



Indonesia Stock Exchange
Bursa Efek Indonesia

Kepada Yth.
Direksi Anggota Bursa Efek
Di Tempat

Jakarta, 11 Oktober 2011

SURAT EDARAN
SE-00005 /BEI/10-2011

Perihal: Persyaratan Teknis Bagi Anggota Bursa Efek yang Menyelenggarakan Fasilitas Penyerahan Pesanan Secara Langsung Bagi Nasabah

Dengan hormat,

Menindaklanjuti ketentuan angka IV.16 Peraturan Nomor III-A tentang Keanggotaan Bursa (Lampiran Keputusan Direksi PT Bursa Efek Indonesia Nomor: Kep-00401/BEI/12-2010 tanggal 28 Desember 2010 perihal Perubahan Peraturan Nomor III-A tentang Keanggotaan Bursa), dengan ini kami sampaikan hal-hal sebagai berikut:

1. Persyaratan Teknis Bagi Anggota Bursa Efek yang Menyelenggarakan Fasilitas Penyerahan Pesanan Secara Langsung Bagi Nasabah yang akan dijelaskan lebih lanjut dalam Surat Edaran ini adalah terkait dengan konsep utama keamanan sistem.
2. Konsep utama keamanan sistem meliputi hal-hal sebagai berikut:
 - a. Ketentuan mengenai implementasi *security*.

Anggota Bursa Efek harus memiliki tata kelola sistem keamanan yang baik guna:

- 1) menjaga kerahasiaan informasi (*confidentiality*) agar diyakinkan bahwa informasi tertentu hanya dapat diakses oleh pihak yang berhak mendapatkannya;
 - 2) keutuhan informasi (*integrity*) untuk menjaga ketepatan dan keutuhan informasi sehingga informasi yang ada layak dipercaya; dan
 - 3) ketersediaan informasi (*availability*) untuk meyakinkan pengguna tetap dapat menggunakan sistem Penyerahan Pesanan Secara Langsung bagi Nasabah setiap saat dibutuhkan.
- b. Pengendalian terhadap program-program berbahaya (*malicious code*), termasuk namun tidak terbatas pada kegiatan berupa penerapan *update* berkala terhadap antivirus atau anti *malware*.

1/11/11
y

msj

A



Indonesia Stock Exchange
Bursa Efek Indonesia

- c. Pengelolaan Informasi dan Pengelolaan Perangkat Cadangan
- 1) Melakukan aktivitas *back up* data dan *audit trail* setiap hari dengan tetap menjaga integritas dan keamanan datanya.
 - 2) Menyediakan peralatan pengganti *alternative* untuk menggantikan peralatan yang rusak, baik disediakan sendiri oleh Anggota Bursa Efek maupun menggunakan jasa vendor melalui kontrak jasa pemeliharaan.
 - 3) Guna menjaga kelangsungan operasi, Anggota Bursa Efek harus memiliki jaminan ketersediaan *source code* aplikasi yang digunakan, dengan ketentuan:
 - a) Memiliki prosedur tertentu, bagi Anggota Bursa Efek yang mengembangkan sendiri aplikasinya; atau
 - b) Melakukan penyimpanan *source code* di *escrow agent* bagi Anggota Bursa Efek yang aplikasinya dikembangkan oleh vendor.
- d. Menerapkan kriptografi dalam bentuk *secure channel* (data diacak dengan metode tertentu) sehingga dapat menutup kemungkinan pihak lain menyalahgunakan data yang dipertukarkan antara Anggota Bursa Efek dengan nasabah.
- e. Menerapkan sistem pemantauan atau monitoring
- 1) Memonitor dan menjaga ketersediaan setiap komponen dalam Fasilitas Penyampaian Pesanan Secara Langsung bagi Nasabah.
 - 2) Catatan aktivitas (*log activity*) di dalam Sistem Fasilitas Penyampaian Pesanan Secara Langsung bagi Nasabah.
 - 3) Memiliki fungsi *audit trail* yaitu catatan kejadian secara urut waktu beserta data yang mendukung kejadian tersebut.
 - 4) Data yang tercatat dalam *audit trail* sekurang-kurangnya memuat waktu kejadian, IP Address, User Id, dan data mengenai kejadian.
 - 5) Menghindari adanya fungsi untuk menonaktifkan *audit trail* kecuali hal tersebut tidak dapat dihindari, misalnya pada peralatan TI yang merupakan produksi massal.
 - 6) Fasilitas *audit trail* ini harus aktif setiap saat.



