BUPATI MAMUJU
PROVINSI SULAWESI BARAT

KEPUTUSAN BUPATI MAMUJU
NOMOR 455 TAHUN 2024

TENTANG
MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DI LINGKUNGAN PEMERINTAH KABUPATEN MAMUJU

BUPATI MAMUJU,

Menimbang : a. bahwa berdasarkan ketentuan Pasal 3 Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Estándar Teknis Dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik, menyebutkan bahwa proses manajemen keamanan informasi ditetapkan oleh setiap pimpinan pusat dan kepala daerah;

b. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, perlu menetapkan manajemen keamanan informasi sistem pemerintahan berbasis elektronik di lingkungan Pemerintah Kabupaten Mamuju;

c. bahwa berdasarkan pertimbangan sebgaimana dimaksud dalam huruf a dan huruf b, perlu menetapkan Keputusan Bupati tentang Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik Di Lingkungan Pemerintah Kabupaten Mamuju;

Mengingat : 1. Undang-Undang Nomor 29 Tahun 1959 tentang Pembentukan Daerah Tingkat II di Sulawesi (Lembaran Negara Republik Indonesia Tahun 1959 Nomor 74. Tambahan Lembaran Negara Republik Indonesia Nomor 1822);

2. Undang-Undang Nomor 26 Tahun 2004 tentang Pembentukan Provinsi Sulawesi Barat (Lembaran Negara Republik Indonesia Tahun 2004 Nomor 105, Tambahan Lembaran Negara Republik Indonesia Nomor 4422);

3. Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Tahun 2008 Nomor

58, Tambahan Lembaran Negara Nomor 4843), sebagaimana telah beberapa kali diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1, Tambahan Lembaran Negara Republik Indonesia Nomor 6905);

4. Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 61, 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 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 244, Tambahan Lembaran Negara Republik Indonesia Nomor 5587) sebagaimana telah diubah beberapa kali, 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 Indonesia Tahun 2023 Nomor 41, Tambahan Lembaran Negara Indonesia Nomor 6856);
7. 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);
8. 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);
9. 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);
10. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);

11. Peraturan Presiden Nomor 39 Tahun 2019 tentang Satu Data Indonesia (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 112);
12. Peraturan Kepala 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);
13. Peraturan Daerah Kabupaten Mamuju Nomor 11 Tahun 2023 tentang Anggaran Pendapatan dan Belanja Daerah Tahun Anggaran 2024 (Lembaran Daerah Kabupaten Mamuju Tahun 2023 Nomor 11);
14. Peraturan Bupati Mamuju Nomor 31 Tahun 2023 tentang Penjabaran Anggaran Pendapatan dan Belanja Daerah Tahun Anggaran 2024 sebagaimana telah diubah beberapa kali, terakhir dengan Peraturan Bupati Mamuju Nomor 13 Tahun 2024 tentang Perubahan Ketiga Atas Peraturan Bupati Mamuju Nomor 31 Tahun 2023 Tentang Penjabaran Anggaran Pendapatan dan Belanja Daerah Tahun Anggaran 2024 (Berita Daerah Kabupaten Mamuju Tahun 2024 Nomor 13);

Memperhatikan : Pedoman Menteri Pendayagunaan Aparatur Sipil Negara dan Reformasi Birokrasi Nomor 3 Tahun 2024 tentang Tata Cara Pemantauan dan Evaluasi Sistem Pemerintahan Berbasis Elektronik

MEMUTUSKAN:

Menetapkan : KEPUTUSAN BUPATI TENTANG MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DI LINGKUNGAN PEMERINTAH KABUPATEN MAMUJU

KESATU : Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik di lingkungan Pemerintah Kabupaten Mamuju, sebagaimana tercantum dalam lampiran yang merupakan bagian tidak terpisahkan dengan Keputusan Bupati ini;

KEDUA : Manajemen Keamanan Informasi sebagaimana dimaksud dalam Diktum KESATU, berfungsi sebagai berikut:

1. Sebagai serangkaian proses untuk mencapai penerapan keamanan Sistem Pemerintahan Berbasis Elektronik

yang efektif, efisien dan berkesinambungan, serta mendukung layanan SPBE yang berkualitas; dan

2. Menjadi acuan dalam melaksanakan serangkaian proses manajemen keamanan informasi.

KETIGA : Segala Biaya yang timbul akibat ditetapkannya Keputusan ini dibebankan pada APBD Kabupaten Mamuju Tahun Anggaran 2024;

KEEMPAT : Keputusan ini mulai berlaku sejak tanggal ditetapkan.

