



SALINAN

GUBERNUR KEPULAUAN RIAU  
PERATURAN GUBERNUR KEPULAUAN RIAU  
NOMOR 50 TAHUN 2022

TENTANG

PEDOMAN MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN  
BERBASIS ELEKTRONIK DAN STANDAR TEKNIS SERTA PROSEDUR  
KEAMANAN SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DI  
LINGKUNGAN PEMERINTAH PROVINSI KEPULAUAN RIAU

DENGAN RAHMAT TUHAN YANG MAHA ESA

GUBERNUR KEPULAUAN RIAU,

Menimbang : bahwa untuk melaksanakan ketentuan Pasal 13 ayat (1) dan Pasal 41 ayat (1) huruf c Peraturan Gubernur Kepulauan Riau Nomor 9 Tahun 2022 tentang Sistem Pemerintahan Berbasis Elektronik di Lingkungan Pemerintah Provinsi Kepulauan Riau, perlu menetapkan Peraturan Gubernur tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik di lingkungan Pemerintah Provinsi Kepulauan Riau;

Mengingat : 1. Pasal 18 ayat (6) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;

2. Undang-Undang Nomor 25 Tahun 2002 tentang Pembentukan Provinsi Kepulauan Riau (Lembaran Negara Republik Indonesia Tahun 2002 Nomor 111, Tambahan Lembaran Negara Republik Indonesia Nomor 4237);

3. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843);

4. Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 671, Tambahan Lembaran Negara Republik Indonesia Nomor 4846);

- Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 671, Tambahan Lembaran Negara Republik Indonesia Nomor 4846);
5. Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik (Lembaran Negara Republik Indonesia Tahun 2009 Nomor 112, Tambahan Lembaran Negara Republik Indonesia Nomor 5038);
  6. Undang-Undang Nomor 5 Tahun 2014 tentang Aparatur Sipil Negara (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 6, Tambahan Lembaran Negara Republik Indonesia Nomor 5494);
  7. Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 224, Tambahan Lembaran Negara Republik Indonesia Nomor 5587) sebagaimana telah diubah beberapa kali terakhir dengan Undang Nomor 9 Tahun 2015 tentang Perubahan Kedua Atas Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2015 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 5679);
  8. Undang-Undang Nomor 30 Tahun 2014 tentang Administrasi Pemerintahan (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 292, Tambahan Lembaran Negara Republik Indonesia Nomor 5601);
  9. Undang-Undang Nomor 1 Tahun 2022 tentang Hubungan Keuangan antara Pemerintah Pusat dan Pemerintah Daerah (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 4, Tambahan Lembaran Negara Republik Indonesia Nomor 6757);
  10. Peraturan Pemerintah Nomor 52 Tahun 2000 tentang Penyelenggaraan Telekomunikasi (Lembaran Negara Republik Indonesia Tahun 2000 Nomor 107, Tambahan Lembaran Negara Republik Indonesia Nomor 3980);
  11. Peraturan Pemerintah Nomor 56 Tahun 2001 tentang Pelaporan Penyelenggaraan Pemerintah Daerah (Lembaran Negara Republik Indonesia Tahun 2001 Nomor 100, Tambahan Lembaran Negara Republik Indonesia Nomor 4124);

12. Peraturan Pemerintah Nomor 61 Tahun 2010 tentang Pelaksanaan Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (Lembaran Negara Republik Indonesia Tahun 2010 Nomor 99, Tambahan Lembaran Negara Republik Indonesia Nomor 5149);
13. Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2012 Nomor 189, Tambahan Lembaran Negara Republik Indonesia Nomor 5348);
14. Peraturan Pemerintah Nomor 96 Tahun 2012 tentang Pelaksanaan undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik (Lembaran Negara Republik Indonesia Tahun 2012 Nomor 215 Tambahan Lembaran Negara Republik Indonesia Nomor 5357);
15. Peraturan Pemerintah Nomor 12 Tahun 2019 tentang Pengelolaan Keuangan Daerah (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 42, Tambahan Lembaran Negara Republik Indonesia Nomor 6322);
16. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185, Tambahan Lembaran Negara Republik Indonesia Nomor 6400);
17. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
18. Peraturan Presiden Nomor 39 Tahun 2019 tentang Satu Data Indonesia (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 112);
19. Peraturan Menteri Komunikasi dan Informatika Nomor 41/PER/MEN.KOMINFO/11/2007 tentang panduan Umum Tata Kelola Teknologi Informasi dan Komunikasi Daerah;
20. Peraturan Menteri Dalam Negeri Nomor 35 Tahun 2010 tentang Pedoman dan Pelayanan Informasi dan Dokumentasi di Lingkungan Kementerian Dalam Negeri dan Pemerintah Daerah (Berita Negara Republik Indonesia Tahun 2010 Nomor 245);