Indonesia Stock Exchange
Bursa Efek Indonesia

- f. Melakukan sinkronisasi waktu di setiap perangkat dan aplikasi yang digunakan dalam penyelenggaraan Fasilitas Penyampaian Pesanan Secara Langsung bagi Nasabah dengan waktu JATS minimal setiap Hari Bursa sebelum jam perdagangan.
- g. Kebijakan Pengendalian Akses dan Penggunaan *Password*

1) Otentikasi

Fungsi-fungsi aplikasi Fasilitas Penyampaian Pesanan Secara Langsung bagi Nasabah hanya dapat diakses setelah proses otentikasi dilakukan. Beberapa bentuk otentikasi yang dapat diterapkan seperti berikut ini:

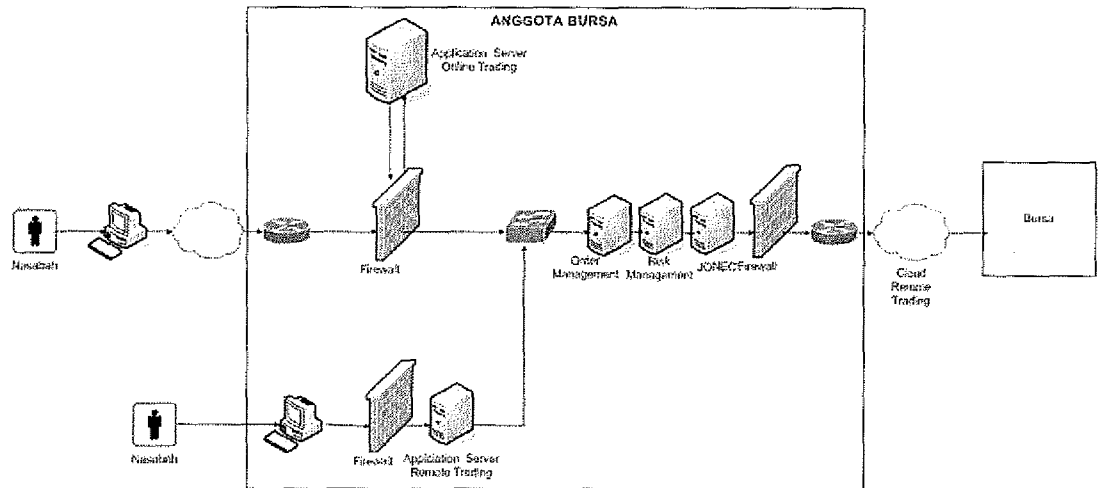
- a) Otentikasi bertahap dengan 2 (*dua*) *password*, misalnya *password* pertama hanya dapat melihat informasi, sedangkan *password* kedua untuk melakukan pemesanan; atau
 - b) Otentikasi dengan 2 (*dua*) metode, misalnya dengan menggunakan *password* dan token yang menghasilkan (*generate*) kode otentikasi kedua; atau
 - c) Penerapan *Public Key Infrastructure*, misalnya menggunakan jasa pihak *Certification Authority (CA)*.
- 2) Tidak terdapat fasilitas tertentu dalam mengakses fungsi-fungsi sistem Fasilitas Penyampaian Pesanan Secara Langsung bagi Nasabah tanpa adanya proses otentikasi dan otorisasi (*backdoor access*). Anggota Bursa Efek harus meyakinkan bahwa aplikasi yang dioperasikan Anggota Bursa Efek tidak mempunyai fasilitas *backdoor access* tersebut.
- 3) Menerapkan *session time out* (misalnya *auto logout* atau *session termination*) apabila di terminal nasabah tidak terdapat aktivitas dari nasabah yang bersangkutan dalam periode selambat-lambatnya 5 menit guna menghindari penyalahgunaan oleh pihak lain.
- 4) Fasilitas *multiple login* tidak diperkenankan, *login* tidak dapat dilakukan lagi jika *user* yang bersangkutan sedang *login*.

h. Penempatan Perangkat di dalam Jaringan.

- 1) Guna menjaga keamanan dan kinerja sistem, Anggota Bursa Efek harus menggunakan *firewall* tersendiri (*dedicated*) yang dikonfigurasi hanya untuk keperluan penyelenggaraan Fasilitas Penyampaian Pesanan Secara Langsung bagi Nasabah. Seluruh *port* yang tidak digunakan untuk penyelenggaraan Fasilitas Penyampaian Pesanan Secara Langsung bagi Nasabah harus ditutup.



