KEMENTERIAN HUKUM DAN HAK ASASI MANUSIA
REPUBLIK INDONESIA

PEDOMAN

Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik Dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik di Lingkungan Kementerian Hukum dan Hak Asasi Manusia

BerAKHLAK SEMAKIN PASTI REFORMASI HUKUM PEMAJUAN HAK ASASI MANUSIA

KATA PENGANTAR

Kemajuan teknologi komunikasi dan informasi yang pesat serta potensi pemanfaatannya secara luas, membuka peluang bagi pengaksesan, pengelolaan, dan pendayagunaan informasi dalam volume yang besar secara tepat dan akurat. Pemanfaatan teknologi komunikasi dan informasi dalam proses pemerintahan (*e-government*) akan meningkatkan efisiensi, efektifitas, transaparansi, dan akuntabilitas penyelenggaraan pemerintahan dan peningkatan layanan publik sehingga dapat terwujud pemerintahan yang baik (*good governance*).

Dengan telah ditetapkannya Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE) yang merupakan kebijakan dalam upaya meningkatkan keterpaduan, efisiensi, dan tata kelola manajemen sistem pemerintahan berbasis elektronik secara nasional guna mewujudkan tata kelola pemerintahan yang bersih, efektif, transparan, dan akuntabel serta pelayanan publik yang berkualitas dan terpercaya diperlukan sistem pemerintahan berbasis elektronik.

Kementerian Hukum dan Hak Asasi Manusia turut serta mendukung penerapan SPBE melalui Peraturan Menteri Hukum dan Hak Asasi Manusia Nomor 30 Tahun 2021 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik di Lingkungan Kementerian Hukum dan Hak Asasi Manusia, peraturan ini ditetapan sebagai bentuk kepatuhan dalam penyelenggaraan SPBE yang lebih baik, efisien, dan terpadu di lingkungan Kementerian Hukum dan Hak Asasi Manusia.

Dalam penyelenggaraan SPBE tersebut ditetapkan kebijakan pengaturan penerapan manajemen keamanan informasi yang mencakup manajemen keamanan informasi yang berlandaskan penjaminan kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan sumber daya terkait data dan informasi, infrastruktur, dan aplikasi SPBE.

Kebijakan pengaturan penerapan manajemen keamanan informasi ini merupakan acuan dalam melaksanakan serangkaian proses manajemen keamanan informasi dan penerapan keamanan SPBE yang memenuhi standar teknis dan prosedur keamanan SPBE yang dilaksanakan oleh setiap satuan kerja di lingkungan Kementerian Hukum dan Hak Asasi Manusia.

Harapan saya, Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik di Lingkungan Kementerian Hukum dan Hak Asasi Manusia dapat menjamin keberlangsungan SPBE dengan meminimalkan dampak risiko keamanan informasi SPBE di lingkungan Kementerian Hukum dan Hak Asasi Manusia dengan memaksimalkan kolaborasi dan sinergitas.

Akhir kata semoga pedoman ini dapat digunakan sebagai panduan bagi pemangku kepentingan dalam rangka penerapan manajemen keamanan informasi SPBE guna mewujudkan penyelenggaraan SPBE yang lebih baik dan terpadu di lingkungan Kementerian Hukum dan Hak Asasi Manusia.

MENTERI HUKUM DAN HAK ASASI MANUSIA,

YASONNA H. LAOLY

DAFTAR ISI

KATA PENGANTAR i

DAFTAR ISI iii

BAB I PENDAHULUAN 1

1. Latar Belakang 1

2. Maksud dan Tujuan 1

3. Ruang Lingkup 2

4. Pengertian 2

5. Dasar 3

BAB II MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK 4

1. Penjelasan Umum 4

2. Proses Manajemen Keamanan Informasi 4

BAB III STANDAR TEKNIS DAN PROSEDUR KEAMANAN SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK 6

1. Keamanan Data dan Informasi 7

2. Keamanan Aplikasi SPBE 7

3. Keamanan Sistem Penghubung Layanan 12

4. Keamanan Jaringan Intra 14

5. Keamanan Pusat Data 16

BAB IV PENUTUP 17

MENTERI HUKUM DAN HAK ASASI MANUSIA
REPUBLIK INDONESIA

PEDOMAN

MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DAN STANDAR TEKNIS DAN PROSEDUR KEAMANAN SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DI LINGKUNGAN KEMENTERIAN HUKUM DAN HAK ASASI MANUSIA