21. Peraturan Menteri Komunikasi dan Informatika Nomor 8 Tahun 2019 tentang Penyelenggaraan Urusan Pemerintahan Konkuren Bidang Komunikasi dan Informatika (Berita Negara Republik Indonesia Tahun 2019 Nomor 1026);
22. Peraturan Menteri Pendayagunaan Aparatur Negara Dan Reformasi Birokrasi Republik Indonesia Nomor 5 Tahun 2020 tentang Pedoman Manajemen Resiko Sistem pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2020 Nomor 261);
23. 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);
24. Peraturan Menteri Dalam Negeri Nomor 77 Tahun 2020 tentang Pedoman Teknis Pengelolaan Keuangan Daerah (Berita Negara Republik Indonesia Tahun 2020 Nomor 1781);
25. 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);
26. Peraturan Daerah Provinsi Kepulauan Riau Nomor 4 Tahun 2016 tentang Penyelenggaraan Pelayanan Publik (Lembaran Daerah Provinsi Kepulauan Riau Tahun 2016 Nomor 4, Tambahan Lembaran Daerah Provinsi Kepulauan Riau Nomor 39);
27. Peraturan Daerah Provinsi Kepulauan Riau Nomor 4 Tahun 2021 tentang Pembentukan dan Susunan Perangkat Daerah (Lembaran Daerah Provinsi Kepulauan Riau Tahun 2021 Nomor 4, Tambahan Lembaran Daerah Provinsi Kepulauan Riau Nomor 55);
28. Peraturan Gubernur Kepulauan Riau Nomor 92 Tahun 2021 tentang Kedudukan, Susunan Organisasi, Tugas dan Fungsi, Serta Tata Kerja Perangkat Daerah (Berita Daerah Provinsi Kepulauan Riau Tahun 2021 Nomor 816);

29. Peraturan Gubernur Kepulauan Riau Nomor 9 Tahun 2022 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik Di Lingkungan Pemerintah Provinsi Kepulauan Riau (Berita Daerah Provinsi Kepulauan Riau Tahun 2022 Nomor 827);

MEMUTUSKAN:

Menetapkan : PERATURAN GUBERNUR TENTANG PEDOMAN MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DAN STANDAR TEKNIS SERTA PROSEDUR KEAMANAN SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DI LINGKUNGAN PEMERINTAH PROVINSI KEPULAUAN RIAU.

BAB I  
KETENTUAN UMUM  
Pasal 1

Dalam Peraturan Gubernur ini yang dimaksud dengan:

1. Daerah adalah Provinsi Kepulauan Riau.
2. Pemerintah Daerah adalah Pemerintah Provinsi Kepulauan Riau.
3. Gubernur adalah Gubernur Kepulauan Riau.
4. Sekretaris Daerah adalah Sekretaris Daerah Provinsi Kepulauan Riau.
5. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintah yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada pengguna SPBE.
6. Keamanan SPBE adalah Pengendalian Keamanan yang terpadu dalam SPBE.
7. Manajemen Keamanan SPBE adalah serangkaian Proses untuk mencapai penerapan keamanan SPBE yang efektif, efisien, dan berkesinambungan, serta mendukung layanan SPBE yang berkualitas.
8. Layanan SPBE adalah keluaran yang dihasilkan oleh 1 (satu) atau beberapa fungsi aplikasi SPBE dan yang memiliki nilai manfaat.
9. Aplikasi SPBE adalah satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas atau fungsi layanan SPBE.
10. 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.
11. Pusat Data adalah fasilitas yang digunakan untuk penempatan sistem elektronik dan komponen terkait

