

LAMPIRAN IA
PERATURAN ANGGOTA DEWAN GUBERNUR
NOMOR 14 TAHUN 2025
TANGGAL 30 JUNI 2025
TENTANG
PERUBAHAN KEDUA PERATURAN ANGGOTA
DEWAN GUBERNUR NOMOR 17 TAHUN
2023 TENTANG PENYELENGGARAAN BANK
INDONESIA-FAST PAYMENT

**PERSYARATAN TEKNIS MINIMUM
PROTEKSI INFRASTRUKTUR TEKNOLOGI INFORMASI BI-FAST**

Dalam rangka menerapkan pengamanan sistem informasi BI-FAST, Peserta dan calon Peserta BI-FAST wajib memenuhi persyaratan teknis minimum proteksi infrastruktur teknologi informasi untuk BI-FAST. Persyaratan teknis tersebut dikelompokkan dalam beberapa kategori pengamanan berlapis dan dapat diperketat oleh Peserta sesuai kebijakan internal, sepanjang tidak bertentangan dengan ketentuan Bank Indonesia.

A. PENGAMANAN SEGMENTASI JARINGAN DAN ARSITEKTUR

1. Peserta melakukan pemisahan jaringan ke dalam segmen BI-FAST *production*, BI-FAST LAN, *management*, dan *monitoring*.
2. Peserta melakukan pemisahan segmen *server* BI-FAST dari segmen non BI-FAST dan dibatasi dengan *firewall*, termasuk *middleware* dan *core banking system*.
3. Perangkat *server* diproteksi dengan *Endpoint Detection and Response* (EDR)/*Extended Detection and Response* (XDR) sesuai dengan matriks *software compatibility* yang berjalan di *server* tersebut. Mekanisme pembaruan maupun pengiriman *log* hasil dari EDR/XDR ke server pusat dan/atau manajemen EDR/XDR dilakukan melalui *broker*.
4. Peserta menyusun dokumen topologi jaringan dan melakukan pemutakhiran dokumen setiap kali dilakukan perubahan atas topologi jaringan. Dokumentasi topologi jaringan paling sedikit mencakup segmen, alamat IP, nomor *port*, serta diagram konektivitas antar komponen BI FAST dan komponen lain yang terhubung.
5. *Server* BI-FAST *production* tidak boleh terhubung dari/ke sambungan jaringan internet. Dalam hal dibutuhkan jaringan internet untuk pembaruan perangkat lunak dapat menggunakan perangkat *server* lain yang mempunyai segmen terpisah dan berlaku sebagai *server repository*.

B. PENGAMANAN AKSES JARAK JAUH DAN ADMINISTRASI

1. Akses administrator ke seluruh komponen BI-FAST hanya dapat dilaksanakan melalui *Privileged Access Management* (PAM) atau *jump server* yang memiliki kemampuan perekaman aktivitas dan *Multi Factor Authentication* (MFA).
2. PAM atau *jump server* harus berada pada segmen jaringan tersendiri dengan alamat IP, nomor *port*, dan protokol khusus sebagaimana telah didokumentasikan pada dokumen topologi jaringan.
3. Akses *Secure Shell* (SSH) hanya diperbolehkan dari alamat IP terdaftar oleh pengguna berwenang.
4. Akses terhadap komponen BI-FAST maupun PAM/*jump server* hanya diperbolehkan menggunakan akun khusus yang berbeda dari akun pegawai Peserta.

5. Dalam hal PAM belum tersedia, akses administrator dapat dilaksanakan melalui *jump server* dengan menggunakan akun khusus yang berbeda dari akun administrator pada target sistem.

C. PENGATURAN KONEKSI ANTAR SISTEM

1. BI-FAST *Connector* hanya diperbolehkan untuk:
 - a. melakukan koneksi dengan *middleware* atau *Core Banking System* (CBS) Peserta melalui protokol *Hypertext Transfer Protocol Secure* (HTTPS) atau *Transmission Control Protocol* (TCP)/*Internet Protocol* (IP).
 - b. melakukan koneksi dengan BI-FAST melalui protokol HTTPS.
 - c. melakukan koneksi dengan *platform manager* dan *config builder* melalui protokol TCP/IP sesuai *port* yang telah ditetapkan oleh Penyelenggara.
 - d. melakukan koneksi dengan *service monitoring* dan *security monitoring* sesuai alamat IP, nomor *port*, protokol, dan/atau URL yang telah didokumentasikan pada dokumen topologi jaringan.
2. *Hardware Security Module* (HSM) hanya diperbolehkan melakukan koneksi dengan BI-FAST *Connector*, *service monitoring*, dan *security monitoring* sesuai alamat IP, nomor *port*, dan protokol yang telah didokumentasikan pada dokumen topologi jaringan.
3. *Database* hanya diperbolehkan melakukan koneksi dengan BI-FAST *Connector*, *service monitoring*, dan *security monitoring* sesuai alamat IP, nomor *port*, dan protokol yang telah didokumentasikan pada dokumen topologi jaringan.
4. *Control Server*/APSF hanya diperbolehkan melakukan koneksi dengan *platform manager & config builder*, *service monitoring*, dan *security monitoring*.
5. *Workstation* yang terinstalasi *platform manager & config builder* hanya diperbolehkan untuk:
 - a. melakukan koneksi dengan BI-FAST *Connector*;
 - b. melakukan koneksi dengan *control server*/APSF; dan
 - c. melakukan koneksi dengan *service monitoring* dan *security monitoring* sesuai alamat IP, nomor *port*, protokol, dan/atau URL yang telah didokumentasikan pada dokumen topologi jaringan.