Ditetapkan di Mamuju
pada tanggal 2 Agustus 2024
BUPATI MAMUJU,

SITTI SUTINAH SUHARDI

Tembusan : Kepada Yth.
1. Ketua DPRD Kabupaten Mamuju di Mamuju.
2. Kepala Dinas Komunikasi, Informatika dan Persandian Kab.Mamuju di Mamuju.
3. Inspektur Daerah Kab. Mamuju di Mamuju.
4. Kepala Badan Pengelola Keuangan dan Aset Daerah Kab. Mamuju di Mamuju
5. Kepala Dinas Perpustakaan dan Kearsipan Kab. Mamuju di Mamuju
6. Kepala Bagian Hukum Setdakab Mamuju di Mamuju.

LAMPIRAN : KEPUTUSAN BUPATI MAMUJU
NOMOR : 455 Tahun 2024
TANGGAL : 2 Agustus 2024

MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK DI LINGKUNGAN PEMERINTAH KABUPATEN MAMUJU

I. Umum

Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada pengguna SPBE. Keamanan SPBE merupakan aspek penting dalam pengendalian keamanan yang terpadu dalam SPBE. Olehnya itu diperlukan Manajemen Keamanan SPBE sebagai serangkaian proses untuk mencapai penerapan keamanan SPBE yang efektif, efisien dan berkesinambungan, serta mendukung layanan SPBE yang berkualitas.

II. Proses Manajemen Keamanan Informasi

1. Manajemen keamanan informasi SPBE dilaksanakan berdasarkan Pedoman Manajemen Keamanan SPBE yaitu serangkaian proses manajemen keamanan informasi SPBE yang meliputi:
   a. Penetapan ruang lingkup;
   b. Penetapan penanggungjawab;
   c. Perencanaan;
   d. Dukungan pengoperasian
   e. Evaluasi kinerja; dan
   f. Perbaikan berkelanjutan
2. Mencermati isu internal dan eksternal keamanan informasi SPBE, ruang lingkup pengamanan informasi, meliputi :
   a. Data dan Informasi, yaitu :
      1) Data dan Informasi Keuangan Pemerintah Daerah;
      2) Data dan Informasi Aset;
      3) Data dan Informasi Kepegawaian Pemerintah Daerah;
      4) Data dan Informasi Kependudukan;
      5) Data dan Informasi Pengadaan Barang dan Jasa;
      6) Data dan Informasi Perencanaan Pembangunan;
      7) Data dan Informasi Investasi dan Perizinan;
      8) Data dan Informasi Kebencanaan;
      9) Data dan Informasi Sektoral Pemerintah Daerah yang bersifat strategis yang dikelola oleh Perangkat Daerah.
   b. Aplikasi SPBE, yaitu :
      1) Aplikasi SPBE yang tercakup dalam Aplikasi Pemerintahan;
      2) Aplikasi SPBE yang tercakup dalam Aplikasi Pelayanan Publik;
      3) Aplikasi SPBE yang tercakup dalam aplikasi khusus dan aplikasi misi tertentu.
   c. Aset Infrastruktur, yaitu :
      1) Pusat Data atau Server;
      2) Jaringan Intra Pemerintah Daerah;

3) Jaringan Intra Perangkat Daerah;
4) Peralatan Teknologi Informasi Komunikasi, seperti Komputer PC; Laptop dan Peralatan lainnya;

d. Kebijakan Keamanan Informasi.

