GUBERNUR MALUKU UTARA

KEPUTUSAN GUBERNUR MALUKU UTARA
NOMOR 516 **/KPTS/MU/ 2024**

TENTANG
PEDOMAN MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK, STANDAR TEKNIS DAN PROSEDUR KEAMANAN SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK
DI LINGKUNGAN PEMERINTAH PROVINSI MALUKU UTARA
GUBERNUR MALUKU UTARA,

Menimbang: a. bahwa pemanfaatan teknologi informasi komunikasi (TIK) dalam proses pemerintahan akan meningkatkan efisiensi, efektifitas, transparansi, akuntabilitas serta perlindungan sistem elektronik milik pemerintah dalam pelaksanaan Sistem Pemerintahan Berbasis Elektronik di lingkungan Pemerintah Provinsi Maluku Utara, diperlukan upaya pengamanan yang memadai dan andal;

b. bahwa pemanfaatan teknologi informasi dan komunikasi (TIK) maupun teknologi terkait dapat menyebabkan kerawanan dan ancaman siber yang meliputi aspek kerahasiaan, keutuhan, ketersediaan, nir-sangkal, otentisitas, akuntabilitas dan keandalan layanan, sehingga dibutuhkan penyediaan pelayanan publik yang cepat, andal, dan aman, yang meliputi tahapan pelaksanaan kegiatan perencanaan, pelaksanaan, monitoring dan evaluasi keamanan informasi;

c. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, dan huruf b, perlu menetapkan dengan Keputusan Gubernur Maluku Utara;

Mengingat : 1. Undang-Undang Nomor 28 Tahun 1999 tentang Penyelenggaraan Negara yang Bersih dan Bebas dari Kolusi, Korupsi dan Nepotisme (Lembaran Negara Tahun 1999 Nomor 75, Tambahan Lembaran Negara Nomor 3851);

2. Undang-Undang Nomor 6 Tahun 2000 tentang Perubahan Atas Undang-Undang Nomor 46 Tahun 1999 tentang Pembentukan Provinsi Maluku Utara, Kabupaten Buru dan Kabupaten Maluku Tenggara Barat (Lembaran Negara Tahun 2000 Nomor 73);

3. Undang-Undang Nomor 17 Tahun 2003 tentang Keuangan Negara (Lembaran Negara Tahun 2003 Nomor 47, Tambahan Lembaran Negara Nomor 4286);

4. Undang-Undang Nomor 1 Tahun 2004 tentang Perbendaharaan Negara (Lembaran Negara Tahun 2004 Nomor 5, Tambahan Lembaran Negara Nomor 4355);
5. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Tahun 2008 Nomor 58, Tambahan Lembaran Negara Nomor 4843);
6. Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah sebagaimana telah beberapa kali diubah, terakhir dengan Undang-Undang Nomor 6 Tahun 2023 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 2 Tahun 2022 tentang Cipta Kerja Menjadi Undang-Undang (Lembaran Negara Tahun 2023 Nomor 41, Tambahan Lembaran Negara Nomor 6841);
7. Undang-Undang Nomor 20 Tahun 2023 tentang Aparatur Sipil Negara (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 141)
8. Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Tahun 2012 Nomor 58, Tambahan Lembaran Negara Nomor 5348);
9. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 6 Tahun 2011 tentang Pedoman Umum Tata Naskah Dinas Elektronik di Lingkungan Instansi Pemerintah;
10. Peraturan Menteri Pendayagunaan Aparatur Negara Nomor 15 Tahun 2017 tentang Pencabutan Peraturan Menteri Pendayagunaan Aparatur Negara Nomor 80 Tahun 2012 tentang Pedoman Tata Naskah Dinas Instansi Pemerintah (Berita Negara Tahun 2017 Nomor 706);
11. Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi (Berita Negara Tahun 2016 Nomor 551);
12. Peraturan Kepala Arsip Nasional Republik Indonesia Nomor 6 Tahun 2005 tentang Pedoman Perlindungan Arsip Vital;
13. Peraturan Kepala Lembaga Sandi Negara Nomor 5 Tahun 2014 tentang Standar Algoritma Kriptografi pada Instansi Pemerintah;
14. Peraturan Kepala Lembaga Sandi Negara Nomor 7 Tahun 2016 tentang Otoritas Sertifikat Digital;
15. Peraturan Kepala Lembaga Sandi Negara Nomor 15 Tahun 2016 tentang Organisasi dan Tata Kerja Balai Sertifikasi Elektronik;
16. Peraturan Kepala Lembaga Sandi Negara Nomor 7 Tahun 2017 tentang Pedoman Penyelenggaraan Persandian Untuk Pengamanan Informasi di Lingkungan Pemerintahan Daerah, Provinsi dan Kabupaten/Kota;
17. Peraturan Kepala Lembaga Sandi Negara Nomor 10 Tahun 2017 tentang Penyelenggaraan Sertifikat Elektronik;

18. Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2021 Nomor 541);
19. Peratuan Daerah Provinsi Maluku Utara Nomor 10 Tahun 2020 tentang Perubahan Atas Peraturan Daerah Provinsi Maluku Utara Nomor 5 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Provinsi Maluku Utara (Lembaran Daerah Provinsi Maluku Utara Tahun 2020 Nomor 10, Tambahan Lembaran Daerah Nomor 10);
20. Peraturan Gubernur Maluku Utara Nomor 27 Tahun 2019 tentang Penyelenggaraan Persandian Untuk Pengamanan Informasi di Lingkungan Pemerintah Daerah Provinsi dan Kabupaten_Kota;
21. Peraturan Gubernur Maluku Utara Nomor 49 Tahun 2021 Tentang Organisasi dan tata Kerja Dinas Komunikasi, Informatika dan Persandian Provinsi Maluku Utara;
22. Peraturan Gubernur Maluku Utara Nomor 18 Tahun 2022 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik;
23. Keputusan Gubernur Maluku Utara Nomor 339/KPTS/MU/2023 tentang Tim Tanggap Insident Siber (*Computer Security Incident Response Team*) /CSIRT Provinsi Maluku Utara;

MEMUTUSKAN :

Menetapkan :

KESATU : Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik, Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik Di Lingkungan Pemerintah Provinsi Maluku Utara sebagaimana tercantum dalam Lampiran Keputusan ini;

KEDUA : Pedoman Manajemen sebagaimana dimaksud pada DIKTUM KESATU Tujuan adalah untuk mewujudkan kelancaran dalam pelaksanaan penyelenggaraan Manajemen keamanan informasi SPBE di Provinsi Maluku Utara;

KETIGA : Ruang lingkup Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik yang meliputi; Penetapan Penanggungjawab, Perencanaan, Dukungan Pengoperasian, Evaluasi Kinerja, dan Perbaikan berkelanjutan;

KEEMPAT : Segala biaya yang timbul sebagai akibat dikeluarkannya Keputusan ini dibebankan pada Anggaran Pendapatan dan Belanja Daerah Provinsi Maluku Utara Pos Dinas Kominfo dan Persandian Provinsi Maluku Utara Tahun Anggaran 2024;

KELIMA : Keputusan ini mulai berlaku pada tanggal ditetapkan.

Ditetapkan di : Sofifi
Pada Tanggal : 9 Agustus 2024
Pj. GUBERNUR MALUKU UTARA

SAMSUDDIN ABDUL KADIR

Tembusan, disampaikan kepada Yth :
1. Menteri Dalam Negeri di Jakarta;
2. Ketua DPRD Provinsi Maluku Utara di Sofifi;
3. Inspektur Provinsi Maluku Utara di Sofifi;
4. Kepala Badan Pengelolaan Keuangan dan Aset Daerah Provinsi Maluku Utara di Sofifi;
5. Kepala BPSDM Provinsi Maluku Utara di Sofifi;
6. Kepala Biro Organisasi Setda Provinsi Maluku Utara di Sofifi;
7. Yang bersangkutan untuk diketahui dan seperlunya.

LAMPIRAN : KEPUTUSAN GUBERNUR MALUKU UTARA
NOMOR : 516 /KPTS/MU/2024
TANGGAL : 9 Agustus 2024
DAFTAR : PEDOMAN MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DAN STANDAR TEKNIS DAN PROSEDUR KEAMANAN SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DI LINGKUNGAN PEMERINTAH PROVINSI MALUKU UTARA

A. Latar Belakang

Keamanan informasi merupakan hal penting dalam penyelenggaraan layanan. Dengan semakin meningkatnya risiko dan insiden keamanan informasi dalam penyelenggaraan sistem elektronik, upaya pengamanan terhadap sistem elektronik yang memiliki data dan informasi strategis dan penting wajib segera dilakukan. Keamanan informasi yang handal, akan meningkatkan kepercayaan masyarakat terhadap penyelenggaraan Sistem Elektronik untuk pelayanan publik.