- lainnya untuk keperluan penempatan, penyimpanan dan pengolahan data, dan pemulihan data.
12. Pusat Data Daerah adalah sekumpulan Pusat Data yang digunakan secara bagi pakai oleh Instansi Pusat dan Pemerintah Daerah, dan yang saling terhubung.
  13. Jaringan Intra Pemerintah Daerah adalah jaringan tertutup yang menghubungkan antar simpul jaringan dalam Organisasi.
  14. Sistem Penghubung Layanan adalah perangkat integrasi/ penghubung untuk melakukan pertukaran Layanan SPBE;
  15. Teknologi Informasi dan Komunikasi yang selanjutnya disingkat TIK adalah suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, membuat laporan menganalisis memindahkan informasi dan/atau menyebarkan informasi antar media.yang mengintegrasikan dua bagian dari aplikasi atau dengan aplikasi yang berbeda secara bersamaan.
  16. *Application Programming Interface* yang selanjutnya disingkat API adalah sekumpulan perintah, fungsi, serta protocol.
  17. Komputer adalah alat untuk memproses data elektronik, magnetik, optik, atau sistem yang melaksanakan fungsi logika, aritmatika, dan penyimpanan.
  18. *Bring Your Own Device* yang selanjutnya disingkat BYOD adalah pengaturan kebijakan terhadap perangkat komputer yang sifatnya bergerak dan digunakan di Pemerintah Daerah.
  19. *Phassprase/password* adalah serangkaian angka dan/atau huruf dan/atau karakter tertentu yang digunakan sebagai alat autentikasi untuk melakukan akses ke pasangan kunci privat.
  20. Perangkat Lunak adalah satu atau sekumpulan program komputer, prosedur, dan/atau dokumentasi yang terkait dalam pengoperasian Sistem Elektronik.
  21. Lisensi adalah ijin yang diberikan oleh pemegang hak cipta atau perangkat lunak kepada pihak lain yang akan menggunakan perangkat lunak tersebut

BAB II  
MAKSUD DAN TUJUAN  
Pasal 2

- (1) Maksud ditetapkannya Peraturan Gubernur ini sebagai pedoman manajemen serta standar teknis dan prosedur keamanan SPBE di Lingkungan Provinsi Kepulauan Riau.
- (2) Peraturan Gubernur ini bertujuan sebagai panduan bagi seluruh OPD, unit kerja dan pegawai dalam pelaksanaan manajemen keamanan informasi dalam penerapan standar teknis dan prosedur keamanan SPBE di lingkungan

Pemerintah Provinsi Kepulauan Riau.

BAB III  
PEDOMAN MANAJEMEN KEAMANAN INFORMASI  
SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK  
Pasal 3

Manajemen keamanan informasi SPBE dilaksanakan oleh Pemerintah Daerah berdasarkan pedoman manajemen keamanan informasi SPBE.

Pasal 4

- (1) Manajemen keamanan informasi SPBE di lingkungan Pemerintah Daerah sebagaimana dimaksud dalam Pasal 3 merupakan acuan dalam melaksanakan serangkaian proses manajemen keamanan informasi yang meliputi:
  - a. penetapan ruang lingkup;
  - b. penetapan penanggung jawab;
  - c. perencanaan;
  - d. dukungan pengoperasian;
  - e. evaluasi kinerja; dan
  - f. perbaikan berkelanjutan.
- (2) Proses sebagaimana dimaksud pada ayat (1) ditetapkan oleh Gubernur.
- (3) Pemerintah Daerah mengomunikasikan dan mendokumentasikan kegiatan manajemen keamanan informasi SPBE masing-masing.
- (4) Proses sebagaimana dimaksud pada ayat (2) dilakukan dengan mendefinisikan:
  - a. isu internal keamanan informasi SPBE dalam organisasi; dan
  - b. isu eksternal keamanan informasi SPBE.
- (5) Isu internal sebagaimana dimaksud pada ayat (4) huruf a didefinisikan berdasarkan area yang menjadi prioritas organisme terhadap pelaksanaan keamanan informasi SPBE.
- (6) Area sebagaimana dimaksud pada ayat (5) paling sedikit meliputi:
  - a. data dan informasi SPBE;
  - b. Aplikasi SPBE;
  - c. aset Infrastruktur SPBE; dan
  - d. kebijakan keamanan informasi SPBE yang telah dimiliki.
- (7) Isu eksternal sebagaimana dimaksud pada ayat (4) huruf b didefinisikan sesuai dengan ketentuan peraturan perundang-undangan.

