SALINAN

BUPATI POLEWALI MANDAR
PROVINSI SULAWESI BARAT

KEPUTUSAN BUPATI POLEWALI MANDAR
NOMOR 722 TAHUN 2021

TENTANG

AUDIT INTERNAL TEKNOLOGI INFORMASI DAN KOMUNIKASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

BUPATI POLEWALI MANDAR

Menimbang : bahwa dalam rangka menjamin kesesuaian dan kualitas penyelenggaraan Sistem Pemerintahan Berbasis Elektronik di lingkungan Pemerintah Kabupaten Kabupaten Polewali Mandar, perlu dilaksanakan Audit Teknologi Informasi dan Komunikasi secara internal, yang ditetapkan dengan Keputusan Bupati;

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);
4. Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (Lembaran Negara Tahun 2008 Nomor 61 Tambahan Lembaran Negara 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 beberapakali terakhir dengan Undang-Undang Nomor 11 Tahun 2020 tentang Cipta Kerja (Lembaran Negara Republik Indonesia Tahun 2020 Nomor 245, Tambahan Lembaran Negara Republik Indonesia Nomor 6573);
7. Peraturan Pemerintah Nomor 74 Tahun 2005 tentang Perubahan Nama Kabupaten Polewali Mamasa Menjadi Kabupaten Polewali Mandar (Lembaran Negara Republik Indonesia Tahun 2005 Nomor 160);

8. Peraturan Pemerintah Nomor 11 Tahun 2010 tentang Pelaksanaan Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik;
9. Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Tahun 2012 Nomor 189 Tambahan Lembaran Negara Nomor 5348);
10. Peraturan Pemerintah Nomor 96 Tahun 2012 tentang Pelaksanaan Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik (Lembaran Negara Tahun 2012 Nomor 215 Tambahan Lembaran Negara Nomor 5357)
11. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Rebuplik Indonesia Tahun 2018 Nomor 182);
12. Peraturan Presiden Nomor 39 Tahun 2019 Tentang Satu Data Indonesia (Lembaran Negara Rebuplik Indonesia Tahun 2019 Nomor 112);
13. Peraturan Daerah Nomor 12 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Kabupaten Polewali Mandar (Lembaran Daerah Kabupaten Polewali Mandar Tahun 2016 Nomor 12);

Memperhatikan : Peraturan Bupati Nomor 22 Tahun 2021 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik (Berita Daerah Kabupaten Polewali Mandar Nomor 22 Tahun 2021);

MEMUTUSKAN:

Menetapkan :

KESATU : Audit Internal Teknologi Informasi dan Komunikasi Sistem Pemerintahan Berbasis Elektronik di lingkungan Pemerintah Kabupaten Polewali Mandar, sebagaimana tercantum dalam lampiran Keputusan ini.

KEDUA : Audit Internal Teknologi Informasi dan Komunikasi sebagaimana dimaksud pada diktum kesatu, berfungsi sebagai berikut :

a. sebagai serangkaian proses yang sistematis untuk memperoleh dan mengevaluasi bukti secara objektif terhadap Infrastruktur, aplikasi dan keamanan informasi Sistem Pemerintahan Berbasis Elektronik; dan
b. menjadi acuan dalam pelaksanaan Audit secara internal terhadap penyelenggaraan Teknologi Informasi Komunikasi di lingkungan Perangkat Daerah Kabupaten Polewali Mandar.

KETIGA : Keputusan Bupati ini mulai berlaku pada tanggal ditetapkan.