NOMOR M.HH-02.TI.01 TAHUN 2023

BAB I
PENDAHULUAN

1. Latar Belakang

Berdasarkan ketentuan Pasal 3 ayat (2), Pasal 4 ayat (1), dan Pasal 5 ayat (1) 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, kementerian diamanatkan untuk menetapkan ketentuan terkait manajemen keamanan informasi yang selaras dengan kebutuhan kebijakan manajemen sistem pemerintahan berbasis elektronik kementerian sebagaimana tercantum pada Pasal 48 Peraturan Menteri Hukum dan Hak Asasi Manusia Nomor 30 Tahun 2021 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik di Lingkungan Kementerian Hukum dan Hak Asasi Manusia.

Dengan adanya penerapan kebijakan keamanan informasi berbasis sistem pemerintahan berbasis elektronik ini diharapkan pelaksanaan manajemen keamanan informasi dan standar teknis dan prosedur keamanan informasi di lingkungan Kementerian terjamin sehingga dapat dikelola dan dimanfaatkan dalam pengambilan keputusan berlandaskan penjaminan kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan (*non-repudiation*) sumber daya terkait data dan informasi, infrastruktur sistem pemerintahan berbasis elektronik, dan aplikasi.

2. Maksud dan Tujuan

Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik di Lingkungan Kementerian Hukum dan Hak Asasi Manusia ini dimaksudkan sebagai pedoman atau standar dalam rangka melaksanakan manajemen keamanan informasi berbasis sistem pemerintahan berbasis elektronik dengan tujuan untuk untuk menjamin keberlangsungan sistem pemerintahan berbasis elektronik dengan meminimalkan dampak risiko keamanan informasi.

3. Ruang Lingkup

Ruang lingkup pedoman ini berlaku dalam hal pelaksanaan manajemen keamanan informasi sistem pemerintahan berbasis elektronik dan standar teknis dan prosedur keamanan sistem pemerintahan berbasis elektronik yang dilaksanakan pada unit kerja eselon I, kantor wilayah, dan unit pelaksana teknis di lingkungan Kementerian Hukum dan Hak Asasi Manusia.

4. Pengertian

a. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada pengguna SPBE;
b. Instansi Penyelenggara Keamanan Siber adalah instansi pemerintah yang menyelenggarakan tugas pemerintahan di bidang keamanan siber;
c. Keamanan SPBE adalah pengendalian keamanan yang terpadu dalam SPBE;
d. Manajemen Keamanan SPBE adalah serangkaian proses untuk mencapai penerapan keamanan SPBE yang efektif, efisien, dan berkesinambungan, serta mendukung layanan SPBE yang berkualitas;
e. Layanan SPBE adalah keluaran yang dihasilkan oleh 1 (satu) atau beberapa fungsi aplikasi SPBE dan yang memiliki nilai manfaat;
f. Aplikasi SPBE adalah satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas atau fungsi Layanan SPBE;
g. Jaringan Intra adalah jaringan tertutup yang menghubungkan antar simpul jaringan dalam suatu organisasi;
h. Sistem Penghubung Layanan adalah perangkat integrasi/penghubung untuk melakukan pertukaran layanan SPBE;
i. 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;
j. *Application Programming Interface* yang selanjutnya disingkat API adalah sekumpulan perintah, fungsi, serta protokol yang mengintegrasikan dua bagian dari aplikasi atau dengan aplikasi yang berbeda secara bersamaan;
k. Pusat Data adalah fasilitas yang digunakan untuk penempatan sistem elektronik dan komponen terkait lainnya untuk keperluan penempatan, penyimpanan dan pengolahan data, dan pemulihan data;
l. Kementerian adalah Kementerian Hukum dan Hak Asasi Manusia;
m. Menteri adalah Menteri Hukum dan Hak Asasi Manusia;
n. Sekretaris Jenderal adalah Sekretaris Jenderal Kementerian Hukum dan Hak Asasi Manusia;
o. Pusat Data Kementerian adalah sekumpulan pusat data yang digunakan secara bagi pakai oleh kementerian dan saling terhubung;
p. Pejabat operasional adalah pimpinan tinggi pratama yang melaksanakan tugas dan fungsi di bidang keamanan teknologi, informasi, dan komunikasi pada unit kerja eselon I Kementerian Hukum dan Hak Asasi Manusia;