#### Pasal 5

- (1) Penetapan Penanggung jawab sebagaimana dimaksud dalam Pasal 4 ayat (1) huruf b ditetapkan oleh Gubernur.
- (2) Penanggung jawab sebagaimana dimaksud pada ayat (1) dijabat oleh Sekretaris Daerah.
- (3) Dalam melaksanakan tugas penanggung jawab sebagaimana dimaksud pada ayat (2), disebut juga sebagai koordinator SPBE.

#### Pasal 6

- (1) Koordinator SPBE sebagaimana dimaksud dalam Pasal 5 ayat (3) menetapkan pelaksana teknis Keamanan SPBE.
- (2) Pelaksana teknis Keamanan SPBE sebagaimana dimaksud pada ayat (1) terdiri atas:
  - a. pejabat pimpinan tinggi pratama yang melaksanakan tugas dan fungsi di bidang keamanan teknologi, informasi dan komunikasi; dan
  - b. pejabat pimpinan tinggi atau pejabat administrator yang membawahi, membangun, memelihara, dan/atau mengembangkan Aplikasi SPBE.

#### Pasal 7

- (1) Pejabat pimpinan tinggi pratama yang melaksanakan tugas dan fungsi di bidang keamanan teknologi, informasi dan komunikasi sebagaimana dimaksud dalam Pasal 6 ayat (2) huruf a mempunyai tugas sebagai berikut:
  - a. memastikan penerapan standar teknis dan prosedur Keamanan SPBE;
  - b. merumuskan, mengoordinasikan, dan melaksanakan program kerja dan anggaran Keamanan SPBE; dan
  - c. melaporkan pelaksanaan manajemen keamanan informasi SPBE dan penerapan standar teknis dan prosedur Keamanan SPBE kepada koordinator SPBE.
- (2) Pejabat pimpinan tinggi atau pejabat administrator yang membawahi, membangun, memelihara, dan/atau mengembangkan Aplikasi SPBE sebagaimana dimaksud dalam Pasal 6 ayat (2) huruf b mempunyai tugas sebagai berikut:
  - a. menerapkan standar teknis dan prosedur keamanan aplikasi di unit kerja masing-masing;
  - b. memastikan seluruh pembangunan atau pengembangan Aplikasi dan Infrastruktur SPBE yang dilakukan oleh pihak ketiga memenuhi standar teknis dan prosedur Keamanan SPBE yang telah ditetapkan;
  - c. memastikan keberlangsungan proses bisnis SPBE; dan
  - d. berkoordinasi dengan pejabat pimpinan tinggi pratama

yang melaksanakan tugas dan fungsi di bidang keamanan teknologi, informasi dan komunikasi terkait perumusan program kerja dan anggaran Keamanan SPBE.

#### Pasal 8

- (1) Perencanaan sebagaimana dimaksud dalam Pasal 4 ayat (1) huruf c dilakukan oleh pelaksana teknis Keamanan SPBE.
- (2) Perencanaan sebagaimana dimaksud pada ayat (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 ayat (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 ayat (2) huruf a ditentukan sesuai dengan ketentuan peraturan perundang-undangan.
- (5) Target realisasi program kerja Keamanan SPBE sebagaimana dimaksud pada ayat (2) huruf b ditetapkan berdasarkan kebutuhanan Pemerintah Daerah.

#### Pasal 9

Edukasi kesadaran Keamanan SPBE sebagaimana dimaksud dalam Pasal 8 ayat (3) huruf a dilaksanakan paling sedikit melalui kegiatan:

- a. sosialisasi; dan
- b. pelatihan.

#### Pasal 10

Penilaian kerentanan Keamanan SPBE sebagaimana dimaksud dalam Pasal 8 ayat (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 asset SPBE; dan
- c. mengukur tingkat risiko Keamanan SPBE.