Ditetapkan di Polewali
pada tanggal 17 Juni 2021

BUPATI POLEWALI MANDAR,

ttd

ANDI IBRAHIM MASDAR

Salinan Sesuai Dengan Aslinya
Polewali 17 Juni 2021

Plt.KEPALA BAGIAN HUKUM,

ABDUL JALAL,SH,MM
Pangkat : Pembina Utama Muda
NIP : 19681118 199803 1 007

LAMPIRAN I KEPUTUSAN BUPATI POLEWALI MANDAR
NOMOR : 722 TAHUN 2021
TANGGAL : 17 JUNI 2021

AUDIT INTERNAL TEKNOLOGI INFORMASI DAN KOMUNIKASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

I. Umum

1. Audit Internal Teknologi Informasi dan Komunikasi (TIK) Sistem Pemerintahan Berbasis Elektronik (SPBE) bertujuan untuk menjamin agar proses-proses yang terkait dalam pengelolaan TIK dapat diterapkan secara efektif, efisien dan konsisten untuk mencapai tujuan dan sasaran SPBE.
2. Prinsip audit internal TIK memastikan adanya pengendalian intern tata Kelola TIK yang memadai.
3. Audit Internal TIK SPB) terdiri atas:
   a. audit Infrastruktur SPBE;
   b. audit Aplikasi SPBE; dan
   c. audit Keamanan SPBE.
4. Audit Internal TIK meliputi pemeriksaan hal pokok teknis pada:
   a. penerapan tata kelola dan manajemen TIK;
   b. fungsionalitas TIK;
   c. kinerja TIK yang dihasilkan; dan
   d. aspek TIK lainnya.
5. Bupati menetapkan Tim Internal Auditor TIK SPBE untuk melaksanakan Audit Internal TIK SPBE atas usulan dari Kepala Dinas Komunikasi dan Informatika Statistik dan Persandian (Dinas) setelah mempertimbangkan kompetensi audit yang dibutuhkan termasuk kompetensi teknis di bidang TIK.
6. Pelaksanaan Audit Internal TIK oleh Tim Audit Internal TIK SPBE mendapatkan pendampingan dan pembinaan aspek manajemen audit dari Inspektorat.
7. Audit Internal TIK SPBE dijadwalkan minimal satu kali dalam satu tahun. Audit Internal TIK dapat dilaksanakan di luar jadwal rutin dalam hal :
   a. terdapat laporan insiden keamanan yang sangat serius;
   b. terdapat permintaan dari Bupati; dan
   c. terdapat permintaan dari Tim Koordinasi SPBE.
8. Rencana dan Jadwal Audit Internal TIK
   a. Setelah mendapat penugasan, Tin Audit Internal TIK Menyusun Rencana Audit Internal TIK
   b. Hal-hal yang minimal harus diuraikan dalam internal audit plan, meliputi:
      1) Tujuan dan jenis Audit Internal TIK
      2) Ruang lingkup Audit Internal TIK
      3) Subyek Audit Internal TIK
      4) Peran dan tanggung jawab dalam pelaksanaan Audit Internal TIK
      5) Metode pelaksanaan Audit Internal TIK
      6) Jadwal pelaksanaan dan jangka waktu penyelesaian Audit Internal TIK
   c. Rencana dan jadwal Audit Internal TIK dikoordinasikan dengan Kepala Dinas

II. Pelaksanaan Audit Internal TIK SPBE

1. Persiapan
   a. Tim Auditor Internal TIK SPBE mengomunikasikan Rencana Audit Internal TIK pada Perangkat Daerah sebelum melaksanan Audit Internal TIK
   b. Tim Audit Internal TIK mempersiapkan seluruh bahan yang dibutuhkan dalam pelaksanaan tugas Audit Internal TIK pada Perangkat Daerah.
2. Pelaksanaan
   a. Jika berdasarkan bukti yang obyektif ditemukan ketidaksesuaian antara kondisi yang terjadi dengan standar TIK dan kebijakan terkait, maka Tim Audit Internal TIK menuliskan temuan tersebut dalam Berita Acara Pelaksanaan Audit Internal TIK.
   b. Penulisan temuan harus mencantumkan rujukan terhadap klausul-klausul standar yang berlaku umum dan/ atau kebijakan SPBE yang relevan
   c. Jika pihak yang diaudit (auditee) menerima hasil Audit Internal TIK maka Kepala Perangkat Daerah menandatangan Berita Acara Pelaksanaan Audit Internal TIK.
   d. Jika terdapat perbedaan pendapat antara Tim Audit Internal TIK dengan Auditee tentang temuan yang dituangkan dalam Berita Acara, maka Kepala Perangkat Daerah dapat memberikan sanggahan.
   e. Setelah selesai melaksanakan Audit, Tim Audit Internal TIK menyampaikan hasil audit untuk mendapatkan tindaklanjut dari Kepala Dinas, yaitu dapat berupa pembahasan bersama Langkah-langkah koreksi yang harus dilakukan, waktu penyelesaian dan pihak yang bertanggungjawab dalan penyelesaian hasil audit.
3. Tindak Lanjut Hasil Audit Internal TIK
   a. Kepala Dinas mengoordinasikan penerapan Tindakan perbaikan dengan Perangkat Daerah terkait
   b. Tim Audit Internal TIK turut memantau status tindakan perbaikan sesuai target waktu penyelesaian yang telah ditetapkan
   c. Tim Audit Internal TIK menyampaikan Laporan Hasil Audit Internal TIK kepada Bupati melalui Kepala Dinas. Sistematika Laporan Audit sekurang-kurangnya memuat: Obyek Audit Internal TIK, metode Audit Internal TIK, Temuan, Audit Internal TIK, Gap Analysis, dan Rekomendasi.

