JAKSA AGUNG
REPUBLIK INDONESIA

PEDOMAN

NOMOR 9 TAHUN 2024

TENTANG

PERUBAHAN ATAS PEDOMAN NOMOR 3 TAHUN 2023 TENTANG SISTEM MANAJEMEN KEAMANAN INFORMASI SERTA STANDAR TEKNIS DAN PROSEDUR KEAMANAN SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DI LINGKUNGAN KEJAKSAAN REPUBLIK INDONESIA

A. Latar Belakang

Adanya implementasi kebijakan internal, tata kelola, dan layanan sistem pemerintahan berbasis elektronik yang didukung dengan sistem manajemen keamanan informasi serta standar teknis dan prosedur keamanan sistem pemerintahan berbasis elektronik yang mampu melindungi sumber daya terkait data dan informasi, infrastruktur, dan aplikasi sistem pemerintahan berbasis elektronik dari berbagai bentuk ancaman keamanan informasi akan menambah keunggulan penerapan sistem pemerintahan berbasis elektronik di lingkungan Kejaksaan Republik Indonesia.

Untuk melaksanakan rekomendasi dari Kementerian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi dalam Laporan Hasil Evaluasi Sistem Pemerintahan Berbasis Elektronik Kejaksaan Agung Tahun 2023 dan mengoptimalkan sistem manajemen keamanan informasi serta standar teknis dan prosedur keamanan sistem pemerintahan berbasis elektronik di lingkungan Kejaksaan Republik Indonesia maka perlu menetapkan Pedoman tentang Perubahan atas Pedoman Nomor 3 Tahun 2023 tentang Sistem Manajemen Keamanan Informasi serta Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik di Lingkungan Kejaksaan Republik Indonesia.

B. Maksud dan Tujuan

1. Maksud

Pedoman ini dimaksudkan sebagai acuan dan merupakan bagian yang tidak terpisahkan dalam melaksanakan sistem manajemen keamanan

informasi serta standar teknis dan prosedur keamanan sistem pemerintahan berbasis elektronik di lingkungan Kejaksaan Republik Indonesia.

2. Tujuan

Pedoman ini bertujuan untuk mengoptimalkan pelaksanaan sistem manajemen keamanan informasi serta standar teknis dan prosedur keamanan sistem pemerintahan berbasis elektronik di lingkungan Kejaksaan Republik Indonesia.

C. Ruang Lingkup

Ruang lingkup Pedoman ini meliputi perubahan ketentuan mengenai keamanan aplikasi sistem pemerintahan berbasis elektronik dan keamanan jaringan intra dalam sistem manajemen keamanan informasi sistem pemerintahan berbasis elektronik serta standar teknis dan prosedur keamanan sistem pemerintahan berbasis elektronik.

D. Dasar Hukum

1. Undang-Undang Nomor 16 Tahun 2004 tentang Kejaksaan Republik Indonesia (Lembaran Negara Republik Indonesia Tahun 2004 Nomor 67, Tambahan Lembaran Negara Republik Indonesia Nomor 4401) sebagaimana telah diubah dengan Undang-Undang Nomor 11 Tahun 2021 tentang Perubahan atas Undang Undang Nomor 16 Tahun 2004 tentang Kejaksaan Republik Indonesia (Lembaran Negara Republik Indonesia Tahun 2021 Nomor 298, Tambahan Lembaran Negara Republik Indonesia Nomor 6755);
2. Peraturan Presiden Nomor 38 Tahun 2010 tentang Organisasi dan Tata Kerja Kejaksaan Republik Indonesia sebagaimana telah beberapa kali diubah terakhir dengan Peraturan Presiden Nomor 15 Tahun 2024 tentang Perubahan Ketiga atas Peraturan Presiden Nomor 38 Tahun 2010 tentang Organisasi dan Tata Kerja Kejaksaan Republik Indonesia (Lembaran Negara Republik Indonesia Tahun 2024 Nomor 28);
3. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintah Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
4. Peraturan Presiden Nomor 132 Tahun 2022 tentang Arsitektur Sistem Pemerintah Berbasis Elektronik Nasional (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 233);

5. Peraturan Jaksa Agung Nomor PER-006/A/JA/07/2017 tentang Organisasi dan Tata Kerja Kejaksaan Republik Indonesia (Berita Negara Republik Indonesia Tahun 2017 Nomor 1069) sebagaimana telah beberapa kali diubah terakhir dengan Peraturan Kejaksaan Nomor 3 Tahun 2024 tentang Perubahan Keempat atas Peraturan Jaksa Agung Nomor PER-006/A/JA/07/2017 tentang Organisasi dan Tata Kerja Kejaksaan Republik Indonesia (Berita Negara Republik Indonesia Tahun 2024 Nomor 448);
6. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 59 Tahun 2020 tentang Pemantauan dan Evaluasi Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2020 Nomor 994);
7. Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2021 Nomor 541);
8. Pedoman Jaksa Agung Nomor 4 Tahun 2022 tentang Sistem Pemerintahan Berbasis Elektronik di Lingkungan Kejaksaan Republik Indonesia;
9. Pedoman Jaksa Agung Nomor 3 Tahun 2023 tentang Sistem Manajemen Keamanan Informasi serta Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik di Lingkungan Kejaksaan Republik Indonesia.

E. Perubahan

Beberapa ketentuan dalam Pedoman Jaksa Agung Nomor 3 Tahun 2023 tentang Sistem Manajemen Keamanan Informasi serta Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik di Lingkungan Kejaksaan Republik Indonesia diubah sebagai berikut:

I. Ketentuan Huruf C angka 6 dan angka 13 dalam BAB III diubah sehingga berbunyi sebagai berikut:

C. Keamanan Aplikasi SPBE

1. Standar teknis dan prosedur keamanan Aplikasi SPBE diterapkan pada:
   a. aplikasi berbasis *web*; dan
   b. aplikasi berbasis *mobile*.

2. Aplikasi berbasis *web* sebagaimana dimaksud pada angka 1 huruf a merupakan aplikasi yang diakses melalui peramban saat terhubung dengan koneksi internet atau intranet.
3. Aplikasi berbasis *mobile* sebagaimana dimaksud pada angka 1 huruf b merupakan aplikasi yang dalam pengoperasiannya dapat berjalan di perangkat bergerak dan memiliki sistem operasi yang mendukung perangkat lunak secara *standalone*.
4. Aplikasi SPBE harus dilakukan pengujian keamanan setiap periode tertentu yang dilakukan dengan:
   a. mengidentifikasi persyaratan minimum keamanan yang belum diterapkan;
   b. memastikan pengodean pemrograman aplikasi yang dibuat tidak memiliki kerawanan;
   c. melakukan pemindaian otomatis dan/atau pengujian penetrasi sistem;
   d. mengidentifikasi kerentanan dan mengelola ancaman sejak awal siklus pengembangan Aplikasi SPBE; dan
   e. menganalisis kerentanan.
5. Standar teknis keamanan aplikasi berbasis *web* sebagaimana dimaksud pada angka 1 huruf a terdiri atas terpenuhinya fungsi:
   a. autentikasi;
   b. manajemen sesi;
   c. persyaratan kontrol akses;
   d. validasi input;
   e. kriptografi pada verifikasi statis;
   f. penanganan eror dan pencatatan log;
   g. proteksi data;
   h. keamanan komunikasi;
   i. pengendalian kode berbahaya;
   j. logika bisnis;
   k. *file*;
   l. keamanan API dan *web service*; dan
   m. keamanan konfigurasi.
6. Terpenuhinya fungsi autentikasi sebagaimana dimaksud pada angka 5 huruf a dilakukan dengan prosedur:

a. menggunakan manajemen kata sandi untuk proses autentikasi;
b. menerapkan verifikasi kata sandi pada sisi *server*;
c. mengatur jumlah karakter minimal 8 (delapan) karakter menggunakan angka, simbol, dan kapital serta mengatur masa berlaku dari kata sandi;
d. mengatur jumlah maksimum kesalahan dalam pemasukan kata sandi;
e. mengatur mekanisme pemulihan kata sandi;
f. menjaga kerahasiaan kata sandi yang disimpan melalui mekanisme kriptografi;
g. menggunakan jalur komunikasi yang diamankan untuk proses autentikasi;
h. menerapkan kontrol anti otomatisasi minimal menggunakan *captcha*; dan
i. memiliki fungsi autentikasi tambahan seperti 2fa/mfa yang dapat diaktifkan secara opsional.

7. Terpenuhinya fungsi manajemen sesi sebagaimana dimaksud pada angka 5 huruf b dilakukan dengan prosedur:
   a. menggunakan pengendali sesi untuk proses manajemen sesi;
   b. menggunakan pengendali sesi yang disediakan oleh kerangka kerja aplikasi;
   c. mengatur pembuatan dan keacakan token sesi yang dihasilkan oleh pengendali sesi;
   d. mengatur kondisi dan jangka waktu habis sesi;
   e. validasi dan pencantuman *session id;*
   f. pelindungan terhadap lokasi dan pengiriman token untuk sesi terautentikasi; dan
   g. pelindungan terhadap duplikasi dan mekanisme persetujuan pengguna.
8. Terpenuhinya fungsi persyaratan kontrol akses sebagaimana dimaksud pada angka 5 huruf c dilakukan dengan prosedur:
   a. menetapkan otorisasi pengguna untuk membatasi kontrol akses;
   b. mengatur peringatan terhadap bahaya serangan otomatis apabila terjadi akses yang bersamaan atau

akses yang terus-menerus pada fungsi;

c. mengatur antarmuka pada sisi administrator; dan

d. mengatur verifikasi kebenaran token ketika mengakses data dan informasi yang dikecualikan.

