

To:
Board of Directors
Securities Exchange Members

Jakarta, October 11th 2011

CIRCULAR LETTER
SE-00005/BEI/10-2011

Regarding: Technical Requirements for Securities Exchange Member Providing Direct Client Access For Order Delivery Facility

Dear Sir/Madam,

In reference to the provision IV.16 of Rule Number III-A concerning Exchange Membership (Attachment of Board of Directors' Decree of the Indonesia Stock Exchange Number Kep-00401/BEI/12-2010 dated December 28, 2010 on the Amendment to the Rule Number III-A concerning Exchange Membership), we hereby inform the following matters:

1. Technical Requirements for Securities Exchange Member Providing Direct Client Access For Order Delivery Facility which will be further explained in this Circular Letter are related to main concept of system security.
2. System security main concept comprises of the following matters:
 - a. Provisions of security implementation.

Securities Exchange Member is required to have a good system security governance in order to:

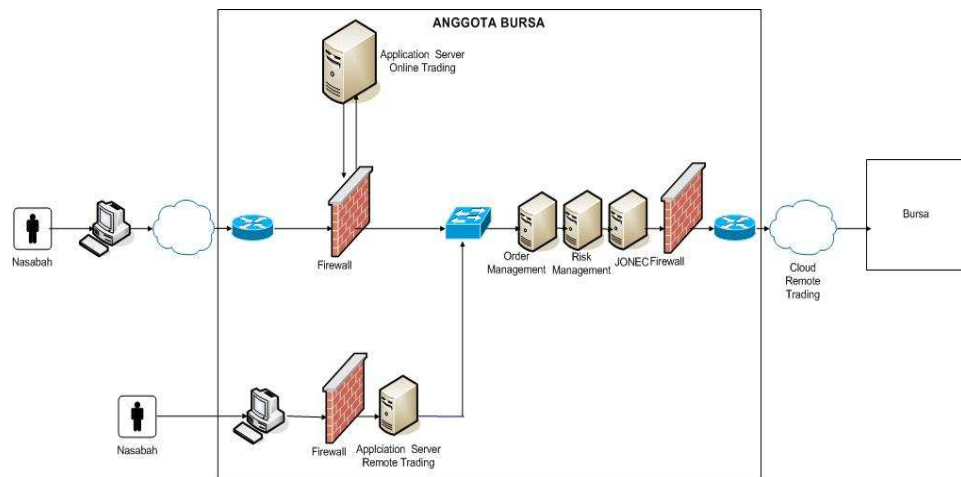
- 1) Preserve the information confidentiality, to make sure that certain information can only be accessed by intended authorized party;
 - 2) Preserve information integrity, to keep the accuracy and completeness of the information to ensure information credibility; and
 - 3) Information availability (availability), to ensure that the users can apply Direct Client Access For Order Delivery Facility system at any given time.
- b. Control toward malicious code, including but not limited to regular update for antivirus or anti malware activities.
 - c. Information Management and Back-up System Management
 - 1) Performing data back-up activity and audit trail everyday while maintaining the information integrity and security.

- 2) Providing alternative hardware to replace damaged equipment, either provided by Securities Exchange Member itself or by using vendor service through maintenance service contract.
- 3) In order to maintain the operation continuity, Securities Exchange Member is required to have source code warranty of application, with condition:
 - a) Having specific procedures for Securities Exchange Member that develops the application by itself; or
 - b) The source code is kept in escrow agent for Securities Exchange Member having its application developed by vendor
- d. Applying cryptography in the form of secure channel (randomization of data using certain method) to prevent data exchanged between Securities Exchange Member and Client accessed by unauthorized party.
- e. Applying monitoring system
 - 1) Monitoring and maintaining the availability of each component in Direct Client Access For Order Delivery Facility.
 - 2) Log activity is available in Direct Client Access For Order Delivery Facility.
 - 3) Having audit trail function, which are chronological record of events and their related supporting data.
 - 4) Data recorded in audit trail at minimum contain of event time, IP Address, User Id, and data related to the event.
 - 5) Avoiding audit trail deactivation function, unless cannot be avoided, such as mass-product IT equipment.
 - 6) Such audit trail facility must be active at any time.
- f. Conducting time synchronization in every hardware and application applied in Direct Client Access For Order Delivery Facility with JATS time on every Exchange Day at minimum before trading hours.
- g. Access Control and Account Policy
 - 1) Authentication