#### Pasal 11

- (1) Peningkatan Keamanan SPBE sebagaimana dimaksud dalam Pasal 8 ayat (3) huruf c dilaksanakan berdasarkan hasil dari penilaian kerentanan Keamanan SPBE sebagaimana dimaksud dalam Pasal 10.
- (2) Peningkatan Keamanan SPBE dilaksanakan paling sedikit melalui:
  - a. menerapkan standar teknis dan prosedur Keamanan SPBE; dan
  - b. menguji fungsi keamanan terhadap Aplikasi SPBE dan Infrastruktur SPBE.

#### Pasal 12

Penanganan insiden Keamanan SPBE sebagaimana dimaksud dalam Pasal 8 ayat (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.

#### Pasal 13

Audit Keamanan SPBE sebagaimana dimaksud dalam Pasal 8 ayat (3) huruf e dilakukan sesuai dengan ketentuan peraturan perundang-undangan.

#### Pasal 14

- (1) Dukungan pengoperasian sebagaimana dimaksud dalam Pasal 4 ayat (1) huruf d dilakukan oleh koordinator SPBE.
- (2) Dukungan pengoperasian sebagaimana dimaksud pada ayat (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 ayat (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

ayat (3), Pemerintah Daerah 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 sebagaimana dimaksud pada ayat (2) huruf b disusun berdasarkan perencanaan yang telah ditetapkan sesuai dengan ketentuan peraturan perundang-undangan.

#### Pasal 15

- (1) Evaluasi kinerja sebagaimana dimaksud dalam Pasal 3 ayat (1) huruf e dilakukan oleh koordinator SPBE.
- (2) Evaluasi kinerja sebagaimana dimaksud pada ayat (1) dilakukan terhadap pelaksanaan Keamanan SPBE.
- (3) Evaluasi kinerja sebagaimana dimaksud pada ayat (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 sebagaimana dimaksud pada ayat (1) dilaksanakan paling sedikit 1 (satu) kali dalam 1 (satu) tahun.

#### Pasal 16

- (1) Perbaikan berkelanjutan sebagaimana dimaksud dalam Pasal 4 ayat (1) huruf f dilakukan oleh pelaksana teknis Keamanan SPBE.
- (2) Perbaikan berkelanjutan sebagaimana dimaksud pada ayat (1) merupakan tindak lanjut dari hasil evaluasi kinerja.
- (3) Perbaikan berkelanjutan sebagaimana dimaksud pada ayat (1) dilakukan dengan:
  - a. mengatasi permasalahan dalam pelaksanaan Keamanan SPBE; dan
  - b. memperbaiki pelaksanaan Keamanan SPBE secara periodik.

BAB IV  
STANDAR TEKNIS DAN PROSEDUR KEAMANAN  
SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

Bagian Kesatu  
Umum  
Pasal 17

- (1) Pemerintah Daerah harus menerapkan Keamanan SPBE.
- (2) Penerapan Keamanan SPBE sebagaimana dimaksud pada ayat (1) harus memenuhi standar teknis dan prosedur Keamanan SPBE.

Pasal 18

Standar teknis dan prosedur Keamanan SPBE sebagaimana dimaksud dalam Pasal 17 ayat (2) diterapkan untuk:

- a. keamanan data dan informasi;
- b. keamanan Aplikasi SPBE;
- c. keamanan Sistem Penghubung Layanan;
- d. keamanan Jaringan Intra.
- e. keamanan Pusat Data Daerah; dan
- f. keamanan BYOD.

Bagian Kedua  
Keamanan data dan informasi  
Pasal 19

Standar teknis keamanan data dan informasi sebagaimana dimaksud dalam Pasal 18 huruf a terdiri atas:

- a. kerahasiaan;
- b. keaslian;
- c. keutuhan;
- d. kenirsangkalan; dan
- e. ketersediaan.

Pasal 20

Terpenuhinya aspek kerahasiaan sebagaimana dimaksud dalam Pasal 19 huruf a dilakukan dengan prosedur:

- a. menetapkan 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.

Pasal 21

Terpenuhinya aspek keaslian sebagaimana dimaksud dalam

Pasal 19 huruf b dilakukan dengan prosedur:

- a. menyediakan mekanisme verifikasi;
- b. menyediakan mekanisme validasi; dan
- c. menerapkan sistem *hash function*.