9. Terpenuhinya fungsi validasi input sebagaimana dimaksud pada angka 5 huruf d dilakukan dengan prosedur:

a. menerapkan fungsi validasi input pada sisi *server*;

b. menerapkan mekanisme penolakan input jika terjadi kesalahan validasi;

c. memastikan *runtime environment* aplikasi tidak rentan terhadap serangan validasi input;

d. melakukan validasi positif pada seluruh input;

e. melakukan filter terhadap data yang tidak dipercaya;

f. menggunakan fitur kode dinamis;

g. melakukan pelindungan terhadap akses yang mengandung konten skrip; dan

h. melakukan pelindungan dari serangan injeksi basis data.

10. Terpenuhinya fungsi kriptografi pada verifikasi statis sebagaimana dimaksud pada angka 5 huruf e dilakukan dengan prosedur:

a. menggunakan algoritma kriptografi, modul kriptografi, protokol kriptografi, dan kunci kriptografi sesuai dengan ketentuan peraturan perundang undangan;

b. melakukan autentikasi data yang dienkripsi;

c. menerapkan manajemen kunci kriptografi; dan

d. membuat angka acak yang menggunakan generator angka acak kriptografi.

11. Terpenuhinya fungsi penanganan eror dan pencatatan log sebagaimana dimaksud pada angka 5 huruf f dilakukan dengan prosedur:

a. mengatur konten pesan yang ditampilkan ketika terjadi kesalahan;

b. menggunakan metode penanganan eror untuk mencegah kesalahan terprediksi dan tidak terduga serta menangani seluruh pengecualian yang tidak ditangani;

c. tidak mencantumkan informasi yang dikecualikan

dalam pencatatan log;

d. mengatur cakupan log yang dicatat untuk mendukung upaya penyelidikan ketika terjadi insiden;
e. mengatur pelindungan log aplikasi dari akses dan modifikasi yang tidak sah;
f. melakukan enkripsi pada data yang disimpan untuk mencegah injeksi log; dan
g. melakukan sinkronisasi sumber waktu sesuai dengan zona waktu dan waktu yang benar.

12. Terpenuhinya fungsi proteksi data sebagaimana dimaksud pada angka 5 huruf g dilakukan dengan prosedur:
    a. melakukan identifikasi dan penyimpanan salinan informasi yang dikecualikan;
    b. melakukan pelindungan dari akses yang tidak sah terhadap informasi yang dikecualikan yang disimpan sementara dalam aplikasi;
    c. melakukan pertukaran, penghapusan, dan audit informasi yang dikecualikan;
    d. melakukan penentuan jumlah parameter;
    e. memastikan data disimpan dengan aman;
    f. menentukan metode untuk menghapus dan mengekspor data sesuai permintaan pengguna; dan
    g. membersihkan memori setelah tidak diperlukan.
13. Terpenuhinya fungsi keamanan komunikasi sebagaimana dimaksud pada angka 5 huruf h dilakukan dengan prosedur:
    a. menggunakan komunikasi terenkripsi;
    b. mengatur koneksi masuk dan keluar yang aman dan terenkripsi dari sisi pengguna;
    c. mengatur jenis algoritma yang digunakan dan alat pengujiannya;
    d. mengatur aktivasi dan konfigurasi sertifikat elektronik yang diterbitkan oleh penyelenggara sertifikasi elektronik; dan
    e. menggunakan domain dan subdomain resmi Kejaksaan yang telah terdaftar (kejaksaan.go.id) untuk aplikasi yang diakses menggunakan jaringan internet publik sebagai upaya menghindari *phising* dan serangan

lainnya;

f. memastikan keamanan dan integritas data, seluruh aplikasi *web* yang menggunakan subdomain *.kejaksaan.go.id diharuskan menjalani penilaian kerentanan (*vulnerability assessment*) atau pengujian penetrasi (*penetration testing*) minimal sekali dalam setahun, hasil penilaian terakhir harus menunjukkan bahwa aplikasi tersebut telah diuji dalam jangka waktu 6 (enam) sampai dengan 12 (dua belas) bulan terakhir;

g. memastikan hasil penilaian kerentanan (*vulnerability assessment*) atau pengujian penetrasi (*penetration testing*) aplikasi *web* yang menggunakan subdomain *.kejaksaan.go.id tidak memiliki tingkat kerentanan yang tinggi (*high*) maupun tingkat kerentanan kritis (*critical*);

h. menonaktifkan registrasi dns untuk aplikasi *web* yang menggunakan subdomain *.kejaksaan.go.id yang belum melakukan dan melampirkan hasil penilaian kerentanan (*vulnerability assessment*) atau pengujian penetrasi (*penetration testing*) atau hasil penilaiannya memiliki kerentanan yang tinggi (*high*) maupun tingkat kerentanan kritis (*critical*); dan

i. registrasi dns untuk aplikasi *web* yang menggunakan subdomain *.kejaksaan.go.id dapat diaktifkan kembali setelah melampirkan hasil penilaian kerentanan (*vulnerability assessment*) atau pengujian penetrasi (*penetration testing*) dengan tingkat kerentanan yang tidak memiliki kerentanan yang tinggi (*high*) maupun tingkat kerentanan kritis (*critical*).

14. Terpenuhinya fungsi pengendalian kode berbahaya sebagaimana dimaksud pada angka 5 huruf i dilakukan dengan prosedur:

a. menggunakan analisis kode dalam kontrol kode berbahaya;

b. memastikan kode sumber aplikasi dan pustaka tidak mengandung kode berbahaya dan fungsionalitas lain yang tidak diinginkan;

c. mengatur izin terkait fitur atau sensor terkait privasi;
d. mengatur pelindungan integritas; dan
e. mengatur mekanisme fitur pembaruan.

15. Terpenuhinya fungsi logika bisnis sebagaimana dimaksud pada angka 5 huruf j dilakukan dengan prosedur:
    a. memproses alur logika bisnis dalam urutan langkah dan waktu yang realistis;
    b. memastikan logika bisnis memiliki batasan dan validasi;
    c. memonitor aktivitas yang tidak biasa;
    d. membantu dalam kontrol anti otomatisasi; dan
    e. memberikan peringatan ketika terjadi serangan otomatis atau aktivitas yang tidak biasa.
16. Terpenuhinya fungsi *file* sebagaimana dimaksud pada angka 5 huruf k dilakukan dengan prosedur:
    a. mengatur jumlah *file* untuk setiap pengguna dan kuota ukuran *file* yang diunggah;
    b. melakukan validasi *file* sesuai dengan tipe konten yang diharapkan;
    c. melakukan pelindungan terhadap metadata input dan metadata *file*;
    d. melakukan pemindaian *file* yang diperoleh dari sumber yang tidak dipercaya; dan
    e. melakukan konfigurasi *server* untuk mengunduh *file* sesuai ekstensi yang ditentukan.
17. Terpenuhinya fungsi keamanan API dan *web service* sebagaimana dimaksud pada angka 5 huruf l dilakukan dengan prosedur:
    a. melakukan konfigurasi layanan *web*;
    b. memverifikasi *uniform resource identifier* API tidak menampilkan informasi yang berpotensi sebagai celah keamanan;
    c. membuat keputusan otorisasi;
    d. menampilkan metode *RESTful hypertext transfer protocol* apabila input pengguna dinyatakan valid;
    e. menggunakan validasi skema dan verifikasi sebelum menerima input;
    f. menggunakan metode pelindungan layanan berbasis

web; dan

g. menerapkan kontrol anti otomatisasi.

18. Terpenuhinya fungsi keamanan konfigurasi sebagaimana dimaksud pada angka 5 huruf m dilakukan dengan prosedur:
    a. mengkonfigurasi *server* sesuai rekomendasi *server* aplikasi dan kerangka kerja aplikasi yang digunakan;
    b. mendokumentasi, menyalin konfigurasi, dan semua dependensi;
    c. menghapus fitur, dokumentasi, sampel, dan konfigurasi yang tidak diperlukan;
    d. memvalidasi integritas aset jika aset aplikasi diakses secara eksternal; dan
    e. menggunakan respon aplikasi dan konten yang aman.
19. Standar teknis keamanan aplikasi berbasis *mobile* sebagaimana dimaksud pada angka 1 huruf b terdiri atas terpenuhinya fungsi:
    a. penyimpanan data dan persyaratan privasi;
    b. kriptografi;
    c. autentikasi dan manajemen sesi;
    d. komunikasi jaringan;
    e. interaksi *platform*;
    f. kualitas kode dan pengaturan *build*; dan
    g. ketahanan.
20. Terpenuhinya fungsi penyimpanan data dan persyaratan privasi sebagaimana dimaksud pada angka 19 huruf a dilakukan dengan prosedur:
    a. menyimpan seluruh data dan informasi yang dikecualikan hanya dalam fasilitas penyimpanan kredensial sistem;
    b. membatasi pertukaran data dan informasi yang dikecualikan dengan *third party*;
    c. menonaktifkan *cache keyboard* pada saat memasukkan data dan informasi yang dikecualikan;
    d. melindungi informasi yang dikecualikan saat terjadi *inter process communication*; dan
    e. melindungi data dan informasi yang dikecualikan yang

dimasukkan melalui antarmuka pengguna.