q. Pelaksana teknis adalah pejabat/administrator/koordinator yang membawahi, membangun, memelihara, dan/atau mengembangkan Aplikasi SPBE pada unit kerja eselon I Kementerian Hukum dan Hak Asasi Manusia.

5. Dasar

a. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);

b. Peraturan Presiden Nomor 18 Tahun 2023 tentang Kementerian Hukum dan Hak Asasi Manusia (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 32);

c. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 5 Tahun 2020 tentang Pedoman Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2020 Nomor 261);

d. 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);

e. Peraturan Menteri Hukum dan Hak Asasi Manusia Nomor 30 Tahun 2021 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik di Lingkungan Kementerian Hukum dan Hak Asasi Manusia (Berita Negara Republik Indonesia Tahun 2021 Nomor 949);

f. Peraturan Menteri Hukum dan Hak Asasi Manusia Nomor 41 Tahun 2021 tentang Organisasi dan Tata Kerja Kementerian Hukum dan Hak Asasi Manusia (Berita Negara Republik Indonesia Tahun 2021 Nomor 1365);

g. Peraturan Menteri Hukum dan Hak Asasi Manusia Nomor 42 Tahun 2021 tentang Uraian Fungsi Organisasi Jabatan Pimpinan Tinggi Pratama dan Tugas Koordinator Jabatan Fungsional di Lingkungan Kementerian Hukum dan Hak Asasi Manusia (Berita Negara Republik Indonesia Tahun 2021 Nomor 1366).

BAB II
MANAJEMEN KEAMANAN INFORMASI
SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

1. Penjelasan Umum

Proses manajemen keamanan informasi SPBE kementerian meliputi:

a. Penetapan ruang lingkup;
b. Penetapan penanggung jawab;
c. Perencanaan;
d. Dukungan pengoperasian;
e. Evaluasi kinerja; dan
f. Perbaikan berkelanjutan.

2. Proses Manajemen Keamanan Informasi

a. Penetapan ruang lingkup
   1) Penetapan ruang lingkup dilakukan dengan mendefinisikan:
      a) Isu internal keamanan informasi SPBE dalam organisasi; dan
      b) Isu eksternal keamanan informasi SPBE;
   2) Isu internal keamanan informasi SPBE dalam organisasi didefinisikan berdasarkan area yang menjadi prioritas organisasi terhadap pelaksanaan keamanan informasi SPBE;
   3) Area yang menjadi prioritas organisasi terhadap pelaksanaan keamanan informasi SPBE sebagaimana dimaksud paling sedikit meliputi:
      a) Data dan informasi SPBE;
      b) Aplikasi SPBE;
      c) Aset infrastruktur SPBE; dan
      d) Kebijakan keamanan informasi SPBE;
   4) Isu eksternal keamanan informasi SPBE didefinisikan sesuai dengan ketentuan peraturan perundang-undangan.

b. Penetapan penanggung jawab
   1) Penetapan penanggung jawab dilaksanakan oleh Menteri;
   2) Penanggung jawab dijabat oleh Sekretaris Jenderal;
   3) Dalam melaksanakan tugas sebagai penanggung jawab keamanan SPBE, Sekretaris Jenderal disebut sebagai Koordinator SPBE;
   4) Dalam melaksanakan tugas sebagai penanggung jawab keamanan SPBE, Koordinator SPBE menetapkan pejabat operasional dan pelaksana teknis keamanan SPBE;
   5) Pejabat operasional mempunyai tugas:
      a) Melaksanakan kebijakan manajemen keamanan informasi SPBE, standar teknis dan prosedur keamanan SPBE;
      b) Merumuskan, mengoordinasikan, dan melaksanakan program kerja dan anggaran Keamanan SPBE; dan

c) Melaporkan penerapan manajemen keamanan informasi SPBE, penerapan standar teknis dan prosedur keamanan SPBE kepada Koordinator SPBE;