3. Penanggungjawab dan Pelaksana Teknis Keamanan Informasi di lingkungan Pemerintah Kabupaten Mamuju, sebagai berikut :
   a. Penanggung Jawab : Sekretaris Daerah Kabupaten Mamuju selaku Koordinator SPBE
   b. Pelaksana Teknis :
      1) Ketua : Kepala Dinas Komunikasi, Informatika dan Persandian;
      2) Anggota : a) Kepala Bidang Persandian Dinas Komunikasi, Informatika dan Persandian;
         b) Para Kepala Bagian dan Kepala Bidang pada setiap Perangkat Daerah yang mengelola Aplikasi SPBE
   c. Tugas Ketua Pelaksana Teknis Keamanan Informasi, sebagai berkut :
      1) Memastikan penerapan standar teknis dan prosedur Keamanan SPBE;
      2) Merumuskan, mengoordinasikan dan melaksanakan program kerja dan anggaran Keamanan SPBE; dan
      3) Melaporkan pelaksanaan manajemen keamanan informasi SPBE dan penerapan standar teknis dan prosedur keamanan SPBE kepada Sekretaris Daerah selaku Koordinator SPBE Pemerintah Daerah
   d. Tugas Anggota Pelaksana Keamanan Informasi, sebagai berikut :
      1) Menerapkan standar teknis dan prosedur keamanan aplikasi di unit kerja masing-masing;
      2) Memastikan seluruh pembangunan dan pengembangan Aplikasi dan Infrastruktur SPBE memenuhi standar teknis dan prosedur Keamanan SPBE yang telah ditetapkan;
      3) Memastikan keberlangsungan proses bisnis SPBE; dan
      4) Berkoordinasi dengan Kepala Dinas Komunikasi, Informatika dan Persandian terkait perumusan program kerja dan anggaran Keamanan SPBE
4. Perencanaan Keamanan Informasi dilaksanakan oleh Kepala Dinas Komunikasi, Informatika dan Persandian bersama Satuan Kerja yang membidangi fungsi penunjang Perencanaan berupa Program Keamanan SPBE yang disusun berdasarkan kategori resiko keamanan SPBE serta target dan realisasi program kerja keamanan SPBE. Program kerja keamanan SPBE, meliputi:
   a. Edukasi kesadaran keamanan SPBE, meliputi: sosialisasi dan pelatihan keamanan SPBE;
   b. Penilaian kerentanan Keamanan SPBE, meliputi: menginvetarisasi seluruh aset SPBE yaitu data dan informasi, aplikasi dan infrasruktur, mengidentifikasi kerentanan dan ancaman terhadap aset SPBE, dan mengukur tingkat risiko Keamanan SPBE;

c. Peningkatan Keamanan SPBE, meliputi: penerapan standar teknis dan prosedur Keamanan SPBE serta menguji fungsi keamanan terhadap Aplikasi SPBE dan Infrastruktur SPBE;
d. Penanganan insiden Keamanan SPBE, meliputi: mengidentifikasi sumber serangan, menganalisis informasi yang berkaitan dengan insiden selanjutnya, memprioritaskan penanganan insiden berdasarkan tingkat dampak yang terjadi, mendokumentasi bukti insiden yang terjadi, dan memitigasi atau mengurangi dampak risiko Keamanan SPBE;
e. Audit Keamanan SPBE sesuai dengan ketentuan Peraturan Perundang-Undangan.

5. Sekretaris Daerah selaku Koordinator SPBE memberikan Dukungan pengoprasian dengan meningkatkan kapasitas terhadap:
   a. Sumber daya manusia Keamanan SPBE, meliputi: kompetensi keamanan infrastruktur teknologi, informasi dan komunikasi dan kompetensi keamanan aplikasi, melalui pelatihan dan/ atau sertifikasi kompetensi keamanan infrastruktur teknologi, informasi dan komunikasi dan keamanan aplikasi serta bimbingan teknis mengenai standar Keamanan SPBE.
   b. Anggaran Keamanan SPBE berdasarkan perencanaan yang telah ditetapkan sesuai dengan ketentuan Peraturan Perundang-Undangan.
6. Sekretaris Daerah selaku Koordinator SPBE melakukan evaluasi kinerja SPBE, yaitu:
   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.
7. Perbaikan berkelanjutan dilakukan oleh pelaksana teknis Keamanan SPBE sebagai bentuk tindak lanjut dari hasil evaluasi kinerja. Perbaikan berkelanjutan dilakukan dengan mengatasi permasalahan dalam pelaksanaan Keamanan SPBE dan memperbaiki pelaksanaan Keamanan SPBE secara periodik