21. Terpenuhinya fungsi kriptografi sebagaimana dimaksud pada angka 19 huruf b dilakukan dengan prosedur:
    a. menghindari penggunaan kriptografi simetrik dengan *hardcoded key;*
    b. mengimplementasikan metode kriptografi yang sudah teruji sesuai kebutuhan;
    c. menghindari penggunaan protokol kriptografi atau algoritma kriptografi yang obsolet;
    d. menghindari penggunaan kunci kriptografi yang sama; dan
    e. menggunakan pembangkit kunci acak yang memenuhi kriteria keacakan kunci.
22. Terpenuhinya fungsi autentikasi dan manajemen sesi sebagaimana dimaksud pada angka 19 huruf c dilakukan dengan prosedur:
    a. menerapkan autentikasi pada *remote endpoint* terhadap aplikasi yang menyediakan akses pengguna untuk layanan jarak jauh;
    b. menggunakan *session identifier* yang acak tanpa perlu mengirimkan kredensial pengguna apabila menggunakan *stateful* manajemen sesi;
    c. memastikan *server* menyediakan token yang telah ditandatangani menggunakan algoritma yang aman apabila menggunakan autentikasi *stateless* berbasis token;
    d. memastikan *remote endpoint* memutus sesi yang ada saat pengguna *log out*;
    e. menerapkan pengaturan sandi pada *remote endpoint;*
    f. membatasi jumlah percobaan *log in* pada *remote endpoint*;
    g. menentukan masa berlaku sesi dan masa kedaluwarsa token pada *remote endpoint*; dan
    h. melakukan otorisasi pada *remote endpoint.*
23. Terpenuhinya fungsi komunikasi jaringan sebagaimana dimaksud pada angka 19 huruf d dilakukan dengan prosedur:

a. menerapkan *secure socket layer* atau *transport layer security* yang tidak obsolet secara konsisten; dan
b. memverifikasi sertifikat *remote endpoint.*

24. Terpenuhinya fungsi interaksi *platform* sebagaimana dimaksud pada angka 19 huruf e dilakukan dengan prosedur:
    a. memastikan aplikasi hanya meminta akses terhadap sumber daya yang diperlukan;
    b. melakukan validasi terhadap seluruh input dari sumber eksternal dan pengguna;
    c. menghindari pengiriman fungsionalitas sensitif melalui skema *custom uniform resource locator* dan fasilitas *inter process communication*;
    d. menghindari penggunaan *JavaScript* dalam *WebView*;
    e. menggunakan protokol *hypertext transfer protocol secure* pada *WebView*; dan
    f. mengimplementasikan penggunaan serialisasi API yang aman.
25. Terpenuhinya fungsi kualitas kode dan pengaturan *build* sebagaimana dimaksud pada angka 19 huruf f dilakukan dengan prosedur:
    a. menandatangani aplikasi dengan sertifikat yang valid;
    b. memastikan aplikasi dalam mode rilis;
    c. menghapus simbol *debugging* dari *native binary*;
    d. menghapus kode *debugging* dan kode bantuan pengembang;
    e. mengidentifikasi kelemahan seluruh komponen *third party*;
    f. menentukan mekanisme penanganan eror;
    g. mengelola memori secara aman; dan
    h. mengaktifkan fitur keamanan yang tersedia.
26. Terpenuhinya fungsi ketahanan sebagaimana dimaksud pada angka 19 huruf g dilakukan dengan prosedur:
    a. mencegah aplikasi berjalan pada perangkat yang telah dilakukan modifikasi yang tidak sah;
    b. mendeteksi dan merespons *debugger*;
    c. mencegah *executable file* melakukan perubahan pada

sumber daya perangkat;

d. mendeteksi dan merespons keberadaan perangkat *reverse engineering*;

e. mencegah aplikasi berjalan dalam *emulator*;

f. mendeteksi perubahan kode dan data di ruang memori;

g. menerapkan fungsi *device binding* dengan menggunakan *property* unik pada perangkat;

h. melindungi seluruh *file* dan *library* pada aplikasi; dan

i. menerapkan metode *obfuscation*.

II. Ketentuan Huruf E angka 5 dan angka 7 dalam BAB III diubah sehingga berbunyi sebagai berikut:

E. Keamanan Jaringan Intra

1. Standar teknis keamanan Jaringan Intra diterapkan pada:
   a. Jaringan Intra pemerintah; dan
   b. Jaringan Intra seluruh satuan kerja Kejaksaan.
2. Standar teknis keamanan Jaringan Intra sebagaimana dimaksud pada angka 1 terdiri atas terpenuhinya:
   a. aspek administrasi keamanan Jaringan Intra;
   b. kontrol akses dan autentikasi;
   c. persyaratan perangkat dan aplikasi keamanan Jaringan Intra;
   d. kontrol keamanan *gateway*;
   e. kontrol keamanan *access point* pada jaringan nirkabel; dan
   f. kontrol konfigurasi *access point* pada jaringan nirkabel.
3. Terpenuhinya aspek administrasi keamanan Jaringan Intra sebagaimana dimaksud pada angka 2 huruf a dilakukan dengan prosedur:
   a. menyusun dan mengevaluasi dokumen arsitektur Jaringan Intra;
   b. mengidentifikasi seluruh aset infrastruktur jaringan;
   c. menyusun dan menetapkan standar operasional prosedur terkait pemeliharaan keamanan Jaringan Intra; dan
   d. membuat laporan pengawasan keamanan jaringan secara periodik.

4. Terpenuhinya kontrol akses dan autentikasi sebagaimana dimaksud pada 2 huruf b dilakukan dengan prosedur:
   a. menempatkan perangkat infrastruktur jaringan yang menyediakan layanan Jaringan Intra pada zona terpisah;
   b. menggunakan autentikasi untuk mengakses Jaringan Intra;
   c. menerapkan pembatasan akses dalam Jaringan Intra;
   d. mematikan atau membatasi *protocol*, *port*, dan layanan yang tidak digunakan;
   e. menerapkan penyaringan tautan dan memblokir akses ke situs berbahaya;
   f. menerapkan fungsi *honeypot* untuk menganalisis celah keamanan berdasarkan jenis serangan;
   g. menerapkan *virtual private network* dan mengaktifkan fungsi enkripsi pada jalur komunikasi yang digunakan;
   h. memberikan kewenangan hanya kepada administrator untuk menginstal perangkat lunak dan/atau mengubah konfigurasi sistem dalam Jaringan Intra;
   i. menerapkan *secure endpoints*;
   j. memblokir layanan yang tidak dikenal;
   k. menerapkan *secure socket layer* atau *transport layer security* versi terkini pada jalur akses Jaringan Intra; dan
   l. menerapkan *server* perantara saat *client* mengakses *server database* dalam rangka pemeliharaan.
5. Terpenuhinya persyaratan perangkat dan aplikasi keamanan Jaringan Intra sebagaimana dimaksud pada angka 2 huruf c dilakukan dengan prosedur:
   a. menggunakan perangkat *security information and event management* (SIEM) untuk *network logging* dan *monitoring*;
   b. menerapkan sistem deteksi dini kerentanan keamanan perangkat jaringan;
   c. menggunakan perangkat *firewall*;
   d. menggunakan perangkat *intrusion detection systems* dan *intrusion prevention systems*;

e. menggunakan perangkat *Endpoint Detection and Response* (EDR), *Network Detection and Response* (NDR), dan *Extended Detection and Response* (XDR);
f. menerapkan *virtual private network* terenkripsi untuk penggunaan akses jarak jauh secara terbatas;
g. menerapkan kontrol *update patching* pada infrastruktur Jaringan Intra dan sistem komputer;
h. menggunakan perangkat *web application firewall*;
i. menggunakan perangkat *load balancer* untuk menjaga ketersediaan akses terhadap jaringan dan aplikasi;
j. memperbarui teknologi keamanan perangkat keras dan perangkat lunak untuk meminimalisasi celah peretas;
k. mengunduh perangkat lunak melalui *enterprise software distribution system*; dan
l. menerapkan sertifikat elektronik.

6. Terpenuhinya kontrol keamanan *gateway* sebagaimana dimaksud pada angka 2 huruf d dilakukan dengan prosedur:
   a. menerapkan *content filtering*;
   b. menerapkan *inspection packet filtering* untuk memeriksa paket yang masuk pada Jaringan Intra;
   c. menerapkan kontrol keamanan pada fitur akses jarak jauh perangkat *gateway*;
   d. memastikan perangkat *gateway* yang menghubungkan antar Jaringan Intra tidak terkoneksi langsung dengan jaringan publik;
   e. melaksanakan manajemen *traffic gateway*; dan
   f. memastikan *port* tidak dibuka secara *default*.
7. Terpenuhinya kontrol keamanan *access point* pada jaringan nirkabel sebagaimana dimaksud pada angka 2 huruf e dilakukan dengan prosedur:
   a. menerapkan protokol keamanan *access point* nirkabel dan teknologi enkripsi terkini;
   b. menerapkan *media access control* pada *address filtering*;
   c. menerapkan *dedicated service set identifier;*
   d. menerapkan pembatasan jangkauan radio transmisi dan pengguna jaringan;
   e. menerapkan pembatasan terkait penambahan

perangkat nirkabel yang dipasang secara tidak sah;

f. mengimplementasikan segmentasi jaringan nirkabel atau *Wireless Fidelity* (Wi-Fi) dengan menggunakan SSID yang berbeda untuk membedakan antara pengguna tamu dan pegawai, sehingga meningkatkan keamanan jaringan;

g. menerapkan manajemen *vulnerability* secara berkala dan berkelanjutan; dan

h. melakukan *patching firmware* secara rutin.