#### Pasal 22

Terpenuhinya aspek keutuhan sebagaimana dimaksud dalam Pasal 19 huruf c dilakukan dengan prosedur:

- a. menerapkan pendeteksian modifikasi; dan
- b. menerapkan tanda tangan elektronik tersertifikasi.

#### Pasal 23

Terpenuhinya aspek kenirsangkalan sebagaimana dimaksud dalam Pasal 19 huruf d dilakukan dengan prosedur:

- a. menerapkan tanda tangan elektronik tersertifikasi; dan
- b. penjaminan oleh penyelenggara sertifikasi elektronik melalui sertifikat elektronik.

#### Pasal 24

Terpenuhinya aspek ketersediaan sebagaimana dimaksud dalam Pasal 19 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.

### Bagian Ketiga Keamanan Aplikasi SPBE Pasal 25

- (1) Standar teknis dan prosedur keamanan Aplikasi SPBE sebagaimana dimaksud dalam Pasal 18 huruf b diterapkan pada:
  - a. aplikasi berbasis web; dan
  - b. aplikasi berbasis *mobile*.
- (2) Aplikasi berbasis web sebagaimana dimaksud pada ayat (1) huruf a merupakan aplikasi yang diakses melalui peramban saat terhubung dengan koneksi internet atau intranet.
- (3) Aplikasi berbasis *mobile* sebagaimana dimaksud pada ayat (1) huruf b merupakan aplikasi yang dalam pengoperasiannya dapat berjalan diperangkat bergerak, dan memiliki sistem operasi yang mendukung perangkat lunak secara *standalone*.
- (4) Aplikasi SPBE sebagaimana dimaksud pada ayat (1) 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.

#### Pasal 26

Standar teknis keamanan aplikasi berbasis web sebagaimana dimaksud dalam Pasal 25 ayat (1) huruf a terdiri atas:

- 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.

#### Pasal 27

(1) Terpenuhinya fungsi autentikasi sebagaimana dimaksud dalam Pasal 26 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.

(2) Terpenuhinya fungsi manajemen sesi sebagaimana dimaksud dalam Pasal 26 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. perlindungan terhadap lokasi dan pengiriman token untuk sesi terautentikasi; dan
  - g. perlindungan terhadap duplikasi dan mekanisme persetujuan pengguna.
- (3) Terpenuhinya fungsi persyaratan kontrol akses sebagaimana dimaksud dalam Pasal 26 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.
- (4) Terpenuhinya fungsi validasi input sebagaimana dimaksud dalam Pasal 26 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 perlindungan terhadap akses yang mengandung konten skrip; dan
  - h. melakukan perlindungan dari serangan injeksi basis data.
- (5) Terpenuhinya fungsi kriptografi pada verifikasi statis sebagaimana dimaksud dalam Pasal 26 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 dienkrripsi;
  - c. menerapkan manajemen kunci kriptografi; dan
  - d. membuat angka acak yang menggunakan generator angka acak kriptografi.
- (6) Terpenuhinya fungsi penanganan eror dan pencatatan log sebagaimana dimaksud dalam Pasal 26 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 perlindungan 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) Terpenuhiya fungsi proteksi data sebagaimana dimaksud dalam Pasal 26 huruf g dilakukan dengan prosedur:
- a. melakukan identifikasi dan penyimpanan salinan informasi yang dikecualikan;
  - b. melakukan perlindungan 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 mengeksport data sesuai permintaan pengguna; dan
  - g. membersihkan memori setelah tidak diperlukan.
- (8) Terpenuhiya fungsi keamanan komunikasi sebagaimana dimaksud dalam Pasal 26 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; dan
  - d. mengatur aktivasi dan konfigurasi sertifikat elektronik yang diterbitkan oleh penyelenggara sertifikasi elektronik.
- (9) Terpenuhiya fungsi pengendalian kode berbahaya sebagaimana dimaksud dalam Pasal 26 huruf i dilakukan dengan prosedur:
- a. menggunakan analisis kode dalam control 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 perlindungan integritas; dan
  - e. mengatur mekanisme fitur pembaruan.
- (10) Terpenuhinya fungsi logika bisnis sebagaimana dimaksud dalam Pasal 26 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 antiotomatisasi; dan
  - e. memberikan peringatan Ketika terjadi serangan otomatis atau aktivitas yang tidak biasa.
- (11) Terpenuhinya fungsi *file* sebagaimana dimaksud dalam Pasal 26 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 perlindungan 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) Terpenuhinya fungsi keamanan API dan *web service* sebagaimana dimaksud dalam Pasal 26 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 perlindungan layanan berbasis web; dan
  - g. menerapkan kontrol antiotomatisasi.
- (13) Terpenuhinya fungsi keamanan konfigurasi sebagaimana dimaksud dalam Pasal 26 huruf m 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.