Sistem Manajemen Keamanan Informasi (SMKI) ini digunakan sebagai pedoman atau standar dalam rangka melindungi aset informasi Pemerintah Provinsi Maluku Utara dari berbagai bentuk ancaman baik dari dalam maupun luar lingkungan Pemerintah Provinsi Maluku Utara, dengan tujuan untuk menjamin kerahasiaan, keutuhan, dan ketersediaan asset informasi.

Standar ini berlaku untuk pengelolaan pengamanan seluruh informasi Pemerintah Provinsi Maluku Utara yang dilaksanakan oleh seluruh unit kerja Pemerintah Provinsi Maluku Utara dan pihak ketiga baik sebagai pengelola dan/atau pengguna Teknologi Informasi dan Komunikasi (TIK).

Sehubungan dengan hal tersebut, dalam rangka keamanan data dan informasi di lingkungan Pemerintah Provinsi Maluku Utara, perlu menyusun sebuah standar tentang manajemen keamanan informasi, yang mengatur bagaimana informasi menjadi aman agar kerahasiaan, integritas, dan ketersediaan informasi tetap terjaga.

B. PEDOMAN MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK (SPBE)

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

2.2 Pedoman manajemen keamanan informasi SPBE sebagaimana dimaksud dalam ketentuan umum merupakan acuan dalam melaksanakan serangkaian proses manajemen keamanan informasi yang meliputi:

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

2.3 Proses sebagaimana dimaksud pada butir 2.2 ditetapkan oleh Gubernur.

2.4 Pemerintah Daerah mengomunikasikan dan mendokumentasikan kegiatan manajemen keamanan informasi SPBE.

3.1 Penetapan ruang lingkup sebagaimana dimaksud dalam butir 2.2 huruf a dilakukan oleh Gubernur.

3.2 Penetapan ruang lingkup sebagaimana dimaksud pada butir 2.2 dilakukan dengan mendefinisikan:

a. Isu internal keamanan informasi SPBE dalam organisasi; dan
b. Isu eksternal keamanan informasi SPBE.

3.3 Isu internal keamanan informasi SPBE dalam organisasi sebagaimana dimaksud pada butir 2.2 huruf a didefinisikan berdasarkan area yang menjadi prioritas organisasi terhadap pelaksanaan keamanan informasi SPBE;

3.4 Area yang menjadi prioritas organisasi terhadap pelaksanaan keamanan informasi SPBE sebagaimana dimaksud pada butir 3.3 paling sedikit meliputi:

a. Data dan informasi SPBE;
b. Aplikasi SPBE;
c. Aset Infrastruktur SPBE; dan
d. Kebijakan keamanan informasi SPBE yang telah dimiliki;
e. Isu eksternal keamanan informasi SPBE sebagaimana dimaksud pada butir 3.2 huruf b didefinisikan sesuai dengan ketentuan peraturan perundang-undangan.

4.1 Penetapan penanggungjawab sebagaimana dimaksud dalam butir 2.2 huruf b dilaksanakan oleh Gubernur;

4.2 Penanggung jawab sebagaimana dimaksud pada butir 4.1 dijabat oleh Sekretaris Daerah Provinsi Maluku Utara;

4.3 Dalam melaksanakan tugas sebagai penanggung jawab Keamanan SPBE, Sekretaris Daerah Provinsi Maluku Utara disebut sebagai koordinator SPBE;

5.1 Dalam melaksanakan tugas sebagai penanggung jawab Keamanan SPBE, koordinator SPBE sebagaimana dimaksud dalam butir 4.3 menetapkan pelaksana teknis Keamanan SPBE;

5.2 Pelaksana teknis Keamanan SPBE sebagaimana dimaksud pada butir 5.1 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.

6.1 Pejabat pimpinan tinggi pratama yang melaksanakan tugas dan fungsi di bidang keamanan teknologi, informasi dan komunikasi sebagaimana dimaksud dalam butir 5.2 huruf a mempunyai tugas :

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.