- 2) Semua server yang digunakan untuk Fasilitas Penyampaian Pesanan Secara Langsung bagi Nasabah harus ditempatkan di dalam *Demilitarized Zone (DMZ)* sehingga akses yang dilakukan dari luar maupun dari dalam harus melalui masing-masing *firewall*.



i. Pengendalian Koneksi Jaringan

Direkomendasikan menggunakan *Intrusion Prevention/ Detection System (IPS / IDS)* untuk melakukan pencegahan/ pemantauan terhadap penyusupan

j. Pengendalian Akses terhadap Informasi dan Aplikasi

Aplikasi Fasilitas Penyampaian Pesanan Secara Langsung bagi Nasabah harus membatasi akses terhadap informasi maupun terhadap fungsi sesuai dengan otorisasi penggunaan sistem. Dengan demikian informasi maupun fungsi yang tidak boleh diakses tidak dapat dilihat atau dipergunakan.

k. Kebijakan Penggunaan Kriptografi dan Pengelolaan *Audit Trail* (seperti *password*, PIN, Token)

- 1) Anggota Bursa Efek harus melakukan pengelolaan dalam pembuatan, penggunaan, pengiriman, reset dan penghapusan *audit trail* untuk menjaga kerahasiaan dan integritas *audit trail*.

Handwritten signatures and initials in the bottom right corner.



Indonesia Stock Exchange
Bursa Efek Indonesia

- 2) Data yang bersifat sensitif atau bersifat rahasia harus tersimpan dalam keadaan terenkripsi, sebagai contoh data yang menyangkut identitas Nasabah atau PIN / *password*.
- 3) Data rahasia seperti PIN / *password* tidak boleh dicatat di *audit trail*.

l. Penghindaran Kebocoran Aplikasi

Aplikasi tidak menggunakan *cookies* atau *file* sementara yang dimanfaatkan untuk menyimpan data yang bersifat rahasia seperti *password*.

m. Pengendalian terhadap Kerawanan Teknis

- 1) Anggota Bursa Efek harus melakukan *vulnerability assessment* dan menindaklanjuti dengan cara menutup celah-celah kerawanan yang ditemukan. Selain itu Anggota Bursa Efek disarankan untuk melaksanakan evaluasi keamanan sistem dengan cara melakukan *penetration test*, serta dilanjutkan dengan menindaklanjuti hasil dari *penetration test* tersebut
 - 2) Aspek-aspek yang perlu diuji di dalam pelaksanaan *vulnerability assessment* dan *penetration test* antara lain perimeter jaringan, *operating system*, *web server*, *database server* serta server-server penunjang lainnya, perangkat jaringan dan aplikasi.
 - 3) Menerapkan *patch* secara berkelanjutan terhadap komponen-komponen sistem seperti aplikasi, *operating system*, server, perangkat keamanan dan perangkat komunikasi.
 - 4) Anggota Bursa Efek perlu melakukan program pemberian kepedulian (*awareness*) mengenai keamanan sistem kepada Nasabah.
3. Anggota Bursa Efek harus meminta persetujuan ke Bursa terkait dengan *Strategic Order Management* sebelum mengimplementasikan Fasilitas Penyampaian Pesanan Secara Langsung bagi Nasabah (misalnya Anggota Bursa Efek ingin menerapkan *algorithmic trading*).
4. Surat Edaran ini merupakan satu kesatuan dengan ketentuan yang ditetapkan dalam Peraturan Nomor III-A tentang Keanggotaan Bursa yang harus dipenuhi oleh Anggota Bursa Efek yang akan menyelenggarakan Fasilitas Penyampaian Pesanan Secara Langsung Bagi Nasabah.



Indonesia Stock Exchange
Bursa Efek Indonesia

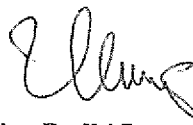
Surat Edaran ini efektif diberlakukan mulai tanggal dikeluarkan.

Ditetapkan di : Jakarta
Pada tanggal : 11 Oktober 2011

PT Bursa Efek Indonesia


Ito Warsito
Direktur Utama




Uriep Budhi Prasetyo
Direktur

Tembusan Yth.:

1. Ketua Badan Pengawas Pasar Modal dan Lembaga Keuangan (Bapepam dan LK)
2. Kepala Biro Transaksi dan Lembaga Efek, Bapepam dan LK
3. Kepala Biro Perundang-undangan dan Bantuan Hukum, Bapepam LK
4. Asosiasi Emiten Indonesia
5. Asosiasi Perusahaan Efek Indonesia
6. Asosiasi Bank Kustodian Indonesia
7. Asosiasi Biro Administrasi Efek
8. Direksi PT Kliring Penjaminan Efek Indonesia
9. Direksi PT Kustodian Sentral Efek Indonesia
10. Pusat Referensi Pasar Modal
11. Dewan Komisaris PT Bursa Efek Indonesia