8. Terpenuhinya kontrol konfigurasi *access point* pada jaringan nirkabel sebagaimana dimaksud pada angka 2 huruf f dilakukan dengan prosedur:

a. menggunakan kata sandi yang kuat;

b. menggunakan protokol model *authentication authorization* dan *accounting* pada perangkat infrastruktur jaringan untuk *management user* atau otentikasi *administrator access point*;

c. memastikan fitur akses konfigurasi jarak jauh hanya dapat digunakan dalam kondisi darurat dengan menerapkan kontrol keamanan;

d. mengisolasi atau melakukan segmentasi jaringan area lokal nirkabel; dan

e. menonaktifkan antarmuka nirkabel, layanan, dan aplikasi yang tidak digunakan.

F. Penutup

Pedoman ini mulai berlaku sejak tanggal ditetapkan.

Ditetapkan di Jakarta
pada tanggal 24 Oktober 2024

JAKSA AGUNG REPUBLIK INDONESIA,

BURHANUDDIN

JAKSA AGUNG
REPUBLIK INDONESIA

PEDOMAN

NOMOR 3 TAHUN 2023

TENTANG

SISTEM MANAJEMEN KEAMANAN INFORMASI
SERTA STANDAR TEKNIS DAN PROSEDUR KEAMANAN
SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK
DI LINGKUNGAN KEJAKSAAN REPUBLIK INDONESIA

BAB I
PENDAHULUAN

A. Latar Belakang

Dalam rangka melindungi kerahasiaan (*confidentiality*), keutuhan (*integrity*), ketersediaan (*availability*), keaslian, dan kenirsangkalan (*non-repudiation*) sumber daya terkait data dan informasi, infrastruktur, dan aplikasi Sistem Pemerintahan Berbasis Elektronik dari berbagai bentuk ancaman keamanan informasi, perlu melakukan pengelolaan keamanan informasi di lingkungan Kejaksaan Republik Indonesia. Untuk keperluan dimaksud, perlu menetapkan Pedoman tentang Sistem Manajemen Keamanan Informasi serta Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik di Lingkungan Kejaksaan Republik Indonesia.

B. Maksud dan Tujuan

1. Maksud

   Pedoman ini dimaksudkan sebagai acuan dalam melaksanakan sistem manajemen keamanan informasi serta standar teknis dan prosedur keamanan Sistem Pemerintahan Berbasis Elektronik di lingkungan Kejaksaan Republik Indonesia.

2. Tujuan

   Pedoman ini ditujukan untuk mengoptimalkan pelaksanaan sistem manajemen keamanan informasi serta standar teknis dan prosedur

keamanan Sistem Pemerintahan Berbasis Elektronik di lingkungan Kejaksaan Republik Indonesia.

C. Ruang Lingkup

Ruang lingkup Pedoman ini meliputi sistem manajemen keamanan informasi Sistem Pemerintahan Berbasis Elektronik serta standar teknis dan prosedur keamanan Sistem Pemerintahan Berbasis Elektronik.

D. Dasar Hukum

1. Undang-Undang Nomor 16 Tahun 2004 tentang Kejaksaan Republik Indonesia (Lembaran Negara Republik Indonesia Tahun 2004 Nomor 67, Tambahan Lembaran Negara Republik Indonesia Nomor 4401) sebagaimana telah diubah dengan Undang-Undang Nomor 11 Tahun 2021 tentang Perubahan atas Undang Undang Nomor 16 Tahun 2004 tentang Kejaksaan Republik Indonesia (Lembaran Negara Republik Indonesia Tahun 2021 Nomor 298, Tambahan Lembaran Negara Republik Indonesia Nomor 6755);
2. Peraturan Presiden Nomor 38 Tahun 2010 tentang Organisasi dan Tata Kerja Kejaksaan Republik Indonesia sebagaimana telah beberapa kali diubah terakhir dengan Peraturan Presiden Nomor 15 Tahun 2021 tentang Perubahan Kedua atas Peraturan Presiden Nomor 38 Tahun 2010 tentang Organisasi dan Tata Kerja Kejaksaan Republik Indonesia (Lembaran Negara Republik Indonesia Tahun 2021 Nomor 67);
3. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintah Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
4. Peraturan Presiden Nomor 132 Tahun 2022 tentang Arsitektur Sistem Pemerintah Berbasis Elektronik Nasional (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 233);
5. Peraturan Jaksa Agung Nomor PER-006/A/JA/07/2017 tentang Organisasi dan Tata kerja Kejaksaan Republik Indonesia (Berita Negara Republik Indonesia Tahun 2017 Nomor 1069) sebagaimana telah beberapa kali diubah terakhir dengan Peraturan Kejaksaan Nomor 1 Tahun 2022 tentang Perubahan Ketiga atas Peraturan Jaksa Agung Nomor PER-006/JA/07/2017 tentang Organisasi dan Tata Kerja Kejaksaan Republik Indonesia (Berita Negara Republik Indonesia Tahun 2022 Nomor 33);

6. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 59 Tahun 2020 tentang Pemantauan dan Evaluasi Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2020 Nomor 994);
7. Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2021 Nomor 541).
8. Pedoman Jaksa Agung Nomor 4 Tahun 2022 tentang Sistem Pemerintahan Berbasis Elektronik di Lingkungan Kejaksaan Republik Indonesia.

E. Pengertian

Dalam Pedoman ini yang dimaksud dengan:

1. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada pengguna SPBE.
2. Kejaksaan Republik Indonesia yang selanjutnya disebut Kejaksaan adalah lembaga pemerintahan yang fungsinya berkaitan dengan kekuasaan kehakiman yang melaksanakan kekuasaan negara di bidang penuntutan serta kewenangan lain berdasarkan Undang-Undang.
3. Keamanan SPBE adalah pengendalian keamanan yang terpadu dalam SPBE.
4. Layanan SPBE adalah keluaran yang dihasilkan oleh 1 (satu) atau beberapa fungsi aplikasi SPBE dan yang memiliki nilai manfaat.
5. Aplikasi SPBE adalah satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas atau fungsi Layanan SPBE.
6. Jaringan Intra adalah jaringan tertutup yang menghubungkan antar simpul jaringan dalam suatu organisasi.
7. Sistem Penghubung Layanan adalah perangkat integrasi/penghubung untuk melakukan pertukaran Layanan SPBE.
8. Infrastruktur SPBE adalah semua perangkat keras, perangkat lunak, dan fasilitas yang menjadi penunjang utama untuk menjalankan sistem, aplikasi, komunikasi data, pengolahan dan penyimpanan data,

perangkat integrasi/penghubung, dan perangkat elektronik lainnya.

9. *Application Programming Interface* yang selanjutnya disingkat API adalah sekumpulan perintah, fungsi, serta protokol yang mengintegrasikan 2 (dua) bagian dari aplikasi atau dengan aplikasi yang berbeda secara bersamaan.
10. Pusat Data Kejaksaan adalah fasilitas yang digunakan untuk penempatan sistem elektronik dan komponen terkait lainnya untuk keperluan penempatan, penyimpanan, dan pengelolaan data, serta pemulihan data Kejaksaan yang dikelola oleh walidata Kejaksaan.

BAB II
SISTEM MANAJEMEN KEAMANAN INFORMASI SPBE

A. Umum

1. Setiap satuan kerja di lingkungan Kejaksaan melaksanakan sistem manajemen keamanan informasi SPBE berdasarkan Pedoman ini.
2. Pedoman sistem manajemen keamanan informasi SPBE di lingkungan Kejaksaan merupakan acuan dalam melaksanakan serangkaian proses manajemen keamanan informasi yang meliputi:
   a. penetapan ruang lingkup;
   b. penanggung jawab;
   c. perencanaan;
   d. dukungan pengoperasian;
   e. evaluasi kinerja; dan
   f. perbaikan berkelanjutan.
3. Walidata Kejaksaan mengomunikasikan dan mendokumentasikan kegiatan manajemen keamanan informasi SPBE Kejaksaan.

B. Penetapan Ruang Lingkup

1. Penetapan ruang lingkup dilakukan dengan mendefinisikan:
   a. isu internal keamanan informasi SPBE di Kejaksaan; dan
   b. isu eksternal keamanan informasi SPBE.
2. Isu internal keamanan informasi SPBE di Kejaksaan sebagaimana dimaksud pada angka 1 huruf a didefinisikan berdasarkan area yang menjadi prioritas Kejaksaan terhadap pelaksanaan keamanan informasi SPBE.
3. Area yang menjadi prioritas Kejaksaan terhadap pelaksanaan keamanan informasi SPBE sebagaimana dimaksud pada angka 2 paling

sedikit meliputi:

a. data dan informasi SPBE;
b. Aplikasi SPBE;
c. aset Infrastruktur SPBE; dan
d. kebijakan keamanan informasi SPBE yang telah dimiliki.

4. Isu eksternal keamanan informasi SPBE sebagaimana dimaksud pada angka 1 huruf b didefinisikan sesuai dengan ketentuan peraturan perundang-undangan.