6.2 Pejabat pimpinan tinggi atau pejabat administrator yang membawahi, membangun, memelihara, dan atau mengembangkan Aplikasi SPBE sebagaimana dimaksud dalam butir 5.2 huruf b mempunyai tugas:

a. Menerapkan standar teknis dan prosedur keamanan aplikasi di unit kerja masing-masing;
b. Memastikan selurnh 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.

7.1 Perencanaan sebagaimana dimaksud dalam butir 2.1 huruf c dilakukan oleh pelaksana teknis Keamanan SPBE.

7.2 Perencanaan sebagaimana dimaksud pada 7.1 dilakukan dengan merumuskan:

a. Program kerja Keamanan SPBE yang disusun berdasarkan kategori risiko Keamanan SPBE; dan
b. Target realisasi program kerja Keamanan SPBE.

7.3 Program kerja Keamanan SPBE sebagaimana dimaksud pada butir 7.2 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.

7.4 Kategori risiko Keamanan SPBE sebagaimana dimaksud pada butir 7.2 huruf a ditentukan sesuai dengan ketentuan peraturan perundang-undangan.

7.5 Target realisasi program kerja Keamanan SPBE sebagaimana dimaksud pada butir 7.2 huruf b ditetapkan berdasarkan kebutuhan Pemerlntah Daerah.

8.1 Edukasi kesadaran Keamanan SPBE sebagaimana dimaksud dalam butir 7.3 huruf a dilaksanakan paling sedikit melalui kegiatan:

a. Sosialisasi; dan
b. Pelatihan.

8.2 Penilaian kerentanan Keamanan SPBE sebagaimana dimaksud dalam butir 7.3 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.

9.1 Peningkatan Keamanan SPBE sebagaimana dimaksud dalam butir 7.3 huruf c dilaksanakan berdasarkan hasil dari penilaian kerentanan Keamanan SPBE sebagaimana dimaksud dalam butir 8.2.

9.2 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.

10.1 Penanganan insiden Keamanan SPBE sebagaimana dimaksud dalam butir 7.3 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.

10.2 Audit Keamanan SPBE sebagaimana dimaksud dalam butir 7.3 huruf e dilakukan sesuai dengan ketentuan peraturan perundang-undangan.

11.1 Dukungan pengoperasian sebagaimana dimaksud dalam butir 2.1 huruf d dilakukan oleh koordinator SPBE.

11.2 Dukungan pengoperasian sebagaimana dimaksud pada butir 11.1 dilakukan dengan meningkatkan kapasitas terhadap:

a. Sumber daya manusia Keamanan SPBE; dan
b. Anggaran Keamanan SPBE.

11.3 Sumber daya manusia Keamanan SPBE sebagaimana dimaksud pada butir 11.2 huruf a paling sedikit harus memiliki kompetensi:

a. Keamanan infrastruktur teknologi, informasi dan komunikasi; dan
b. Keamanan aplikasi.

11.4 Untuk memenuhi kompetensi sebagaimana dimaksud pada butir 11.3, Pemerintah Daerah paling sedikit melakukan kegiatan:

a. Pelatihan dan/ atau sertiftkasi kompetensi keamanan infrastruktur teknologi, informasi dan komunikasi dan keamanan aplikasi; dan
b. Bimbingan teknis mengenai standar Keamanan SPBE.

11.5 Anggaran Keamanan SPBE sebagaimana dimaksud pada butir 11.2 huruf b disusun berdasarkan perencanaan yang telah ditetapkan sesuai dengan ketentuan peraturan perundang-undangan.

12.1 Evaluasi kinerja sebagaimana dimaksud dalam butir 2.1 huruf e dilakukan oleh koordinator SPBE.

12.2 Evaluasi kinerja sebagaimana dimaksud butir 12.1 dilakukan terhadap pelaksanaan Keamanan SPBE.

12.3 Evaluasi kinerja sebagaimana dimaksud pada butir 12.2 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.

12.4 Evaluasi kinerja sebagaimana dimaksud pada butir 12.1 dilaksanakan paling sedikit 1 (satu) kali dalam 1 (satu) tahun.