III. Standar Teknis Dan Prosedur Keamanan

1. Penerapan Standar Teknis dan Prosedur Keamanan SPBE, meliputi:
   a. Keamanan data dan informasi;
   b. Keamanan Aplikasi SPBE;
   c. Keamanan Sistem Penghubung Layanan;
   d. Keamanan Jaringan Intra; dan
   e. Keamanan Pusat Data.
2. Standar teknis keamanan data dan informasi terdiri atas terpenuhinya aspek:
   a. Kerahasiaan, dilakukan dengan prosedur:
      1) Menetapkan klasifikasi informasi;
      2) Menerapkan enskripsi dengan sistem kriptografi; dan
      3) Menerapkan pembatasan akses terhadap data dan informasi sesuai dengan kewenangan dan kebijakan yang telah ditetapkan.

b. Keaslian, dilakukan dengan prosedur:
   1) Menyediakan mekanisme verifikasi;
   2) Menyediakan mekanisme validasi; dan
   3) Menerapkan sistem *hash function*
c. Keutuhan, dilakukan dengan prosedur:
   1) Menerapkan pendeteksian modifikasi; dan
   2) Menerapkan tanda tangan elektronik tersertifikasi.
d. Kenirsangkalan, dilakukan dengan prosedur:
   1) Menerapkan tanda tangan elektronik tersertifikasi; dan
   2) Penjaminan oleh penyelenggara sertifikasi elektronik melalui sertifikat elektronik.
e. 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

3. Standar teknis dan prosedur keamanan Aplikasi SPBE diterapkan pada:
   a. aplikasi berbasis web yaitu aplikasi yang diakses melalui peramban saat terhubung dengan koneksi internet atau intranet. Standar teknis keamanan aplikasi berbasis web terdiri atas terpenuhinya fungsi:
      1) 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, 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, 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, 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, dilakukan dengan prosedur:
a) menggunakan algoritma kriptografi, modul kriptografi, protokol kriptografi, dan kunci kriptografi sesuai dengan ketentuan peraturan perundangundangan;
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, 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, 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, dilakukan dengan prosedur:
a) menggunakan komunikasi terenskripsi;
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, dilakukan dengan prosedur:
a) Menggunakan analisis kode dalam konntrol 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;
e) Mengatur mekanisme fitur pembaruan

10) 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 control antiotomatisasi; dan
e) Memberikan peringatan ketika terjadi serangan otomatis atau aktivitas yang tidak biasa.

11) 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 perlindungan terhadap metadata input dan metadata file;
d) Melakukan pemindaian file yang diperoleh dari sumber yang tidak dipercaya;
e) Melakukan konfigurasi server untuk mengunduh file sesuai ekstensi yang ditentukan.

12) 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* protokol apabila input pengguna dinyatakan valid;
e) Menggunakan validasi skema dan verifikasi sebelum menerima input;
f) Menggunakan metode perlindungan layanan berbasis web; dan
g) Menerapkan control antiotomatis.

13) Keamanan Konfigurasi, dilakukan dengan prosedur;
a) Mengonfigurasi server sesuai rekomendasi server aplikasi dan kerangka aplikasi yang digunakan;
b) Mendokumentasi, menyalin konfigurasi dan semua dependensi;
c) Menghapus fitur, dokumentasi, sampel dan konfigurasi yang tidak diperlukan;
d) Memvalidasi integritas aset jika aset aplikasi diakses secara eksternal; dan
e) Menggunakan respon aplikasi dan konten yang aman.

b. Aplikasi berbasis mobile yaitu aplikasi yang dalam pengoperasiannya dapat berjalan diperangkat bergerak, dan memiliki ssitem operasi yang mendukung perangkat lunak secara *standalone.* Standar teknis keamanan aplikasi berbasis mobile terdiri atas terpenuhinya fungsi:

1) 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, dilakukan dengan prosedur;
a) Menghindari penggunaan kriptografi simetrik dengan *hardoded key*;
b) Mengimplementasikan metode kriptografi yang sudah teruji sesuai kebutuhan;
c) Menghindari penggunaan protokol kriptografi atau algoritme kriptografi yang obsolete;
d) Menghindari penggunaan kunci kriptografi yang sama; dan
e) Menggunakan pembangkit kunci acak yang memenuhi kriteria keacakan kunci.