C. Penanggung Jawab

1. Penanggung jawab sistem manajemen keamanan informasi adalah Wakil Jaksa Agung selaku Koordinator SPBE.
2. Dalam melaksanakan tugas sebagai penanggung jawab sistem manajemen keamanan informasi sebagaimana dimaksud pada angka 1, Wakil Jaksa Agung dibantu oleh pelaksana teknis Keamanan SPBE.
3. Pelaksana teknis Keamanan SPBE sebagaimana dimaksud pada angka 2 merupakan pejabat pimpinan tinggi pratama yang menyelenggarakan urusan di bidang teknologi, informasi dan komunikasi, yang membawahi, membangun, memelihara, dan/atau mengembangkan Aplikasi SPBE.
4. Pelaksana teknis Keamanan SPBE sebagaimana dimaksud pada angka 3 mempunyai tugas:
   a. memastikan penerapan standar teknis dan prosedur Keamanan SPBE;
   b. merumuskan, mengoordinasikan, dan melaksanakan program kerja dan anggaran Keamanan SPBE;
   c. melaporkan pelaksanaan sistem manajemen keamanan informasi SPBE dan penerapan standar teknis dan prosedur Keamanan SPBE kepada penanggung jawab Keamanan SPBE;
   d. memastikan penerapan standar teknis dan prosedur keamanan aplikasi pada seluruh satuan kerja Kejaksaan;
   e. memastikan seluruh pembangunan atau pengembangan Aplikasi dan Infrastruktur SPBE yang dilakukan oleh pihak ketiga memenuhi standar teknis dan prosedur Keamanan SPBE yang telah ditetapkan; dan
   f. memastikan keberlangsungan proses bisnis SPBE.

D. Perencanaan

1. Perencanaan sistem manajemen keamanan informasi dilakukan oleh pelaksana teknis Keamanan SPBE.
2. Perencanaan sebagaimana dimaksud pada angka 1 dilakukan dengan merumuskan:
   a. program kerja Keamanan SPBE yang disusun berdasarkan kategori risiko Keamanan SPBE; dan
   b. target realisasi program kerja Keamanan SPBE.
3. Program kerja Keamanan SPBE sebagaimana dimaksud pada angka 2 huruf a paling sedikit meliputi:
   a. edukasi kesadaran Keamanan SPBE;
   b. penilaian kerentanan Keamanan SPBE;
   c. peningkatan Keamanan SPBE;
   d. penanganan insiden Keamanan SPBE; dan
   e. audit Keamanan SPBE.
4. Kategori risiko Keamanan SPBE sebagaimana dimaksud pada angka 2 huruf a ditentukan sesuai dengan ketentuan peraturan perundang-undangan.
5. Target realisasi program kerja Keamanan SPBE sebagaimana dimaksud pada angka 2 huruf b ditetapkan berdasarkan kebutuhan.
6. Edukasi kesadaran Keamanan SPBE sebagaimana dimaksud pada angka 3 huruf a dilaksanakan paling sedikit melalui kegiatan:
   a. sosialisasi; dan
   b. pelatihan.
7. Penilaian kerentanan Keamanan SPBE sebagaimana dimaksud pada angka 3 huruf b dilaksanakan paling sedikit melalui:
   a. menginventarisasi seluruh aset SPBE meliputi data dan informasi, aplikasi, dan infrastruktur;
   b. mengidentifikasi kerentanan dan ancaman terhadap aset SPBE; dan
   c. mengukur tingkat risiko Keamanan SPBE.
8. Peningkatan Keamanan SPBE sebagaimana dimaksud pada angka 3 huruf c dilaksanakan berdasarkan hasil dari penilaian kerentanan Keamanan SPBE.
9. Peningkatan Keamanan SPBE sebagaimana dimaksud pada angka 8 dilaksanakan paling sedikit melalui:
   a. menerapkan standar teknis dan prosedur Keamanan SPBE; dan
   b. menguji fungsi keamanan terhadap Aplikasi SPBE dan Infrastruktur SPBE.

10. Penanganan insiden Keamanan SPBE sebagaimana dimaksud pada angka 3 huruf d dilaksanakan paling sedikit melalui:
    a. mengidentifikasi sumber serangan;
    b. menganalisis informasi yang berkaitan dengan insiden selanjutnya;
    c. memprioritaskan penanganan insiden berdasarkan tingkat dampak yang terjadi;
    d. mendokumentasi bukti insiden yang terjadi; dan
    e. memitigasi atau mengurangi dampak risiko Keamanan SPBE.
11. Audit Keamanan SPBE sebagaimana dimaksud pada angka 3 huruf e dilakukan sesuai dengan ketentuan peraturan perundang-undangan.

E. Dukungan Pengoperasian

1. Dukungan pengoperasian sistem manajemen keamanan informasi dilakukan oleh seluruh Koordinator SPBE dalam Tim Koordinasi SPBE Kejaksaan.
2. Dukungan pengoperasian sebagaimana dimaksud pada angka 1 dilakukan dengan meningkatkan kapasitas terhadap:
    a. sumber daya manusia Keamanan SPBE; dan
    b. anggaran Keamanan SPBE.
3. Sumber daya manusia Keamanan SPBE sebagaimana dimaksud pada angka 2 huruf a paling sedikit harus memiliki kompetensi:
    a. keamanan infrastruktur teknologi, informasi, dan komunikasi; dan
    b. keamanan aplikasi.
4. Untuk memenuhi kompetensi sebagaimana dimaksud pada angka 3, paling sedikit melakukan kegiatan:
    a. pelatihan dan/atau sertifikasi kompetensi keamanan infrastruktur teknologi, informasi, dan komunikasi serta keamanan aplikasi; dan
    b. bimbingan teknis mengenai standar Keamanan SPBE.
5. Anggaran Keamanan SPBE sebagaimana dimaksud pada angka 2 huruf b disusun berdasarkan perencanaan yang telah ditetapkan sesuai dengan ketentuan peraturan perundang-undangan.

F. Evaluasi Kinerja

1. Evaluasi kinerja sistem manajemen keamanan informasi dilakukan oleh penanggung jawab Keamanan SPBE.
2. Evaluasi kinerja sebagaimana dimaksud pada angka 1 dilakukan terhadap pelaksanaan Keamanan SPBE.

3. Evaluasi kinerja sistem manajemen keamanan informasi dilaksanakan dengan:
   a. mengidentifikasi area proses yang memiliki risiko tinggi terhadap keberhasilan pelaksanaan Keamanan SPBE;
   b. menetapkan indikator kinerja pada setiap area proses;
   c. memformulasi pelaksanaan Keamanan SPBE dengan mengukur secara kuantitatif kinerja yang diharapkan;
   d. menganalisis efektivitas pelaksanaan Keamanan SPBE; dan
   e. mendukung dan merealisasikan program audit Keamanan SPBE.
4. Evaluasi kinerja sebagaimana dimaksud pada angka 1 dilaksanakan paling sedikit 1 (satu) kali dalam 1 (satu) tahun.

G. Perbaikan Berkelanjutan
1. Perbaikan berkelanjutan sistem manajemen keamanan informasi dilakukan oleh pelaksana teknis Keamanan SPBE.
2. Perbaikan berkelanjutan sebagaimana dimaksud pada angka 1 merupakan tindak lanjut dari hasil evaluasi kinerja.
3. Perbaikan berkelanjutan sistem manajemen keamanan informasi dilakukan dengan:
   a. mengatasi permasalahan dalam pelaksanaan Keamanan SPBE; dan
   b. memperbaiki pelaksanaan Keamanan SPBE secara periodik.

BAB III
STANDAR TEKNIS DAN PROSEDUR KEAMANAN SPBE

A. Umum
1. Setiap satuan kerja harus menerapkan Keamanan SPBE.
2. Penerapan Keamanan SPBE sebagaimana dimaksud pada angka 1 harus memenuhi standar teknis dan prosedur Keamanan SPBE.
3. Standar teknis dan prosedur Keamanan SPBE diterapkan untuk:
   a. keamanan data dan informasi;
   b. keamanan Aplikasi SPBE;
   c. keamanan Sistem Penghubung Layanan;
   d. keamanan Jaringan Intra; dan
   e. keamanan Pusat Data Kejaksaan.

B. Keamanan Data dan Informasi

1. Standar teknis keamanan data dan informasi terdiri atas terpenuhinya aspek:
   a. kerahasiaan;
   b. keaslian;
   c. keutuhan;
   d. kenirsangkalan; dan
   e. ketersediaan.
2. Terpenuhinya aspek kerahasiaan sebagaimana dimaksud pada angka 1 huruf a dilakukan dengan prosedur:
   a. menerapkan klasifikasi informasi;
   b. menerapkan enkripsi dengan sistem kriptografi; dan
   c. menerapkan pembatasan akses terhadap data dan informasi sesuai dengan kewenangan dan kebijakan yang telah ditetapkan.
3. Terpenuhinya aspek keaslian sebagaimana dimaksud pada angka 1 huruf b dilakukan dengan prosedur:
   a. menyediakan mekanisme verifikasi;
   b. menyediakan mekanisme validasi; dan
   c. menerapkan sistem fungsi *hash*.
4. Terpenuhinya aspek keutuhan sebagaimana dimaksud pada angka 1 huruf c dilakukan dengan prosedur:
   a. menerapkan pendeteksian modifikasi; dan
   b. menerapkan tanda tangan elektronik tersertifikasi.
5. Terpenuhinya aspek kenirsangkalan sebagaimana dimaksud pada angka 1 huruf d dilakukan dengan prosedur:
   a. menerapkan tanda tangan elektronik tersertifikasi; dan
   b. penjaminan oleh penyelenggara sertifikasi elektronik melalui sertifikat elektronik.
6. Terpenuhinya aspek ketersediaan sebagaimana dimaksud pada angka 1 huruf e dilakukan dengan prosedur:
   a. menerapkan sistem pencadangan secara berkala;
   b. membuat perencanaan untuk menjamin data dan informasi dapat selalu diakses; dan
   c. menerapkan sistem pemulihan.