13.1 Perbaikan berkelanjutan sebagaimana dimaksud dalam butir 2.1 huruf f dilakukan oleh pelaksana teknis Keamanan SPBE.

13.2 Perbaikan berkelanjutan sebagaimana dimaksud pada butir 13.1 merupakan tindak lanjut dari hasil evaluasi kinerja.

13.3 Perbaikan berkelanjutan sebagaimana dimaksud pada butir 13.1 dilakukan dengan:

a. Mengatasi permasalahan dalam pelaksanaan Keamanan SPBE; dan
b. Memperbaiki pelaksanaan Keamanan SPBE secara periodik.

C. STANDAR TEKNIS DAN PROSEDUR KEAMANAN SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK (SPBE)

➢ Bagian Kesatu Umum

15.1 Pemerintah Daerah harus menerapkan Keamanan SPBE.

15.2 Penerapan Keamanan SPBE sebagaimana dimaksud pada butir 14.1 harus memenuhi standar teknis dan prosedur Keamanan SPBE.

15.3 Standar teknis dan prosedur Keamanan SPBE sebagaimana dimaksud dalam butir 15.2 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 Daerah

➢ Bagian Kedua Keamanan Data dan Informasi

16.1 Standar teknis keamanan data dan informasi sebagaimana dimaksud dalam butir 15.3 huruf a terdiri atas terpenuhinya aspek:

a. Kerahasiaan;
b. Keaslian;
c. Keutuhan;
d. Kenirsangkalan; dan
e. Ketersediaan.

16.2 Terpenuhinya aspek kerahasiaan sebagaimana dimaksud dalam butir 16.1 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.

16.3 Terpenuhinya aspek keaslian sebagaimana dimaksud dalam butir 16.1 huruf b dilakukan dengan prosedur :

a. Menyediakan mekanisme verifikasi;
b. Menyediakan mekanisme validasi; dan
c. Menerapkan sistem hash function.

16.4 Terpenuhinya aspek keutuhan sebagaimana dimaksud dalam butir 16.1 huruf c dilakukan dengan prosedur :

a. Menerapkan pendeteksian modifikasi; dan
b. Menerapkan tanda tangan elektronik tersertifikasi.

16.5 Terpenuhinya aspek kenirsangkalan sebagaimana dimaksud dalam butir 16.1 huruf d dilakukan dengan prosedur :

a. Menerapkan tanda tangan elektronik tersertifikasi; dan
b. Penjaminan oleh penyelenggara sertifikasi elektronik melalui sertifikat elektronik.

16.6 Terpenuhinya aspek ketersediaan sebagaimana dimaksud dalam butir 16.1 huruf e dilakukan dengan prosedur :

a. Menerapkan sistem pencadangan secara berkala;
b. Membuat perencanaan untuk menjamin data dan informasi dapat selalu diakses;
c. Menerapkan sistem pemulihan.

➢ **Bagian Ketiga Keamanan Aplikasi SPBE**

17.1 Standar teknis dan prosedur keamanan Aplikasi SPBE sebagaimana dimaksud dalam butir 16.1 huruf b diterapkan pada:

a. Aplikasi berbasis web; dan
b. Aplikasi berbasis mobile.

17.2 Aplikasi berbasis web sebagaimana dimaksud pada butir 17.1 huruf a merupakan aplikasi yang diakses melalui peramban saat terhubung dengan koneksi internet atau intranet.

17.3 Aplikasi berbasis mobile sebagaimana dimaksud pada butir 17.1 huruf b merupakan aplikasi yang dalam pengoperasiannya dapat berjalan diperangkat bergerak, dan memiliki sistem operasi yang mendukung perangkat lunak secara standalone.

17.4 Aplikasi SPBE sebagaimana dimaksud pada butir 17.1 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.

17.5 Standar teknis keamanan aplikasi berbasis web sebagaimana dimaksud dalam butir 17.1 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 error 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.

18.1 Terpenuhinya fungsi autentikasi sebagaimana dimaksud dalam butir 17.5 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.

18.2 Terpenuhinya fungsi manajemen sesi sebagaimana dimaksud dalam butir 17.5 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.

18.3 Terpenuhinya fungsi persyaratan kontrol akses sebagaimana dimaksud dalam butir 17.5 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.

18.4 Terpenuhinya fungsi validasi input sebagaimana dimaksud dalam butir 17.5 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.

5. Terpenuhinya fungsi kriptografi pada verifikasi statis sebagaimana dimaksud dalam Poin 26 huruf e dilakukan dengan prosedur :

a. Menggunakan algoritma kriptografi, modul kriptografi, protocol 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.