D. KRIPTOGRAFI DAN MANAJEMEN KUNCI

1. Seluruh komunikasi antara BI-FAST *Connector* dengan *middleware* atau CBS Peserta dan BI-FAST *Connector* dengan BI-FAST *Hub* menggunakan protokol TLS dengan versi paling rendah yang ditetapkan oleh Penyelenggara dan algoritma kriptografi yang sesuai dengan standar keamanan terkini.
2. *Private key* untuk *message signing* antara BI-FAST *Connector* dengan BI-FAST, BI-FAST *Connector* dengan *middleware* atau CBS Peserta dan sertifikat disimpan di dalam HSM.

E. PENGENDALIAN AKSES DAN AUTENTIKASI

1. Peserta melakukan penyusunan *User Access Matrix* (UAM) untuk seluruh lapisan sistem (*Virtual Machine* (VM), *Operating System* (OS), aplikasi, dan *database*) berdasarkan prinsip *least privilege*.
2. UAM ditinjau paling sedikit 1 (satu) kali dalam 1 (satu) tahun atau setiap terjadi perubahan peran.
3. Peserta menonaktifkan atau menghapus akun serta layanan yang tidak digunakan, serta mengganti seluruh kata sandi bawaan.

4. Kebijakan kata sandi mencakup kompleksitas, masa berlaku, mekanisme penguncian setelah percobaan gagal, dan penyimpanan aman menggunakan algoritma *hashing* modern.
5. Peserta mengaktifkan IP *whitelist*, *message signing*, dan menonaktifkan rute komunikasi yang tidak digunakan.

F. PEMUTAKHIRAN, KERENTANAN, DAN MANAJEMEN PERUBAHAN

1. *Hypervisor*, sistem operasi, *firmware*, dan perangkat lunak BI-FAST diperbarui dengan *security patch* terbaru.
2. Penerapan pembaruan keamanan hanya dapat dilakukan setelah pengujian di lingkungan pengembangan dengan fokus pada temuan berisiko tinggi dan kritis.
3. Peserta melaksanakan *vulnerability scanning* paling sedikit 1 (satu) kali dalam 1 (satu) tahun atau setiap terjadi perubahan signifikan pada lingkungan sistem.
4. Pengujian keamanan (*penetration test*) dilakukan paling sedikit 1 (satu) kali dalam 1 (satu) tahun atau setiap terjadi perubahan signifikan pada lingkungan sistem oleh auditor independen eksternal.

G. PENCATATAN DAN PEMANTAUAN LOG

1. Waktu pada seluruh sistem operasi disinkronkan dengan *Network Time Protocol* (NTP) guna memastikan korelasi antar *log*.
2. Peserta mengumpulkan *log* dari seluruh komponen BI-FAST ke perangkat pengumpul *log* (*log collector*) dan memastikan *log* tidak dapat diubah dan/atau dihapus serta melakukan pencadangan *log* secara berkala.
3. Perangkat dan perangkat lunak pemantauan hanya dapat diakses oleh pengguna berwenang melalui alamat IP, nomor *port*, dan/atau URL yang telah didaftarkan, serta diperbarui secara berkala.

H. KEAMANAN PIHAK KETIGA

1. Akses ke *server* oleh penyedia jasa pihak ketiga hanya dapat dilakukan setelah memperoleh persetujuan pejabat internal yang berwenang.
2. Riwayat aktivitas pihak ketiga disimpan paling singkat 3 (tiga) bulan dan diverifikasi secara berkala.
3. Peserta membatasi hak akses pihak ketiga sebatas kebutuhan operasional paling minimum.
4. Peserta memberikan pelatihan kesadaran keamanan secara rutin kepada personel operasional BI-FAST.
5. Setiap pegawai pihak ketiga yang menangani BI-FAST menandatangani Perjanjian Kerahasiaan atau *Non Disclosure Agreement* (NDA) sesuai ketentuan peraturan perundang-undangan.

I. KEAMANAN FISIK DAN LINGKUNGAN

1. HSM dan *server* BI-FAST ditempatkan di pusat data atau ruangan terkunci yang dilengkapi sistem pengawasan video berupa *Closed Circuit Television* (CCTV) serta pengendalian akses fisik.
2. Akses fisik hanya diberikan kepada pegawai dan pengunjung yang telah memperoleh otorisasi.

ANGGOTA DEWAN GUBERNUR,

TTD

FILIANINGSIH HENDARTA