6) Pelaksana teknis keamanan SPBE mempunyai tugas:

a) Melaksanakan program kerja standar teknis dan prosedur keamanan aplikasi di satuan kerja masing-masing;

b) Memastikan seluruh pembangunan atau pengembangan aplikasi dan infrastruktur SPBE memenuhi standar teknis dan prosedur keamanan SPBE yang telah ditetapkan;

c) Memastikan keberlangsungan proses bisnis SPBE;

d) Mendukung pejabat operasional dalam pelaksanaan kebijakan manajemen keamanan informasi SPBE, standar teknis dan prosedur keamanan SPBE; dan

e) Berkoordinasi dengan pejabat operasional terkait perumusan program kerja dan anggaran keamanan SPBE.

c. Perencanaan

1) Perencanaan dilakukan oleh pejabat operasional dengan merumuskan program kerja keamanan SPBE yang disusun berdasarkan kategori risiko keamanan SPBE dan target realisasi program kerja Keamanan SPBE;

2) Program kerja keamanan SPBE paling sedikit meliputi:

a) Edukasi kesadaran keamanan SPBE

Edukasi kesadaran keamanan SPBE dilaksanakan paling sedikit melalui kegiatan sosialisasi dan pelatihan;

b) Penilaian kerentanan keamanan SPBE

Penilaian kerentanan keamanan SPBE dilaksanakan paling sedikit melalui:

(1) Menginventarisasi seluruh aset SPBE meliputi data dan informasi, aplikasi, dan infrastruktur;

(2) Mengidentifikasi kerentanan dan ancaman terhadap aset SPBE; dan

(3) Mengukur tingkat risiko keamanan SPBE;

c) Peningkatan keamanan SPBE

Peningkatan keamanan SPBE dilaksanakan berdasarkan hasil dari penilaian kerentanan keamanan SPBE dengan paling sedikit melalui:

(1) Menerapkan kebijakan standar teknis dan prosedur keamanan SPBE; dan

(2) Menerapkan kebijakan keamanan terhadap aplikasi SPBE dan infrastruktur SPBE;

d) Penanganan insiden keamanan SPBE

Penanganan insiden Keamanan SPBE dilaksanakan paling sedikit melalui:

(1) Mengidentifikasi sumber serangan;

(2) Menganalisis informasi yang berkaitan dengan insiden selanjutnya;

(3) Memprioritaskan penanganan insiden berdasarkan tingkat dampak yang terjadi;

(4) Mendokumentasi bukti insiden yang terjadi; dan

(5) Memitigasi atau mengurangi dampak risiko keamanan SPBE;

e) Audit keamanan SPBE

Audit keamanan SPBE dilakukan sesuai dengan ketentuan peraturan perundang-undangan;

3) Kategori risiko keamanan SPBE ditentukan sesuai dengan ketentuan peraturan perundang-undangan;
4) Target realisasi program kerja keamanan SPBE ditetapkan berdasarkan kebutuhan Kementerian.

d. Dukungan pengoperasian
1) Dukungan pengoperasian dilakukan oleh koordinator SPBE melalui pejabat operasional;
2) Dukungan pengoperasian dilakukan dengan meningkatkan kapasitas terhadap:
a) Sumber daya manusia keamanan SPBE; dan
b) Anggaran keamanan SPBE;
3) Sumber daya manusia keamanan SPBE 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, Kementerian paling sedikit melakukan kegiatan:
a) Pelatihan dan/atau sertifikasi kompetensi keamanan infrastruktur teknologi, informasi, dan komunikasi dan keamanan aplikasi; dan
b) Bimbingan teknis mengenai standar keamanan SPBE;
5) Anggaran keamanan SPBE disusun berdasarkan perencanaan yang telah ditetapkan sesuai dengan ketentuan peraturan perundang-undangan.