18.5 Terpenuhinya fungsi penanganan error dan pencatatan log sebagaimana dimaksud dalam butir 17.5 huruf f dilakukan dengan prosedur :

a. Mengatur konten pesan yang ditampilkan ketika teljadi kesalahan;
b. Menggunakan metode penanganan error 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 sum ber waktu sesuai dengan zona waktu dan waktu yang benar.

18.6 Terpenuhinya fungsi proteksi data sebagaimana dimaksud dalam butir 17.5 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.

18.7 Terpenuhinya fungsi keamanan komunikasi sebagaimana dimaksud dalam butir 17.5 huruf h dilakukan dengan prosedur :
a. Menggunakan komunikasi terenkripsi;
b. Mengatur koneksi masuk dan keluar yang aman dan terenkripsi dati 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.

18.8 Terpenuhinya fungsi pengendalian kode berbahaya sebagaimana dimaksud dalam butir 17.5 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.

18.9 Terpenuhinya fungsi logika bisnis sebagaimana dimaksud dalam butir 17.5 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 antiotomatisasi; dan
e. Memberikan peringatan ketika terjadi serangan otomatis atau aktivitas yang tidak biasa.

18.10 Terpenuhinya fungsi file sebagaimana dimaksud dalam butir 17.5 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 dati sumber yang tidak dipercaya; dan
e. Melakukan konfigurasi server untuk mengunduh file sesuai ekstensi yang ditentukan.

18.11 Terpenuhinya fungsi keamanan API dan web service sebagaimana dimaksud dalam butir 17.5 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 antiotomatisasi.

18.12 Terpenuhinya fungsi keamanan konfigurasi sebagaimana dimaksud dalam butir 17.5 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, 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.

19.1 Standar teknis keamanan aplikasi berbasis mobile sebagaimana dimaksud dalam butir 15.3 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
g. Ketahanan.

20.1 Terpenuhinya fungsi penyimpanan data dan persyaratan privasi sebagaimana dimaksud dalam butir 19.1 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 mela1ui antarmuka pengguna.

20.2 Terpenuhinya fungsi kriptografi sebagaimana dimaksud dalam butir 19.1 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.

20.3 Terpenuhinya fungsi autentikasi dan manajemen sesi sebagaimana dimaksud dalam butir 19.1 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 logout;
e. Menerapkan pengaturan sandi pada remote endpoint;
f. Membatasi jumlah percobaan login pada remote endpoint;
g. Menentukan masa berlaku sesi dan masa kedaluwarsa token pada remote endpoint; dan
h. Melakukan otorisasi pada remote endpoint.

20.4 Terpenuhinya fungsi komunikasi jaringan sebagaimana dimaksud dalam butir 19.1 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.

20.5 Terpenuhinya fungsi interaksi platform sebagaimana dimaksud dalam butir 19.1 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 fasllitas inter process communication;
d. Menghindari penggunaan JavaScript dalam Web VieW;
e. Menggunakan protokol hypertext transfer protocol secure pada Web View; dan
f. Mengimplementasikan penggunaan serialisasi API yang aman.

20.6 Terpenuhinya fungsi kualitas kode dan pengaturan build sebagaimana dimaksud dalam butir 19.1 huruf f dilakukan dengan prosedur:
a. Menandatangani aplikasi dengan sertifikat yang valid;
b. Memastikan aplikasi dalam mode rills;
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 error,
g. Mengelola memori secara aman; dan
h. Mengaktifkan fitur keamanan yang tersedia.

20.7 Terpenuhinya fungsi ketahanan sebagaimana dimaksud dalam butir 19.1 huruf g dilakukan dengan prosedur:

a. Mencegah aplikasi berjal an pada perangkat yang telah dilakukan modifikasi yang tidak sah;
b. Mendeteksi dan merespon debugger,
c. Mencegah executable file melakukan perubahan pada sumber daya perangkat;
d. Mendeteksi dan merespons keberadaan perangkat reverse engineering;
e. Mencegah aplikasi beljalan 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**

21.1 Standar teknis keamanan Sistem Penghubung Layanan sebagaimana dimaksud dalam butir 15.3 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.

22.1 Terpenuhinya fungsi keamanan interoperabilitas data dan informasi sebagaimana dimaksud dalam butir 21.1 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 hash function pada file.