#### Pasal 28

Standar teknis keamanan aplikasi berbasis mobile sebagaimana dimaksud dalam Pasal 25 ayat (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.

#### Pasal 29

- (1) Terpenuhinya fungsi penyimpanan data dan persyaratan privasi sebagaimana dimaksud dalam Pasal 28 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.
- (2) Terpenuhinya fungsi kriptografi sebagaimana dimaksud dalam Pasal 28 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 algoritme kriptografi yang obsolet;
  - d. menghindari penggunaan kunci kriptografi yang sama; dan
  - e. menggunakan pembangkit kunci acak yang memenuhi kriteria keacakan kunci.
- (3) Terpenuhinya fungsi autentikasi dan manajemen sesi sebagaimana dimaksud dalam Pasal 28 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 algoritme 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) Terpenuhinya fungsi komunikasi jaringan sebagaimana dimaksud dalam Pasal 28 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*.
- (5) Terpenuhinya fungsi interaksi platform sebagaimana dimaksud dalam Pasal 28 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.
- (6) Terpenuhinya fungsi kualitas kode dan pengaturan *build* sebagaimana dimaksud dalam Pasal 28 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.
- (7) Terpenuhinya fungsi ketahanan sebagaimana dimaksud dalam Pasal 28 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*.

Bagian Keempat  
Keamanan Sistem Penghubung Layanan  
Pasal 30

Standar teknis keamanan Sistem Penghubung Layanan sebagaimana dimaksud dalam Pasal 18 huruf c 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.

Pasal 31

- (1) Terpenuhinya fungsi keamanan interoperabilitas data dan informasi sebagaimana dimaksud dalam Pasal 30 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 *hash function* pada *file*.
- (2) Terpenuhinya fungsi kontrol sistem integrasi sebagaimana dimaksud dalam Pasal 30 huruf b dilakukan dengan prosedur:

- a. menerapkan protocol *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 per seratus); dan
  - n. memastikan sistem integrasi tidak memiliki kerentanan yang berpotensi menjadi celah peretas.
- (3) Terpenuhinya fungsi control perangkat integrator sebagaimana dimaksud dalam Pasal 30 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.
- (4) Terpenuhinya fungsi keamanan API dan *web service* sebagaimana dimaksud dalam Pasal 30 huruf d dilakukan dengan prosedur:
- a. menerapkan protocol *secure socket layer* atau protokol *transport layer security* diantar 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.
- (5) Terpenuhinya fungsi keamanan migrasi data sebagaimana dimaksud dalam Pasal 30 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.

Bagian Kelima  
Keamanan Jaringan Intra  
Pasal 32

- (1) Standar teknis keamanan Jaringan Intra sebagaimana dimaksud dalam Pasal 18 huruf d diterapkan pada:
- a. Jaringan Intra pemerintah; dan
  - b. Jaringan Intra Instansi Pusat dan Pemerintah Daerah.
- (2) Standar teknis keamanan Jaringan Intra sebagaimana dimaksud pada ayat (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.

- (1) Terpenuhinya aspek administrasi keamanan Jaringan Intra sebagaimana dimaksud dalam Pasal 32 ayat (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.
- (2) Terpenuhinya kontrol akses dan autentikasi sebagaimana dimaksud dalam Pasal 32 ayat (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.
- (3) Terpenuhinya persyaratan perangkat dan aplikasi keamanan Jaringan Intra sebagaimana dimaksud dalam Pasal 32 ayat (2) huruf c 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) Terpenuhinya kontrol keamanan *gateway* sebagaimana dimaksud dalam Pasal 32 ayat (2) huruf d 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) Terpenuhinya kontrol keamanan *access point* pada jaringan nirkabel sebagaimana dimaksud dalam Pasal 32 ayat (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.
- (7) Terpenuhinya control konfigurasi *access point* pada jaringan nirkabel sebagaimana dimaksud dalam Pasal 32 ayat (2) huruf f dilakukan dengan prosedur:
- a. menggunakan kata sandi yang kuat;
  - b. menggunakan protocol 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.