3) 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 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 kedaluarsa token pada *remote endpoint;* dan
h) Melakukan otorisasi pada *remote endpoint.*

4) 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, 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, 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, dilakukan dengan prosedur:
a) Mencegah aplikasi berjalan pada perangkat yang telah dilakukan modifikasi yang tidak sah;
b) Mendeteksi dan merespon *debugging*;
c) Mencegah *executable* file melakukan perubahan pada sumber daya perangkat;
d) Mendeteksi dan merespon 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.*

4. Standar teknis keamanan Sistem Penghubung Layanan terdiri atas terpenuhi fungsi:
   a. Keamanan interoperabilitas data dan informasi, dilakukan dengan prosedur:
      1) Menerapkan sistem tanda tangan elektronik tersertifikasi untuk pengamanan dokumen dan surat elektronik;
      2) Menerapkan sistem enkripsi data;
      3) Memastikan data dan informasi selalu dapat diakses sesuai otoritasnya; dan
      4) Menerapkan sistem *hash function* pada *file.*
   b. Kontrol sistem integrasi, dilakukan dengan prosedur:
      1) Menerapkan *protokol secure socket layer* atau *protokol transport layer security* versi terkini pada sesi pengiriman data dan informasi;
      2) Menerapkan *internet protocol security* untuk mengamankan transmisi data dalam jaringan berbasis *transmission control protocol/internet protocol*;
      3) Menerapkan sistem *anti distributed denial of service*; menerapkan autentikasi untuk memverifikasi identitas eksternal antar layanan SPBE yang terhubung;
      4) Menerapkan manajemen keamanan sesi;
      5) Menerapkan pembatasan akses pengguna berdasarkan otorisasi yang telah ditetapkan;
      6) Menerapkan validasi input;
      7) Menerapkan kriptografi pada verifikasi statis;
      8) Menerapkan sertifikat elektronik pada *web authentication*;
      9) Menerapkan penangangan eror dan pencatatan log;
      10) Menerapkan proteksi data dan jalur komunikasi; menerapkan pendeteksi virus untuk memeriksa beberapa konten file;
      11) Menetapkan perjanjian tingkat layanan dengan standar paling rendah 95%; dan
      12) Memastikan sistem integrasi tidak memiliki kerentanan yang berpotensi menjadi celah peretas.
   c. Kontrol perangkat integrator, dilakukan dengan prosedur;
      1) Menggunakan sistem operasi dan perangkat lunak dengan *security patches* terkini;
      2) Menggunakan anti virus dan anti-*spyware* terkini;
      3) Mengaktifkan fitur keamanan pada peramban web;
      4) Menerapkan *firewall* dan *host-based intrusion detection systems*;
      5) Mencegah instalasi perangkat lunak yang belum terverifikas;
      6) Mencegah akses terhadap situs yang tidak sah; dan
      7) Mengaktifkan sistem *recovery* dan *restore* pada perangkat *integrator.*

d. Keamanan API dan web service, dilakukan dengan prosedur:
   1) Menerapkan protokol *secure socket layer* atau protokol *transport layer security* diantara pengirim dan penerima API;
   2) Menerapkan protokol *open authorization* versi terkini untuk menjembatani interaksi antara *resource owner, resource server* dan/ atau *third party*;
   3) Menampilkan metode *RESTful hypertext transfer protocol* apabila input pengguna dinyatakan valid;
   4) Melindungi layanan *web RESTful* yang menggunakan cookie dari cross-site request forgery; dan
   5) Memvalidasi parameter yang masuk oleh penerima API untuk memastikan data yang diterima valid dan tidak menyebabkan kerusakan.
e. Keamanan migrasi data, dilakukan dengan prosedur:
   1) Memastikan migrasi data dilakukan secara bertahap dan terprogram oleh sistem;
   2) Memastikan aplikasi yang menggunakan sistem basis data lama tetap dipertahankan sampai sistem pendukung basis data baru dapat berjalan atau berfungsi dengan normal;
   3) Mendokumentasikan format sistem basis data lama secara rinci;
   4) Melakukan pencadangan seluruh data yang tersimpan pada sistem sebelum melakukan migrasi data;
   5) Menerapkan teknik kriptografi pada proses penyimpanan dan pengambilan data; dan
   6) Melakukan validasi data ketika proses migrasi data selesai.
f. Standar teknis keamanan Jaringan Intra Pemerintah Daerah terdiri atas terpenuhinya:
   1) 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, 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 berdasrkan jenis serangan;

g. Menerapkan *virtual private network* dan mengaktifkan fungsi enskripsi 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;
l. Menerapkan server perantara saat client mengakses server database dalam rangka pemeliharaan.

