notice PSX/N-1006
0.8	03/03/2017	Mr. Arif Rehman (CISO)	TREC Holders Review	--	--

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 TREC Holders 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 TREC Holders 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 TREC Holders 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 TREC Holders in order to ensure that the order management system, front office system, back office system and other related software used by TREC Holders which directly or indirectly supports trading or related activities meet the minimum standards and requirements prescribed by the frontline regulator.

Furthermore, vendor(s) providing penetration testing or source code review services are subject to eligibility criteria thereby ensuring quality of the software and creating accountability.

3 SCOPE

The document prescribes application security standards, specifications, and requirements to be met by the application or software, regular testing and certification requirements, as well as eligibility criteria for the vendor who may provide penetration testing or source code review services to the TREC Holders of the Pakistan Stock Exchange (PSX), and matters considered necessary thereto.

The document is intended for PSX TREC Holders 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 need. 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 TREC Holders.
- 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 awareness of stakeholders concerning these standards, specifications, requirements, and assuring its compliance through regular system audits.

- The TREC Holders 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 TREC Holders 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 TREC Holders or/and software vendor shall provide sufficient details of those controls that are not implemented along with the justification.

7 TESTING & CERTIFICATION

The vulnerability assessment or source code review of applications which store or process market sensitive data shall be completed independently atleast 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 within 6 months of identification.

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

8 VENDOR ELIGIBILITY CRITERIA

In order to ensure that the vulnerability assessment or source code review 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 shall utilise following pre-established criteria against which prospective vendors shall be evaluated prior to being approved.

a) Vendor shall be a registered company with established office in Pakistan.

b) Vendor shall be a registered company with established office in Pakistan.

c) Vendor shall be profit making for atleast last three (3) years.

d) Vendor shall have atleast three (3) certified technical staff in related services.

e) Vendor must have atleast five (5) years of experience in related services.

f) Vendor shall have successfully delivered ten (10) similar assignments within past three (3) years.

g) Vendor shall be able to furnish three (3) verifiable references from within past three (3) years.

The Exchange will assess the interested vendors and maintain a list of approved vendor on the Exchange website.

9 Control Definitions

9.1 Access Controls

All computer systems must have a logon authentication procedure that includes at least a unique user ID and password.

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 30 minutes of inactivity, 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) 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 shall be transmitted encrypted 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 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,

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

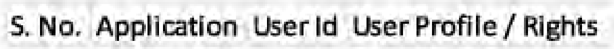
g) The application shall create detailed logs for each of the above activities.

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

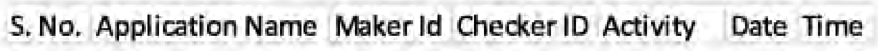
S. No.	Application Name	User Id	User ID / Access Status	User id creation date	User id deletion date	User access last modification date	User access last enablement date

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

9.2 Encryption

Encryption Requirements –

a) 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) 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.

Algorithm Requirements –

a) The encryption should be achieved using secure algorithms, such as AES, 3DES, RSA or comparable algorithm.

b) The 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) 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) The encryption keys shall be unique and known to TREC Holders’ authorised 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.*)

9.3 Logging

General Controls –

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.
c) The log shall contain sufficient details, for example, date & time, user ID, event ID, concise description of activity etc., to track an activity.
d) The 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.

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 shall store logs within database and maintain provision to make logs available as and when needed in structured human readable format.

9.4 Data Preview, Export and Transfer Controls

The application should follow best practices to maintain the confidentiality of data in preview, exports or transfer processes. Ensure that following controls are sufficiently in place within the application:

a) The 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) 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.
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.

9.5 Input Handling

The most common application security weakness is the failure to properly validate input entered by the user using application client 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.

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

a) All input is validated to be correct and fit for the intended purpose.

b) Server side validation shall be used as a second line of defence, in addition to client side validation.

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

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

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

f) 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.

g) Application shall not be susceptible to LDAP, OS Command, and Remote File Inclusion (RFI) injections, as applicable.

h) Application is not susceptible to common XML attacks, such as XPath query tampering, XML External Entity attacks, and XML injection attacks.

i) 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.

j) 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.

k) 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.).

l) 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)

m) 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).

n) 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.

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

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

9.6 Web Application Security Controls

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,

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) **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.

c) **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.

d) **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.

e) **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.

f) **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.

10 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.

PAKISTAN
STOCK EXCHANGE
LIMITED

PAKISTAN STOCK EXCHANGE

(FORMERLY KARACHI STOCK EXCHANGE LTD.)

Information Security Office (ISO)

Together Ahead