III. Audit Internal TIK Infrastruktur SPBE

1. Audit Internal TIK Infrastruktur SPBE, meliputi:
   a. Audit Internal TIK Pusat Data, terdiri atas:
      1) Perencanaan Pusat Data
      2) Pengembangan Pusat Data
      3) Pengoperasian Pusat Data
      4) Pemeliharaan Pusat Data
   b. Audit Internal TIK Jaringan Intra Pemerintah, terdiri atas:
      1) Perencanaan Jaringan Intra Pemerintah
      2) Pengembangan Jaringan Intra Pemerintah
      3) Pengoperasian Jaringan Intra Pemerintah
      4) Pemeliharaan Jaringan Intra Pemerintah

c. Audit Internal TIK Sistem Penghubung Layanan Pemerintah, terdiri atas:

1) Perencanaan Sistem Penghubung Layanan Pemerintah
2) Pengembangan Sistem Penghubung Layanan Pemerintah
3) Pengoperasian Sistem Penghubung Layanan Pemerintah
4) Pemeliharaan Sistem Penghubung Layanan Pemerintah

2. Kriteria penilaian Audit Internal TIK Infrastruktur SPBE, sebagaimana terlampir.

IV. Audit Internal TIK Aplikasi SPBE

1. Audit Internal TIK Aplikasi SPBE, meliputi:

a. Perencanaan Aplikasi, mencakup:
b. Kemampuan Aplikasi
c. Persyaratan Proses Bisnis

2. Pengembangan Aplikasi, mencakup:

a. Penggunaan aplikasi secara umum, antara lain: cara instalasi, akses terhadap aplikasi, operasi terhadap data;
b. Tutorials;
c. Dokumen Teknis; dan
d. Pesan kesalahan dan penangannya (Troubleshooting)

3. Pengoperasian Aplikasi, mencakup:

a. Lingkup pemeliharaan;
b. Alokasi sumberdaya;
c. Pencatatan kinerja;
d. Urutan/rangkaian proses pemeliharaan

4. Pemeliharaan Aplikasi, mencakup:

a. Lingkup konfigurasi;
b. Aktivitas dan manajemen konfigurasi;
c. Sumberdaya konfigurasi;
d. Penjadwalan manajemen konfigurasi

5. Kriteria penilaian Audit Internal TIK Aplikasi SPBE, sebagaimana terlampir

V. Audit Internal TIK Keamanan SPBE

1. Domain Audit Internal Keamanan SPBE, terdiri atas:

a. Keamanan Aplikasi SPBE, mencakup pengujian atas kontrol keamanan dalam:

1) Perencanaan Aplikasi SPBE;
2) Pengembangan Aplikasi SPBE;
3) Operasional Aplikasi SPBE;
4) Pemantauan Aplikasi SPBE.

b. Keamanan Infrastruktur SBPE, terdiri atas:

1) Pusat data, meliputi aspek perencanaan, pengembangan, operasional dan pemantauan Pusat Data

2) Sistem Penghubung Layanan, meliputi aspek perencanaan, pengembangan, operasional dan pemantauan Sistem Penghubung Layanan

3) Jaringan Intra, meliputi aspek perencanaan, pengembangan, operasional dan pemantauan Jaringan Intra.

2. Audit atas manajemen keamanan SPBE, terdiri ats:

   a. Audit Tata Kelola keamanan SPBE, mencakup:

      1) Pengevaluasian tata kelola keamanan SPBE
      2) Pengarahan tata kelola keamanan SPBE
      3) Pemantauan tata kelola keamanan SPBE
      4) Komunikasi tata kelola keamanan SPBE
      5) Asuransi tata kelola keamanan SPBE

   b. Audit Sistem Manajemen Keamanan SPBE, mencakup:

      1) Perencanaan Sistem Manajemen Keamanan SPBE
      2) Pengembangan Sistem Manajemen Keamanan SPBE
      3) Pelaksanaan Sistem Manajemen Keamanan SPBE
      4) Evaluasi Sistem Manajemen Keamanan SPBE
      5) Peningkatan Sistem Manajemen Keamanan SPBE

   c. Audit Pengendalian Keamanan SPBE, mencakup:

      1) kebijakan keamanan;
      2) organisasi keamanan
      3) keamanan personil;
      4) keamanan aset;
      5) keamanan akses;
      6) keamanan kriptografi;
      7) keamanan fisik dan lingkungan;
      8) keamanan operasional;
      9) keamanan komunikasi;
      10) keamanan pengembangan dan pemeliharaan;
      11) keamanan rekanan;
      12) insiden keamanan;
      13) keamanan kontinuitas; atau
      14) kepatuhan keamanan

   d. Kriteria penilaian Audit Internal TIK Keamanan SPBE, sebagaimana terlampir

BUPATI POLEWALI MANDAR

ttd

ANDI IBRAHIM MASDAR

Salinan Sesuai Dengan Aslinya
Polewali 17 Juni 2021

Plt.KEPALA BAGIAN HUKUM,

ABDUL JALAL,SH,MM
Pangkat : Pembina Utama Muda
NIP : 19681118 199803 1 007

LAMPIRAN II KEPUTUSAN BUPATI POLEWALI MANDAR
NOMOR : 722 TAHUN 2021
TANGGAL : 17 JUNI 2021

KRITERIA PENILAIAN AUDIT INTERNAL
TEKNOLOGI INFORMASI DAN KOMUNIKASI
SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

I. Audit Internal TIK Infrastruktur SPBE

1. Pusat Data

Tahapan 1	Perencanaan
Aktivitas 1	Analisis Kebutuhan
1	Apakah sudah menyusun dokumen rencana pertumbuhan (growth plan) Pusat Data seperti beban daya, pendingin, ruangan dan lain-lain?
2	Apakah sudah ada kebijakan untuk melakukan analisis kebutuhan layanan Pusat Data?
3	Apakah sudah memiliki ruang lingkup layanan Pusat Data dari sisi cakupan geografis jenis industri yang dilayani?
4	Apakah sudah memiliki dokumen tentang jenis layanan yang dibutuhkan di Pusat Data?
5	Apakah memiliki prosedur pelaporan masalah yang terjadi di Pusat Data?
Aktivitas 2	Pengelolaan Lokasi
1	Apakah bangunan Pusat Data berada pada lokasi yang aman dari bahaya seperti bencana alam, polusi, interferensi elektromagnetik, getaran dll?
2	Apakah bangunan Pusat Data mempunyai akses jalan yang cukup dan fasilitas parkir?
3	Apakah lokasi Pusat Data memiliki temperatur sekitar yang rendah dan tidak berada di kawasan yang memiliki kelembapan yang tinggi?
4	Apakah Penyelenggara Pusat Data sudah memilih lokasi Pusat Data yang aman dari bencana, mudah diakses dan mudah melakukan pengembangan /pembangunan Pusat Data?
Aktivitas 3	Pengelolaan Bangunan
1	Apakah ruang komputer tidak berada di bawah area perpipaan (plumbing) yang berbahaya?
2	Apakah jendela ruang komputer yang menghadap ke sinar matahari sudah ditutup untuk mencegah panas?
3	Apakah Pusat Data memiliki area bongkar muat yang memadai untuk menangani penghantaran barang/ peralatan?
4	Apakah Pusat Data memiliki akses/ jalur penyelamatan jika terjadi bahaya/ ancaman?
Aktivitas 4	Pengelolaan Kebakaran
1	Apakah jumlah dan lokasi pintu darurat kebakaran sudah sesuai dengan ketentuan perundang-undangan?
2	Apakah pintu darurat kebakaran dapat dibuka ke arah luar?
3	Apakah semua tanda peringatan kebakaran sudah ditempatkan pada posisinya sesuai ketentuan peraturan perundang-undangan?
4	Apakah bangunan sudah dilengkapi dengan sistem proteksi petir?