e. Evaluasi kinerja
1) Evaluasi kinerja ditetapkan oleh pejabat operasional dan dilaksanakan oleh pelaksana teknis keamanan SPBE;
2) Evaluasi kinerja dilakukan terhadap pelaksanaan keamanan SPBE;
3) Evaluasi kinerja sebagaimana dimaksud pada angka (2) 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 efektifitas pelaksanaan keamanan SPBE; dan
e) Mendukung dan merealisasikan program audit keamanan SPBE;
4) Evaluasi kinerja dilaksanakan paling sedikit 1 (satu) kali dalam 1 (satu) tahun.

f. Perbaikan berkelanjutan
1) Perbaikan berkelanjutan dilakukan oleh pelaksana teknis Keamanan SPBE;
2) Perbaikan berkelanjutan merupakan tindak lanjut dari hasil evaluasi kinerja;
3) Perbaikan berkelanjutan dilakukan dengan:
a) Mengatasi permasalahan dalam pelaksanaan Keamanan SPBE; dan
b) Memperbaiki pelaksanaan Keamanan SPBE; dan
c) Melaporkan hasil pelaksanaan Keamanan SPBE secara periodik.

BAB III
STANDAR TEKNIS DAN PROSEDUR KEAMANAN SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

1. Keamanan Data dan Informasi

Standar teknis keamanan data dan informasi terdiri atas terpenuhinya aspek:

a. Kerahasiaan

Terpenuhinya aspek kerahasiaan dilakukan dengan prosedur:

1) Menetapkan klasifikasi informasi;
2) Menerapkan enkripsi dengan sistem kriptografi; dan
3) Menerapkan pembatasan akses terhadap data dan informasi sesuai dengan kewenangan dan kebijakan yang telah ditetapkan;

b. Keaslian

Terpenuhinya aspek keaslian dilakukan dengan prosedur:

1) Menyediakan mekanisme verifikasi;
2) Menyediakan mekanisme validasi; dan
3) Menerapkan sistem *hash function*;

c. Keutuhan

Terpenuhinya aspek keutuhan dilakukan dengan prosedur:

1) Menerapkan pendeteksian modifikasi; dan
2) Menerapkan tanda tangan elektronik tersertifikasi;

d. Kenirsangkalan

Terpenuhinya aspek kenirsangkalan dilakukan dengan prosedur:

1) Menerapkan tanda tangan elektronik tersertifikasi; dan
2) Penjaminan oleh penyelenggara sertifikasi elektronik melalui sertifikat elektronik;

e. Ketersediaan

Terpenuhinya aspek ketersediaan dilakukan dengan prosedur:

1) Menerapkan sistem pencadangan secara berkala;
2) Membuat perencanaan untuk menjamin data dan informasi dapat selalu diakses; dan
3) Menerapkan sistem pemulihan.

2. Keamanan Aplikasi SPBE

a. Standar teknis dan prosedur keamanan aplikasi SPBE diterapkan pada:

1) Aplikasi berbasis web

Aplikasi berbasis web merupakan aplikasi yang diakses melalui peramban saat terhubung dengan koneksi internet atau intranet;

2) Aplikasi berbasis *mobile*

Aplikasi berbasis *mobile* merupakan aplikasi yang dalam pengoperasiannya dapat berjalan di perangkat bergerak dan memiliki sistem operasi yang mendukung perangkat lunak secara *standalone*;

b. Aplikasi SPBE harus dilakukan pengujian keamanan setiap periode tertentu yang dilakukan dengan:
   1) Mengidentifikasi persyaratan minimum keamanan yang belum diterapkan;
   2) Memastikan pengkodean pemrograman aplikasi yang dibuat tidak memiliki kerawanan;
   3) Melakukan pemindaian otomatis dan/atau pengujian penetrasi sistem;
   4) Mengidentifikasi kerentanan dan mengelola ancaman sejak awal siklus pengembangan aplikasi SPBE; dan
   5) Menganalisis kerentanan;

c. Standar teknis keamanan aplikasi berbasis web terdiri atas terpenuhinya fungsi:
   1) Autentikasi