C. Keamanan Aplikasi SPBE

1. Standar teknis dan prosedur keamanan Aplikasi SPBE diterapkan pada:
   a. aplikasi berbasis *web*; dan

b. aplikasi berbasis *mobile*.

2. Aplikasi berbasis *web* sebagaimana dimaksud pada angka 1 huruf a merupakan aplikasi yang diakses melalui peramban saat terhubung dengan koneksi internet atau intranet.
3. Aplikasi berbasis *mobile* sebagaimana dimaksud pada angka 1 huruf b merupakan aplikasi yang dalam pengoperasiannya dapat berjalan di perangkat bergerak dan memiliki sistem operasi yang mendukung perangkat lunak secara *standalone*.
4. Aplikasi SPBE harus dilakukan pengujian keamanan setiap periode tertentu yang dilakukan dengan:
   a. mengidentifikasi persyaratan minimum keamanan yang belum diterapkan;
   b. memastikan pengkodean pemrograman aplikasi yang dibuat tidak memiliki kerawanan;
   c. melakukan pemindaian otomatis dan/atau pengujian penetrasi sistem;
   d. mengidentifikasi kerentanan dan mengelola ancaman sejak awal siklus pengembangan Aplikasi SPBE; dan
   e. menganalisis kerentanan.
5. Standar teknis keamanan aplikasi berbasis *web* sebagaimana dimaksud pada angka 1 huruf a terdiri atas terpenuhinya fungsi:
   a. autentikasi;
   b. manajemen sesi;
   c. persyaratan kontrol akses;
   d. validasi input;
   e. kriptografi pada verifikasi statis;
   f. penanganan eror dan pencatatan log;
   g. proteksi data;
   h. keamanan komunikasi;
   i. pengendalian kode berbahaya;
   j. logika bisnis;
   k. *file*;
   l. keamanan API dan *web service*; dan
   m. keamanan konfigurasi.
6. Terpenuhinya fungsi autentikasi sebagaimana dimaksud pada angka 5 huruf a dilakukan dengan prosedur:
   a. menggunakan manajemen kata sandi untuk proses autentikasi;

b. menerapkan verifikasi kata sandi pada sisi *server*;
c. mengatur jumlah karakter, kombinasi jenis karakter, dan masa berlaku dari kata sandi;
d. mengatur jumlah maksimum kesalahan dalam pemasukan kata sandi;
e. mengatur mekanisme pemulihan kata sandi;
f. menjaga kerahasiaan kata sandi yang disimpan melalui mekanisme kriptografi; dan
g. menggunakan jalur komunikasi yang diamankan untuk proses autentikasi.

7. Terpenuhinya fungsi manajemen sesi sebagaimana dimaksud pada angka 5 huruf b dilakukan dengan prosedur:
   a. menggunakan pengendali sesi untuk proses manajemen sesi;
   b. menggunakan pengendali sesi yang disediakan oleh kerangka kerja aplikasi;
   c. mengatur pembuatan dan keacakan token sesi yang dihasilkan oleh pengendali sesi;
   d. mengatur kondisi dan jangka waktu habis sesi;
   e. validasi dan pencantuman *session id;*
   f. pelindungan terhadap lokasi dan pengiriman token untuk sesi terautentikasi; dan
   g. pelindungan terhadap duplikasi dan mekanisme persetujuan pengguna.
8. Terpenuhinya fungsi persyaratan kontrol akses sebagaimana dimaksud pada angka 5 huruf c dilakukan dengan prosedur:
   a. menetapkan otorisasi pengguna untuk membatasi kontrol akses;
   b. mengatur peringatan terhadap bahaya serangan otomatis apabila terjadi akses yang bersamaan atau akses yang terus-menerus pada fungsi;
   c. mengatur antarmuka pada sisi administrator; dan
   d. mengatur verifikasi kebenaran token ketika mengakses data dan informasi yang dikecualikan.
9. Terpenuhinya fungsi validasi input sebagaimana dimaksud pada angka 5 huruf d dilakukan dengan prosedur:
   a. menerapkan fungsi validasi input pada sisi *server*;
   b. menerapkan mekanisme penolakan input jika terjadi kesalahan validasi;

c. memastikan *runtime environment* aplikasi tidak rentan terhadap serangan validasi input;
d. melakukan validasi positif pada seluruh input;
e. melakukan filter terhadap data yang tidak dipercaya;
f. menggunakan fitur kode dinamis;
g. melakukan pelindungan terhadap akses yang mengandung konten skrip; dan
h. melakukan pelindungan dari serangan injeksi basis data.

10. Terpenuhinya fungsi kriptografi pada verifikasi statis sebagaimana dimaksud pada angka 5 huruf e dilakukan dengan prosedur:
    a. menggunakan algoritma kriptografi, modul kriptografi, protokol kriptografi, dan kunci kriptografi sesuai dengan ketentuan peraturan perundang undangan;
    b. melakukan autentikasi data yang dienkripsi;
    c. menerapkan manajemen kunci kriptografi; dan
    d. membuat angka acak yang menggunakan generator angka acak kriptografi.
11. Terpenuhinya fungsi penanganan eror dan pencatatan log sebagaimana dimaksud pada angka 5 huruf f dilakukan dengan prosedur:
    a. mengatur konten pesan yang ditampilkan ketika terjadi kesalahan;
    b. menggunakan metode penanganan eror untuk mencegah kesalahan terprediksi dan tidak terduga serta menangani seluruh pengecualian yang tidak ditangani;
    c. tidak mencantumkan informasi yang dikecualikan dalam pencatatan log;
    d. mengatur cakupan log yang dicatat untuk mendukung upaya penyelidikan ketika terjadi insiden;
    e. mengatur pelindungan log aplikasi dari akses dan modifikasi yang tidak sah;
    f. melakukan enkripsi pada data yang disimpan untuk mencegah injeksi log; dan
    g. melakukan sinkronisasi sumber waktu sesuai dengan zona waktu dan waktu yang benar.
12. Terpenuhinya fungsi proteksi data sebagaimana dimaksud pada angka 5 huruf g dilakukan dengan prosedur:
    a. melakukan identifikasi dan penyimpanan salinan informasi yang dikecualikan;

b. melakukan pelindungan dari akses yang tidak sah terhadap informasi yang dikecualikan yang disimpan sementara dalam aplikasi;
c. melakukan pertukaran, penghapusan, dan audit informasi yang dikecualikan;
d. melakukan penentuan jumlah parameter;
e. memastikan data disimpan dengan aman;
f. menentukan metode untuk menghapus dan mengekspor data sesuai permintaan pengguna; dan
g. membersihkan memori setelah tidak diperlukan.

13. Terpenuhinya fungsi keamanan komunikasi sebagaimana dimaksud pada angka 5 huruf h dilakukan dengan prosedur:
a. menggunakan komunikasi terenkripsi;
b. mengatur koneksi masuk dan keluar yang aman dan terenkripsi dari sisi pengguna;
c. mengatur jenis algoritma yang digunakan dan alat pengujiannya;
d. mengatur aktivasi dan konfigurasi sertifikat elektronik yang diterbitkan oleh penyelenggara sertifikasi elektronik; dan
e. menggunakan domain dan subdomain resmi Kejaksaan yang telah terdaftar (kejaksaan.go.id) untuk aplikasi yang diakses menggunakan jaringan internet publik sebagai upaya menghindari *phising* dan serangan lainnya.

14. Terpenuhinya fungsi pengendalian kode berbahaya sebagaimana dimaksud pada angka 5 huruf i dilakukan dengan prosedur:
a. menggunakan analisis kode dalam kontrol kode berbahaya;
b. memastikan kode sumber aplikasi dan pustaka tidak mengandung kode berbahaya dan fungsionalitas lain yang tidak diinginkan;
c. mengatur izin terkait fitur atau sensor terkait privasi;
d. mengatur pelindungan integritas; dan
e. mengatur mekanisme fitur pembaruan.

15. Terpenuhinya fungsi logika bisnis sebagaimana dimaksud pada angka 5 huruf j dilakukan dengan prosedur:
a. memproses alur logika bisnis dalam urutan langkah dan waktu yang realistis;
b. memastikan logika bisnis memiliki batasan dan validasi;
c. memonitor aktivitas yang tidak biasa;
d. membantu dalam kontrol anti otomatisasi; dan

e. memberikan peringatan ketika terjadi serangan otomatis atau aktivitas yang tidak biasa.