22.2 Terpenuhinya fungsi kontrol sistem integrasi sebagaimana dimaksud dalam butir 22.1 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 error dan pencatatan log;
k. Menerapkan proteksi data dan jalur komunikasi;
1. 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.

22.3 Terpenuhinya fungsi kontrol perangkat integrator sebagaimana dimaksud dalam butir 22.1 huruf c dilakukan dengan prosedur:
a. Menggunakan sistem operasi dan perangkat lunak dengan security patches terkini;
b. Menggunakan anti virus dan anti-spyware terkini;
c. Mengaktifkan fitur keamanan pada peram ban 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.

22.4 Terpenuhinya fungsi keamanan API dan web service sebagaimana dimaksud dalam butir 22.1 huruf d dilakukan dengan prosedur :
a. Menerapkan protokol secure socket layer atau protokol transport layer security diantara 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.

22.5 Terpenuhinya fungsi keamanan migrasi data sebagaimana dimaksud dalam butir 22.1 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 sam pai sistem pendukung basis data bam dapat beljalan atau berfungsi dengan normal;
c. Mendokumentasikan format sistem basis data lama secara rinci;
d. Melakukan pencadangan seluruh data yang tersimpan pada system sebelum melakukan migrasi data;
e. Menerapkan teknik kriptografi pad a proses penyimpanan dan pengambilan data; dan
f. Melakukan validasi data ketika proses migrasi data selesai.

➢ **Bagian Kelima Keamanan Jaringan Intra**

23.1 Standar teknis keamanan Jaringan Intra sebagaimana dimaksud dalam butir 15.3 huruf d diterapkan pada :

a. Jaringan Intra pemerintah; dan
b. Jaringan Intra Instansi Pusat dan Pemerintah Daerah.

23.2 Standar teknis keamanan Jaringan Intra sebagaimana dimaksud pada butir 23.1 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 padajaringan nirkabel; dan
f. Kontrol konfigurasi access point pada jaringan nirkabel.

24.1 Terpenuhinya aspek administrasi keamanan Jaringan Intra sebagaimana dimaksud dalam butir 23.2 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.

24.2 Terpenuhinya kontrol akses dan autentikasi sebagaimana dimaksud dalam butir 23.2 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 padajalur komunikasi yang digunakan;
h. Memberikan kewenangan hanya kepada administrator untuk menginstal perangkat lunak dan Iatau 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.

24.3 Terpenuhinya persyaratan perangkat dan aplikasi keamanan Jaringan Intra sebagaimana dimaksud dalam butir 23.2 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 lunakuntuk meminimalisasi celah peretas;
j. Mengunduh perangkat lunak melalui enterprise software distribution system; dan
k. Menerapkan sertifikat elektronik.

24.4 Terpenuhinya kontrol keamanan gateway sebagaimana dimaksud dalam 23.2 huruf d dilakukan dengan prosedur:

a. Menerapkan content filtering;
b. Menerapkan inspection packet filtering untuk memeriksa packet yang masuk pad a 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.

24.5 Terpenuhinya kontrol keamanan access point pada jaringan nirkabel sebagaimana dimaksud dalam butir 23.2 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.

24.6 Terpenuhinya kontrol konfigurasi access point pada jaringan nirkabel sebagaimana dimaksud dalam butir 23.2 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. Menonaktitkan antarmuka nirkabel, layanan, dan aplikasi yang tidak digunakan.

➢ **Bagian Keenam Keamanan Pusat Data Daerah**

25.1 Standar teknis keamanan Pusat Data Daerah sebagaimana dimaksud dalam butir 15.3 huruf e terdiri atas terpenuhinya:

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

25.2 Terpenuhinya persyaratan keamanan fisik dan manajemen Pusat Data Daerah sebagaimana dimaksud dalam butir 25.1 huruf a dilakukan dengan prosedur sesuai dengan Standar Nasional Indonesia yang terkait dengan Pusat Data.

25.3 Terpenuhinya persyaratan koneksi perangkat ke Pusat Data Daerah sebagaimana dimaksud dalam butir 25.1 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.

D. PENUTUP

Pj. GUBERNUR MALUKU UTARA

GUBERNUR MALUKU UTARA

SAMSUDDIN ABDUL KADIR