Bagian Keenam  
Keamanan Pusat Data Daerah  
Pasal 34

Standar teknis keamanan Pusat Data Daerah sebagaimana dimaksud dalam Pasal 18 huruf e terdiri atas terpenuhinya:

- a. persyaratan keamanan fisik dan manajemen Pusat Data Daerah; dan
- b. persyaratan koneksi perangkat ke Pusat Data Daerah.

Pasal 35

- (1) Terpenuhinya persyaratan keamanan fisik dan manajemen Pusat Data Daerah sebagaimana dimaksud dalam Pasal 34 huruf a dilakukan dengan prosedur sesuai dengan Standar Nasional Indonesia yang terkait dengan Pusat Data.
- (2) Terpenuhinya persyaratan koneksi perangkat ke Pusat Data Daerah sebagaimana dimaksud dalam Pasal 34 huruf b dilakukan dengan prosedur:
  - a. memastikan keamanan perangkat yang terkoneksi ke infrastruktur Pusat Data Daerah;
  - 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 Daerah;
  - e. melakukan *backup* informasi dan perangkat lunak yang berada di Pusat Data Daerah secara berkala;
  - f. memastikan perangkat komputer Pusat Data Daerah terbebas dari virus dan *malware*;
  - g. melakukan pembatasan akses pemanfaatan *removable media* di area Pusat Data Daerah;
  - 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 Daerah menggunakan *internet protocol address* dan *hostname* yang telah ditentukan; dan
- j. menerapkan *server* perantara saat *client* mengakses *server database* dalam rangka pemeliharaan.

Bagian Ketujuh  
Standar Keamanan BYOD  
Pasal 36

Standar teknis keamanan BYOD sebagaimana dimaksud dalam Pasal 18 huruf f terdiri atas terpenuhinya:

- a. keamanan pada perangkat komputer
- b. pembatasan akses perangkat komputer

Pasal 37

(1) Terpenuhinya persyaratan keamanan pada perangkat komputer sebagaimana dimaksud dalam Pasal 36 huruf a dilakukan dengan prosedur :

- a. menerapkan *antivirus* yang memiliki lisensi pada perangkat komputer yang digunakan dilingkungan Pemerintah Daerah;
- b. tidak menggunakan perangkat lunak yang tidak memiliki lisensi;
- c. perangkat komputer yang ditujukan sebagai operator *server* tidak boleh terkoneksi ke jaringan *internet* publik. dan
- d. perangkat komputer yang digunakan dilingkungan Pemerintah Daerah harus dilakukan pergantian katasandi secara berkala.

(2) Terpenuhinya pembatasan akses pada perangkat komputer sebagaimana dimaksud dalam Pasal 36 huruf b dilakukan dengan prosedur :

- a. tidak membawa perangkat komputer dan alat rekam dalam bentuk apapun kedalam ruang rapat yang membahas isu strategis; dan
- b. perangkat komputer milik tamu hanya boleh terkoneksi pada jaringan *internet* tamu

BAB V  
KETENTUAN PENUTUP  
Pasal 38

Peraturan Gubernur ini mulai berlaku pada tanggal diundangkan.

Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Gubernur ini dengan penempatannya dalam Berita Daerah Provinsi Kepulauan Riau.

Ditetapkan di Tanjungpinang  
pada tanggal 12 Juli 2022

GUBERNUR KEPULAUAN RIAU,

ttd

ANSAR AHMAD

Diundangkan di Tanjungpinang  
pada tanggal 12 Juli 2022

SEKRETARIS DAERAH  
PROVINSI KEPULAUAN RIAU,

ttd

ADI PRIHANTARA

BERITA DAERAH PROVINSI KEPULAUAN RIAU TAHUN 2022 NOMOR 868

Salinan sesuai dengan aslinya  
KEPALA BIRO HUKUM SEKRETARIAT DAERAH  
PROVINSI KEPULAUAN RIAU,

ttd

KUNTUM PURNOMO, S.H., M.H.  
NIP. 196603281997031004