Application functions of Direct Client Access For Order Delivery Facility can only be accessed after authentication process is performed. Some authentication forms that can be applied are as follow:

 - a) Multilevel authentication with 2 (two) passwords, e.g. first password is applied to see the information only, while second password is applied to make order; or

- b) Authentication with 2 (two) methods, e.g. using password and pin pad which generate second authentication code; or
 - c) Implementation of Public Key Infrastructure, e.g. using Certification Authority (CA) service.
- 2) There is no certain facility in accessing the function of Direct Client Access For Order Delivery Facility system without authentication and authorization processes (backdoor access). Securities Exchange Member is required to ensure that the application being operated by Securities Exchange Member has no such backdoor access facility.
 - 3) Applying session time out (e.g. auto logout or session termination) if the Client's terminal shows no activity by no more than 5 minutes to avoid misuse by other party.
 - 4) Multiple login facility is not allowed, login cannot be conducted when the respective user is still login.
- h. Hardware Placement in the Network.
- 1) In order to maintain the system security and performance, Securities Exchange Member is required to apply dedicated firewall that is configured only for Direct Client Access For Order Delivery Facility. All unused ports in Direct Client Access For Order Delivery Facility must be closed.
 - 2) All servers of Direct Client Access For Order Delivery Facility must be placed in Demilitarized Zone (DMZ) so access from outside or inside must be performed through respective firewall.



i. Network Connection Control

It is highly recommended to use the Application of Intrusion Prevention/Detection System (IPS/IDS) as preventive action/monitoring against infiltration.

j. Information and Application Access Control

Direct Client Access For Order Delivery Facility application must limit the access to information or function based on system authorization of system application. Therefore, restricted information or function cannot be displayed or used.

k. Cryptography Application Policy and Audit Trail Management (e.g. password, PIN, PIN Pad)

1) Securities Exchange Member is required to perform management in making, using, sending, resetting, and removing audit trail to keep the audit trail confidentiality and integrity.

2) Sensitive and confidential Data must be saved in encrypted form, e.g. data concerning Client identity or PIN/password.

3) Confidential Data such as: PIN / password cannot be recorded in audit trail.

l. Preventing Application Infiltration

The application applies no cookies or temporary file which can be used to save confidential data, e.g. password.

m. Control toward Technical Vulnerability

1) Securities Exchange Member is required to perform vulnerability assessment followed by securing all vulnerability holes found. Additionally, it is suggested that Securities Exchange Member conduct evaluation on system security by performing penetration test, followed by remedial action.

2) Aspects which are required to be tested in the vulnerability assessment and penetration test among others: network perimeter, operating system, web server, database server as well as other supporting servers, network devices, and applications.

3) Applying patch continuously on system components, e.g. application, operating system, server, security and communication devices.

4) Securities Exchange Member is required to provide awareness program (awareness) concerning system security to Client.

3. Securities Exchange Member shall request an approval from the Exchange related to Strategic Order Management before implementing Direct Client Access For Order Delivery Facility (e.g. Securities Exchange Member intends to implement the algorithmic trading).

4. This Circular Letter is an inseparable part of the provisions set forth in the Rule Number III-A concerning Exchange Membership that must be complied by Securities Exchange Member that intends to provide Direct Client Access For Order Delivery Facility.

This Circular Letter shall take into effect as of the enactment date.

Stipulated in : Jakarta
Date : 11 October 2011

The Indonesia Stock Exchange

Ito Warsito
President Director

Uriep Budhi Prasetyo
Director

Carbon copy to the honorable:

1. Chairman of Capital Market and Financial Institutions Supervisory Agency (Bapepam and LK)
2. Head of Market Institutions & Transactions Bureau, Bapepam and LK
3. Head of Regulation & Legal Counsel Bureau, Bapepam and LK
4. Indonesia Public Listed Companies Association
5. Association of Indonesian Securities Companies
6. Association of Indonesia Custodian Bank
7. Indonesian Registrar Association
8. Board of Directors of The Indonesian Clearing and Guarantee Corporation
9. Board of Directors of The Indonesian Central Securities Depository
10. Capital Market Reference Center
11. Board of Commissioners of The Indonesia Stock Exchange