Application Security Standards, Specifications and Requirements

---

Information Security Office (ISO)
Pakistan Stock Exchange Limited

Version 1.0

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.

Copyright © 2016 Pakistan Stock Exchange Ltd.
All Rights Reserved

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)	SECP Review	--	SECP 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	18/04/2017	Mr. Arif Rehman (CISO)	TREC Holders Review	--	TREC Holders Review & Feedback sought via Notice PSX/N- 2355
0.9	20/07/2017	Mr. Arif Rehman (CISO)	Internal Audit (Deloitte) Review	--	Deloitte Review & Feedback

1.0	22/09/2017	Mr. Arif Rehman (CISO)	--	Mr. Haroon Askari (MD)	MD Approval  MD Approvals - without attachment

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 profit making for atleast last three (3) years.

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

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

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

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

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

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

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

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

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

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

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

j) **Unvalidated Redirects & Forwards** – Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the

destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages.

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

(FORMERLY KARACHI STOCK EXCHANGE LTD.)

Information Security Office (ISO)

Together Ahead