16. Terpenuhinya fungsi *file* sebagaimana dimaksud pada angka 5 huruf k dilakukan dengan prosedur:
    a. mengatur jumlah *file* untuk setiap pengguna dan kuota ukuran *file* yang diunggah;
    b. melakukan validasi *file* sesuai dengan tipe konten yang diharapkan;
    c. melakukan pelindungan terhadap metadata input dan metadata *file*;
    d. melakukan pemindaian *file* yang diperoleh dari sumber yang tidak dipercaya; dan
    e. melakukan konfigurasi *server* untuk mengunduh *file* sesuai ekstensi yang ditentukan.
17. Terpenuhinya fungsi keamanan API dan *web service* sebagaimana dimaksud pada angka 5 huruf l dilakukan dengan prosedur:
    a. melakukan konfigurasi layanan *web*;
    b. memverifikasi *uniform resource identifier* API tidak menampilkan informasi yang berpotensi sebagai celah keamanan;
    c. membuat keputusan otorisasi;
    d. menampilkan metode *RESTful hypertext transfer protocol* apabila input pengguna dinyatakan valid;
    e. menggunakan validasi skema dan verifikasi sebelum menerima input;
    f. menggunakan metode pelindungan layanan berbasis *web*; dan
    g. menerapkan kontrol anti otomatisasi.
18. Terpenuhinya fungsi keamanan konfigurasi sebagaimana dimaksud pada angka 5 huruf m dilakukan dengan prosedur:
    a. mengkonfigurasi *server* sesuai rekomendasi *server* aplikasi dan kerangka kerja aplikasi yang digunakan;
    b. mendokumentasi, menyalin konfigurasi, dan semua dependensi;
    c. menghapus fitur, dokumentasi, sampel, dan konfigurasi yang tidak diperlukan;
    d. memvalidasi integritas aset jika aset aplikasi diakses secara eksternal; dan
    e. menggunakan respon aplikasi dan konten yang aman.
19. Standar teknis keamanan aplikasi berbasis *mobile* sebagaimana dimaksud pada angka 1 huruf b terdiri atas terpenuhinya fungsi:
    a. penyimpanan data dan persyaratan privasi;

b. kriptografi;
c. autentikasi dan manajemen sesi;
d. komunikasi jaringan;
e. interaksi *platform*;
f. kualitas kode dan pengaturan *build*; dan
g. ketahanan.

20. Terpenuhinya fungsi penyimpanan data dan persyaratan privasi sebagaimana dimaksud pada angka 19 huruf a dilakukan dengan prosedur:
    a. menyimpan seluruh data dan informasi yang dikecualikan hanya dalam fasilitas penyimpanan kredensial sistem;
    b. membatasi pertukaran data dan informasi yang dikecualikan dengan *third party*;
    c. menonaktifkan *cache keyboard* pada saat memasukkan data dan informasi yang dikecualikan;
    d. melindungi informasi yang dikecualikan saat terjadi *inter process communication*; dan
    e. melindungi data dan informasi yang dikecualikan yang dimasukkan melalui antarmuka pengguna.
21. Terpenuhinya fungsi kriptografi sebagaimana dimaksud pada angka 19 huruf b dilakukan dengan prosedur:
    a. menghindari penggunaan kriptografi simetrik dengan *hardcoded key;*
    b. mengimplementasikan metode kriptografi yang sudah teruji sesuai kebutuhan;
    c. menghindari penggunaan protokol kriptografi atau algoritma kriptografi yang obsolet;
    d. menghindari penggunaan kunci kriptografi yang sama; dan
    e. menggunakan pembangkit kunci acak yang memenuhi kriteria keacakan kunci.
22. Terpenuhinya fungsi autentikasi dan manajemen sesi sebagaimana dimaksud pada angka 19 huruf c dilakukan dengan prosedur:
    a. menerapkan autentikasi pada *remote endpoint* terhadap aplikasi yang menyediakan akses pengguna untuk layanan jarak jauh;
    b. menggunakan *session identifier* yang acak tanpa perlu mengirimkan kredensial pengguna apabila menggunakan *stateful* manajemen sesi;

c. memastikan *server* menyediakan token yang telah ditandatangani menggunakan algoritma yang aman apabila menggunakan autentikasi *stateless* berbasis token;
d. memastikan *remote endpoint* memutus sesi yang ada saat pengguna *log out*;
e. menerapkan pengaturan sandi pada *remote endpoint;*
f. membatasi jumlah percobaan *log in* pada *remote endpoint*;
g. menentukan masa berlaku sesi dan masa kedaluwarsa token pada *remote endpoint*; dan
h. melakukan otorisasi pada *remote endpoint.*

23. Terpenuhinya fungsi komunikasi jaringan sebagaimana dimaksud pada angka 19 huruf d dilakukan dengan prosedur:
    a. menerapkan *secure socket layer* atau *transport layer security* yang tidak obsolet secara konsisten; dan
    b. memverifikasi sertifikat *remote endpoint.*
24. Terpenuhinya fungsi interaksi *platform* sebagaimana dimaksud pada angka 19 huruf e dilakukan dengan prosedur:
    a. memastikan aplikasi hanya meminta akses terhadap sumber daya yang diperlukan;
    b. melakukan validasi terhadap seluruh input dari sumber eksternal dan pengguna;
    c. menghindari pengiriman fungsionalitas sensitif melalui skema *custom uniform resource locator* dan fasilitas *inter process communication*;
    d. menghindari penggunaan *JavaScript* dalam *WebView*;
    e. menggunakan protokol *hypertext transfer protocol secure* pada *WebView*; dan
    f. mengimplementasikan penggunaan serialisasi API yang aman.
25. Terpenuhinya fungsi kualitas kode dan pengaturan *build* sebagaimana dimaksud pada angka 19 huruf f dilakukan dengan prosedur:
    a. menandatangani aplikasi dengan sertifikat yang valid;
    b. memastikan aplikasi dalam mode rilis;
    c. menghapus simbol *debugging* dari *native binary*;
    d. menghapus kode *debugging* dan kode bantuan pengembang;
    e. mengidentifikasi kelemahan seluruh komponen *third party*;
    f. menentukan mekanisme penanganan eror;
    g. mengelola memori secara aman; dan

h. mengaktifkan fitur keamanan yang tersedia.

26. Terpenuhinya fungsi ketahanan sebagaimana dimaksud pada angka 19 huruf g dilakukan dengan prosedur:
    a. mencegah aplikasi berjalan pada perangkat yang telah dilakukan modifikasi yang tidak sah;
    b. mendeteksi dan merespons *debugger*;
    c. mencegah *executable file* melakukan perubahan pada sumber daya perangkat;
    d. mendeteksi dan merespons keberadaan perangkat *reverse engineering*;
    e. mencegah aplikasi berjalan dalam *emulator*;
    f. mendeteksi perubahan kode dan data di ruang memori;
    g. menerapkan fungsi *device binding* dengan menggunakan *property* unik pada perangkat;
    h. melindungi seluruh *file* dan *library* pada aplikasi; dan
    i. menerapkan metode *obfuscation*.

D. Keamanan Sistem Penghubung Layanan

1. Standar teknis keamanan Sistem Penghubung Layanan terdiri atas terpenuhinya fungsi:
    a. keamanan interoperabilitas data dan informasi;
    b. kontrol sistem integrasi;
    c. kontrol perangkat integrator;
    d. keamanan API dan *web service*; dan
    e. keamanan migrasi data.
2. Terpenuhinya fungsi keamanan interoperabilitas data dan informasi sebagaimana dimaksud pada angka 1 huruf a dilakukan dengan prosedur:
    a. menerapkan sistem tanda tangan elektronik tersertifikasi untuk pengamanan dokumen dan surat elektronik;
    b. menerapkan sistem enkripsi data;
    c. memastikan data dan informasi selalu dapat diakses sesuai otoritasnya; dan
    d. menerapkan sistem fungsi *hash* pada *file*.
3. Terpenuhinya fungsi kontrol sistem integrasi sebagaimana dimaksud pada angka 1 huruf b dilakukan dengan prosedur:
    a. menerapkan protokol *secure socket layer* atau protokol *transport*

layer security versi terkini pada sesi pengiriman data dan informasi;

b. menerapkan internet *protocol security* untuk mengamankan transmisi data dalam jaringan berbasis *transmission control protocol/ internet protocol*;
c. menerapkan sistem anti *distributed denial of service*;
d. menerapkan autentikasi untuk memverifikasi identitas eksternal antar Layanan SPBE yang terhubung;
e. menerapkan manajemen keamanan sesi;
f. menerapkan pembatasan akses pengguna berdasarkan otorisasi yang telah ditetapkan;
g. menerapkan validasi input;
h. menerapkan kriptografi pada verifikasi statis;
i. menerapkan sertifikat elektronik pada *web authentication*;
j. menerapkan penanganan eror dan pencatatan *log*;
k. menerapkan proteksi data dan jalur komunikasi;
l. menerapkan pendeteksi virus untuk memeriksa beberapa konten *file*;
m. menetapkan perjanjian tingkat layanan dengan standar paling rendah 95% (sembilan puluh lima persen); dan
n. memastikan sistem integrasi tidak memiliki kerentanan yang berpotensi menjadi celah peretas.

4. Terpenuhinya fungsi kontrol perangkat integrator sebagaimana dimaksud pada angka 1 huruf c dilakukan dengan prosedur:
   a. menggunakan sistem operasi dan perangkat lunak dengan *security patches* terkini;
   b. menggunakan antivirus dan anti-*spyware* terkini;
   c. mengaktifkan fitur keamanan pada peramban *web*;
   d. menerapkan *firewall* dan *host-based intrusion detection systems*;
   e. mencegah instalasi perangkat lunak yang belum terverifikasi;
   f. mencegah akses terhadap situs yang tidak sah; dan
   g. mengaktifkan sistem *recovery* dan *restore* pada perangkat integrator.
5. Terpenuhinya fungsi keamanan API dan *web service* sebagaimana dimaksud pada angka 1 huruf d dilakukan dengan prosedur:
   a. menerapkan protokol *secure socket layer* atau protokol *transport layer security* di antara pengirim dan penerima API;
   b. menerapkan protokol *open authorization* versi terkini untuk menjembatani interaksi antara *resource owner, resource server*

dan/atau *third party*;

c. menampilkan metode *RESTful hypertext transfer protocol* apabila input pengguna dinyatakan valid;

d. melindungi layanan *web RESTful* yang menggunakan *cookie* dari *cross-site request forgery*; dan

e. memvalidasi parameter yang masuk oleh penerima API untuk memastikan data yang diterima valid dan tidak menyebabkan kerusakan.