      Terpenuhinya fungsi autentikasi 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;
   2) Manajemen sesi

      Terpenuhinya fungsi manajemen sesi 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;
   3) Persyaratan kontrol akses

      Terpenuhinya fungsi persyaratan kontrol akses 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;
   4) Validasi input

      Terpenuhinya fungsi validasi input 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;

5) Kriptografi pada verifikasi statis

Terpenuhinya fungsi kriptografi pada verifikasi statis 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;

6) Penanganan eror dan pencatatan log

Terpenuhinya fungsi penanganan eror dan pencatatan log 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;

7) Proteksi data

Terpenuhinya fungsi proteksi data 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;

8) Keamanan komunikasi

Terpenuhinya fungsi keamanan komunikasi 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; dan
d) mengatur aktivasi dan konfigurasi sertifikat elektronik yang diterbitkan oleh penyelenggara sertifikasi elektronik;

9) Pengendalian kode berbahaya

Terpenuhinya fungsi pengendalian kode berbahaya 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;

10) Logika bisnis

Terpenuhinya fungsi logika bisnis 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 antiotomatisasi; dan
e) Memberikan peringatan ketika terjadi serangan otomatis atau aktivitas yang tidak biasa;

11) *File*;

Terpenuhinya fungsi *file* 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;

12) Keamanan API dan web *service*

Terpenuhinya fungsi keamanan API dan web *service* 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 antiotomatisasi;

13) Keamanan konfigurasi

Terpenuhinya fungsi keamanan konfigurasi dilakukan dengan prosedur:

a) Mengonfigurasi *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 respons aplikasi dan konten yang aman;

d. Standar teknis keamanan aplikasi berbasis mobile terdiri atas terpenuhinya fungsi:

1) Penyimpanan data dan persyaratan privasi

Terpenuhinya fungsi penyimpanan data dan persyaratan privasi 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;

2) Kriptografi

Terpenuhinya fungsi kriptografi 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;

3) Autentikasi dan manajemen sesi

Terpenuhinya fungsi autentikasi dan manajemen sesi 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*;

4) Komunikasi jaringan

Terpenuhinya fungsi komunikasi jaringan dilakukan dengan prosedur:

a) Menerapkan *secure socket layer* atau *transport layer security* yang tidak obsolet secara konsisten; dan
b) Memverifikasi sertifikat *remote endpoint*;

5) Interaksi platform

Terpenuhinya fungsi interaksi platform 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;

6) Kualitas kode dan pengaturan *build*

Terpenuhinya fungsi kualitas kode dan pengaturan *build* 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;

7) Ketahanan

Terpenuhinya fungsi ketahanan 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*.

3. Keamanan Sistem Penghubung Layanan

a. Standar teknis keamanan sistem penghubung layanan terdiri atas terpenuhinya fungsi:

1) Keamanan interoperabilitas data dan informasi

Keamanan interoperabilitas data dan informasi 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 *hash function* pada *file*;

2) Kontrol sistem integrasi

Kontrol sistem integrasi dilakukan dengan prosedur:

a) Menerapkan protokol *secure socket layer* atau *protokol transport layer security* versi terbaru 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 per seratus persen); dan
n) Memastikan sistem integrasi tidak memiliki kerentanan yang berpotensi menjadi celah peretas;

3) Kontrol perangkat integrator

Kontrol perangkat integrator dilakukan dengan prosedur:

a) Menggunakan sistem operasi dan perangkat lunak dengan *security patches* terbaru;
b) Menggunakan anti virus dan *anti-spyware* terbaru;
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 *system recovery* dan *restore* pada perangkat integrator;

4) Keamanan API dan *web service*

Keamanan API dan *web service* 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 terbaru 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;

5) Keamanan migrasi data

Keamanan migrasi data 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;

b. Mekanisme teknis keamanan sistem penghubung layanan dilakukan melalui aplikasi, perkembangan ilmu pengetahuan dan teknologi, dan sesuai dengan ketentuan peraturan perundang-undangan.