3) Persyaratan perangkat dan aplikasi keamanan jaringan intra, Dilakukan dengan prosedur;
   a) Menggunakan perangkat *security information and event Management* untuk network longing dan monitoring;
   b) Menerapkan sistem deteksi dini kerentanan keamanan perangkat jaringan;
   c) Menggunakan perangkat firewall;
   d) Menggunakan perangkat *intrusion delection systems dan intrusion prevention systems;*
   e) Menerapkan *virtual private network* terenkripsi untuk menggunakan akses jarak jauh secara terbatas;
   f) Menerapkan kontrol *update patching* pada intrastuktur jaringan intra dan sistem computer;
   g) Menggunakan perangkat *web aplicasion firewall;*
   h) menggunakan perangkat *load balancer* untuk menjaga ketersediaan akses terhadap jaringan dan aplikasi;
   i) memperbarui teknologi keamanan perangkat keras dan perangkat lunak untk meminimalisasi celah peretas;
   j) mengunduh perangkat lunak *melalui enterprise software distribution system*; dan
   k) menerapkan sertifikat elektronik
   4) 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 kemanan pada fitur akses jarak jauh perangkat *gateway*;
      d) memastikan perangkat gateway yang menghubungkan antar jaringan intra tidak terkoneksi langsun dengan jarinagn publik;
      e) melaksanakan manajemen *traffic gateway*; dan
      f) memastikan port tidak dibuka secara default.

5) Kontrol keamanan *access point* pada jaringan nirkabel, 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 indentifier;*
   d) Menerapkan pembatasan jangkauan radio transmisi dan pengguna jaringan;
   e) Menerapkan pembatasan terkait penambahan perangkat nirkabel yang dipasang secara tidak sah;
   f) Menerapkan manajemen *uulnerabittily* secara berkala dan berkelanjutan; dan
   g) Melakukan *patching firmware* secara rutin
6) 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 intrastruktuk jaringan untuk *management user* atau otentikasi administrator *access poin't*;
   c) Memastikan fitur akses konfigurasi jarak jauh hanya dapat digunakan dalam kondisi darurat dengan menerapkan kontrol keamanan;
   d) Mengisolasi atau melakukan segmentasi jaringan area local nirkabel; dan
   e) Menonaktifkan antarmuka nirkabel, layanan dan aplikasi yang tidak digunakan

g. Standar teknis kemanan pusat Data, terdiri atas terpenuhinya;
   1) Persyaratan kemanan fisik dan manajemen pusat Data, dilakukan dengan prosedur sesuai dengan Standar Nasional Indonesia yang terkait dengan Pusat Data.
   2) Persyaratan koneksi perangkat ke Pusat Data,dilakukan dengan prosedur;
      a) Memastikan keamanan perangkat yang terkoneksi ke intrastruktur Pusat Data;
      b) Memutus akses fisik atau *logic* dari perangkat yang tidak terotorosasi;
      c) Memastikan akses tingkat administrator ke *server* dan perangkat jaringan utama tidak boleh dilakukan secara remoter;
      d) Memastikan hanya personil yang berwenang yang boleh mengunakan computer di area Pusat Data;
      e) Melakukan *backup* informasi dan perangkat lunak yang berada di Pusat Data secara berkala;

f) Memastikan perangkat computer Pusat Data terbebas dari virus dan *malware*;
g) Melakukan pembatasan akses pemanfaatan remofable media di area Pusat Data;
h) Memastikan pengaktifan konfigurasi port universal serial bus telah mendapatkan izin dari personil yang berwenang;
i) Memastikan setiap perangkat yang akan terkoneksi ke intrastruktur Pusat Data mengguakan *internet protokol* address dan *hostname* yang telah dilakukan; dan
j) Menerapkan *server* perantara saat client mengakses *server database* dalam rangka pemeliharaan

BUPATI MAMUJU,

SITTI SUTINAH SUHARDI