6. Terpenuhinya fungsi keamanan migrasi data sebagaimana dimaksud pada angka 1 huruf e dilakukan dengan prosedur:

a. memastikan migrasi data dilakukan secara bertahap dan terprogram oleh sistem;

b. memastikan aplikasi yang menggunakan sistem basis data lama tetap dipertahankan sampai sistem pendukung basis data baru dapat berjalan atau berfungsi dengan normal;

c. mendokumentasikan format sistem basis data lama secara rinci;

d. melakukan pencadangan seluruh data yang tersimpan pada sistem sebelum melakukan migrasi data;

e. menerapkan teknik kriptografi pada proses penyimpanan dan pengambilan data; dan

f. melakukan validasi data ketika proses migrasi data selesai.

E. Keamanan Jaringan Intra

1. Standar teknis keamanan Jaringan Intra diterapkan pada:

a. Jaringan Intra pemerintah; dan

b. Jaringan Intra seluruh satuan kerja Kejaksaan.

2. Standar teknis keamanan Jaringan Intra sebagaimana dimaksud pada angka 1 terdiri atas terpenuhinya:

a. aspek administrasi keamanan Jaringan Intra;

b. kontrol akses dan autentikasi;

c. persyaratan perangkat dan aplikasi keamanan Jaringan Intra;

d. kontrol keamanan *gateway*;

e. kontrol keamanan *access point* pada jaringan nirkabel; dan

f. kontrol konfigurasi *access point* pada jaringan nirkabel.

3. Terpenuhinya aspek administrasi keamanan Jaringan Intra sebagaimana dimaksud pada angka 2 huruf a dilakukan dengan prosedur:

a. menyusun dan mengevaluasi dokumen arsitektur Jaringan Intra;
b. mengidentifikasi seluruh aset infrastruktur jaringan;
c. menyusun dan menetapkan standar operasional prosedur terkait pemeliharaan keamanan Jaringan Intra; dan
d. membuat laporan pengawasan keamanan jaringan secara periodik.

4. Terpenuhinya kontrol akses dan autentikasi sebagaimana dimaksud pada 2 huruf b dilakukan dengan prosedur:
   a. menempatkan perangkat infrastruktur jaringan yang menyediakan layanan Jaringan Intra pada zona terpisah;
   b. menggunakan autentikasi untuk mengakses Jaringan Intra;
   c. menerapkan pembatasan akses dalam Jaringan Intra;
   d. mematikan atau membatasi *protocol*, *port*, dan layanan yang tidak digunakan;
   e. menerapkan penyaringan tautan dan memblokir akses ke situs berbahaya;
   f. menerapkan fungsi *honeypot* untuk menganalisis celah keamanan berdasarkan jenis serangan;
   g. menerapkan *virtual private network* dan mengaktifkan fungsi enkripsi pada jalur komunikasi yang digunakan;
   h. memberikan kewenangan hanya kepada administrator untuk menginstal perangkat lunak dan/atau mengubah konfigurasi sistem dalam Jaringan Intra;
   i. menerapkan *secure endpoints*;
   j. memblokir layanan yang tidak dikenal;
   k. menerapkan *secure socket layer* atau *transport layer security* versi terkini pada jalur akses Jaringan Intra; dan
   l. menerapkan *server* perantara saat *client* mengakses *server database* dalam rangka pemeliharaan.
5. Terpenuhinya persyaratan perangkat dan aplikasi keamanan Jaringan Intra sebagaimana dimaksud pada angka 2 huruf c dilakukan dengan prosedur:
   a. menggunakan perangkat *security information and event management* (SIEM) untuk *network logging* dan *monitoring*;
   b. menerapkan sistem deteksi dini kerentanan keamanan perangkat jaringan;
   c. menggunakan perangkat *firewall*;
   d. menggunakan perangkat *intrusion detection systems* dan *intrusion*

prevention systems;

e. menerapkan *virtual private network* terenkripsi untuk penggunaan akses jarak jauh secara terbatas;

f. menerapkan kontrol *update patching* pada infrastruktur Jaringan Intra dan sistem komputer;

g. menggunakan perangkat *web application firewall*;

h. menggunakan perangkat *load balancer* untuk menjaga ketersediaan akses terhadap jaringan dan aplikasi;

i. memperbarui teknologi keamanan perangkat keras dan perangkat lunak untuk meminimalisasi celah peretas;

j. mengunduh perangkat lunak melalui *enterprise software distribution system*; dan

k. menerapkan sertifikat elektronik.

6. Terpenuhinya kontrol keamanan *gateway* sebagaimana dimaksud pada angka 2 huruf d dilakukan dengan prosedur:

a. menerapkan *content filtering*;

b. menerapkan *inspection packet filtering* untuk memeriksa paket yang masuk pada Jaringan Intra;

c. menerapkan kontrol keamanan pada fitur akses jarak jauh perangkat *gateway*;

d. memastikan perangkat *gateway* yang menghubungkan antar Jaringan Intra tidak terkoneksi langsung dengan jaringan publik;

e. melaksanakan manajemen *traffic gateway*; dan

f. memastikan *port* tidak dibuka secara *default.*

7. Terpenuhinya kontrol keamanan *access point* pada jaringan nirkabel sebagaimana dimaksud pada angka 2 huruf e dilakukan dengan prosedur:

a. menerapkan protokol keamanan *access point* nirkabel dan teknologi enkripsi terkini;

b. menerapkan *media access control* pada *address filtering*;

c. menerapkan *dedicated service set identifier;*

d. menerapkan pembatasan jangkauan radio transmisi dan pengguna jaringan;

e. menerapkan pembatasan terkait penambahan perangkat nirkabel yang dipasang secara tidak sah;

f. menerapkan manajemen *vulnerability* secara berkala dan berkelanjutan; dan

g. melakukan *patching firmware* secara rutin.

8. Terpenuhinya kontrol konfigurasi *access point* pada jaringan nirkabel sebagaimana dimaksud pada angka 2 huruf f dilakukan dengan prosedur:
   a. menggunakan kata sandi yang kuat;
   b. menggunakan protokol model *authentication authorization* dan *accounting* pada perangkat infrastruktur jaringan untuk *management user* atau otentikasi *administrator access point*;
   c. memastikan fitur akses konfigurasi jarak jauh hanya dapat digunakan dalam kondisi darurat dengan menerapkan kontrol keamanan;
   d. mengisolasi atau melakukan segmentasi jaringan area lokal nirkabel; dan
   e. menonaktifkan antarmuka nirkabel, layanan, dan aplikasi yang tidak digunakan.

F. Keamanan Pusat Data Kejaksaan

1. Standar teknis keamanan Pusat Data Kejaksaan terdiri atas terpenuhinya:
   a. persyaratan keamanan fisik dan manajemen Pusat Data Kejaksaan; dan
   b. persyaratan koneksi perangkat ke Pusat Data Kejaksaan.
2. Terpenuhinya persyaratan keamanan fisik dan manajemen Pusat Data Kejaksaan sebagaimana dimaksud pada angka 1 huruf a dilakukan dengan prosedur sesuai dengan Standar Nasional Indonesia yang terkait dengan Pusat Data.
3. Terpenuhinya persyaratan koneksi perangkat ke Pusat Data Kejaksaan sebagaimana dimaksud pada angka 1 huruf b dilakukan dengan prosedur:
   a. memastikan keamanan perangkat yang terkoneksi ke infrastruktur Pusat Data Kejaksaan;
   b. memutus akses fisik atau *logic* dari perangkat yang tidak terotorisasi;
   c. memastikan akses tingkat administrator ke *server* dan perangkat jaringan utama tidak boleh dilakukan secara *remote*;
   d. memastikan hanya personil yang berwenang yang boleh menggunakan komputer di area Pusat Data Kejaksaan;

e. melakukan *backup* informasi dan perangkat lunak yang berada di Pusat Data Kejaksaan secara berkala;
f. memastikan perangkat komputer Pusat Data Kejaksaan terbebas dari virus atau *malware*;
g. melakukan pembatasan akses pemanfaatan *removable* media di area Pusat Data Kejaksaan;
h. memastikan pengaktifan konfigurasi *port universal serial bus* telah mendapatkan izin dari personil yang berwenang;
i. memastikan setiap perangkat yang akan terkoneksi ke infrastruktur Pusat Data Kejaksaan menggunakan *internet protocol address* dan *hostname* yang telah ditentukan; dan
j. menerapkan *server* perantara saat *client* mengakses *server database* dalam rangka pemeliharaan.

BAB IV
PENUTUP

1. Pedoman ini mulai berlaku sejak tanggal ditetapkan.
2. Pedoman ini agar dilaksanakan sebaik-baiknya dengan penuh tanggung jawab.

Ditetapkan di Jakarta
pada tanggal 14 Juli 2023

JAKSA AGUNG REPUBLIK INDONESIA,

BURHANUDDIN