4. Keamanan Jaringan Intra

Standar teknis keamanan jaringan intra terdiri atas terpenuhinya:

1) Aspek administrasi keamanan jaringan intra

Aspek administrasi keamanan jaringan intra 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;

2) Kontrol akses dan autentikasi

Kontrol akses dan autentikasi 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 terbaru pada jalur akses jaringan intra; dan

l) Menerapkan server perantara saat *client* mengakses *server database* dalam rangka pemeliharaan;

3) Persyaratan perangkat dan aplikasi keamanan jaringan intra

Terpenuhinya persyaratan perangkat dan aplikasi keamanan jaringan intra dilakukan dengan prosedur:

a) Menggunakan perangkat *security information and event management* 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;

4) Kontrol keamanan *gateway*

Kontrol keamanan *gateway* dilakukan dengan prosedur:

a) Menerapkan *content filtering*;

b) Menerapkan *inspection packet filtering* untuk memeriksa *packet* 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*;

5) Kontrol keamanan *access point* pada jaringan nirkabel

Kontrol keamanan *access point* pada jaringan nirkabel dilakukan dengan prosedur:

a) Menerapkan protokol keamanan *access point nirkabel* dan teknologi enkripsi terbaru;

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;

6) Kontrol konfigurasi *access point* pada jaringan nirkabel

Kontrol konfigurasi *access point* pada jaringan nirkabel 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 autentikasi 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.

5. Keamanan Pusat Data

Standar teknis keamanan pusat data terdiri atas terpenuhinya:

a. Persyaratan keamanan fisik dan manajemen pusat data

Persyaratan keamanan fisik dan manajemen pusat data dilakukan dengan prosedur sesuai dengan Standar Nasional Indonesia yang terkait dengan pusat data;

b. Persyaratan koneksi perangkat ke pusat data

Persyaratan koneksi perangkat ke pusat data dilakukan dengan prosedur:

1) Memastikan keamanan perangkat yang terkoneksi ke infrastruktur pusat data;
2) Memutus akses fisik atau *logic* dari perangkat yang tidak terotorisasi;
3) Memastikan akses tingkat administrator ke *server* dan perangkat jaringan utama tidak boleh dilakukan secara *remote*;
4) Memastikan hanya personil yang berwenang yang boleh menggunakan komputer di area pusat data;
5) Melakukan backup informasi dan perangkat lunak yang berada di pusat data secara berkala;
6) Memastikan perangkat komputer pusat data terbebas dari *virus* dan *malware*;
7) Melakukan pembatasan akses pemanfaatan *removable media* di area pusat data;
8) Memastikan pengaktifan konfigurasi *port universal serial bus* telah mendapatkan izin dari personil yang berwenang;
9) Memastikan setiap perangkat yang akan terkoneksi ke infrastruktur pusat data menggunakan *internet protocol address* dan *hostname* yang telah ditentukan; dan
10) Menerapkan *server* perantara saat *client* mengakses *server database* dalam rangka pemeliharaan.

BAB IV
PENUTUP

Pedoman Menteri Hukum dan Hak Asasi Manusia tentang Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik di Lingkungan Kementerian Hukum dan Hak Asasi Manusia ini merupakan wujud tata kelola dan manajemen keamanan informasi SPBE Kementerian Hukum dan Hak Asasi Manusia agar dapat meningkatkan kualitas penerapan kebijakan SPBE yang lebih baik dan optimal di lingkungan Kementerian Hukum dan Hak Asasi Manusia.

Diharapkan pedoman ini bermanfaat bagi seluruh pihak dalam penyelenggaraan SPBE Kementerian Hukum dan Hak Asasi Manusia.

Jakarta, 29 Maret 2023

MENTERI HUKUM DAN HAK ASASI MANUSIA,

YASONNA H. LAOLY

SEKRETARIAT JENDERAL KEMENTERIAN HUKUM DAN HAK ASASI MANUSIA
PUSAT DATA DAN TEKNOLOGI INFORMASI
Jl. HR Rasuna Said Kav 6-7 Kuningan
Jakarta Selatan 12940
(021) 5263082
pusdatin@kemenkumham.go.id