Aktivitas 5	Pengelolaan Kelistrikan
1	Apakah Pusat Data menyediakan ruang panel kelistrikan?
2	Apakah sudah tersedia catu daya listrik alternatif (seperti generator) dengan kapasitas yang memadai untuk operasional Pusat Data paling sedikit 6 (enam) jam selama kejadian gangguan listrik utama?
3	Apakah perangkat Pusat Data sudah diproteksi dengan UPS atau catu daya cadangan lainnya?
4	Apakah Pusat Data memiliki perhitungan efisiensi pemakaian listrik pada pusat data (Power Usage Effectiveness) terhadap keseluruhan beban daya maksimum pusat data?
Aktivitas 6	Pengelolaan Suhu Ruangan
1	Apakah ruang komputer sudah dijaga dan dikendalikan temperatur dengan suhu antara 18-24 °C?
2	Apakah ruang komputer sudah dijaga dan dikendalikan kelembaban ruangnya dengan kelembaban antara 50-55%?
3	Apakah peralatan pengkondisian udara sudah dihubungkan ke catu daya utama dan didukung oleh catu daya alternatif?
Aktivitas 7	Pengelolaan Pengkabelan
1	Apakah seluruh pengkabelan interior dengan tipe tidak mudah terbakar (low flammability)?
2	Apakah setiap rak memiliki akses ke sistem saluran kabel, di atas atau di bawahnya, yang memungkinkan kabel-kabel dapat ditata secara baik antar rak?
3	Apakah kabel yang melewati dinding sudah dilindungi terhadap bahaya api sesuai ketentuan peraturan perundang-undangan?
4	Apakah kabel sudah tidak diletakkan di pintu, lantai, atau digantung antar rak?
5	Apakah setiap kabel sudah memiliki label identifikasi yang unik pada kedua ujung awal dan akhir?
6	Apakah setiap rak peralatan sudah memiliki label identifikasi?
Aktivitas 8	Pengelolaan Pembagian Ruangan
1	Apakah sudah memiliki area server yang merupakan ruang penempatan rak server, server, storage dan berbagai perangkat penunjang keberlangsungan operasi server seperti sistem pendingin, UPS, sistem pemadam api dan sistem catu daya listrik?
Aktivitas 9	Pengelolaan sistem pendinginan
1	Apakah Pusat Data memiliki dokumen spesifikasi teknis sistem pendingin, skema diagram sistem pendinginan, jaminan layanan purna jual, nomor kontak layanan, dan kontrak perawatan?
2	Apakah Pusat Data memiliki temperatur ruangan : 18oC – 27oC?
3	Apakah Pusat Data memiliki tingkat perubahan temperatur ruangan per-jam maksimum : 5 oC?
4	Apakah Pusat Data memiliki kelembaban ruangan : RH (Relative Humidity) ≤ 60%, titik embun : 5.5oC – 15oC?

Aktivitas 10	Pengelolaan sistem jaringan data
1	Apakah Pusat Data memiliki label kabel yang terdiri dari nomor rak dan nomor baris pada rak?
2	Apakah Pusat Data sudah menyediakan bandwidth untuk keperluan komunikasi yang diperlukan dan memiliki jalur komunikasi data alternatif guna menghindari kepadatan lintas data serta mencegah kegagalan satu jalur (single point of failure)?
3	Apakah Pusat Data sudah menggunakan teknologi komputasi awan sehingga bagi pakai data, aplikasi, dan infrastruktur dapat dilakukan?
Tahapan 2	Pengembangan
Aktivitas 1	Implementasi
1	Apakah dalam mengembangkan Pusat Data sudah memiliki metode/standard tertentu sebagai acuan?
2	Apakah sudah ada dokumentasi selama pengembangan Pusat Data?
3	Apakah terdapat perubahan realisasi pengembangan Pusat Data dan sudah didokumentasikan?
4	Apakah pengembangan Pusat Data sudah memiliki rencana penerapan?
Aktivitas 2	Instalasi
1	Apakah sudah memiliki prosedur instalasi Pusat Data?
2	Apakah sudah memiliki daftar personil yang bertugas melakukan instalasi Pusat Data?
3	Apakah sudah memiliki rencana pelatihan terhadap personil yang melakukan instalasi Pusat Data?
4	Apakah sudah memiliki daftar fasilitas yang dibutuhkan selama instalasi Pusat Data?
Aktivitas 3	Pengujian
1	Apakah sudah memiliki rencana pengujian (Test Plan) terhadap Pusat Data?
2	Apakah sudah memiliki rancangan pengujian (Test Design) terhadap Pusat Data?
3	Apakah sudah memiliki prosedur pengujian (Test Procedures) terhadap Pusat Data?
4	Apakah sudah memiliki laporan pengujian (Test Report) terhadap Pusat Data?
Tahapan 3	Pengoperasian
Aktivitas 1	Organisasi
1	Apakah sudah memiliki struktur organisasi Pusat Data yang efektif dan efisien dengan klasifikasi tugas, distribusi dan hirarki kewenangan sesuai standard?
2	Apakah sudah mendefinisikan tugas, tanggung jawab dan ukuran kompetensi SDM Pusat Data?
Aktivitas 2	Tata Kerja
1	Apakah telah menyusun prosedur (SOP) dan tutorial terkait pengoperasian Pusat Data?
2	Apakah telah menyusun dan menyediakan Fasilitas Bantuan yang membantu petugas dalam mengoperasikan Pusat Data?
3	Apakah disediakan ruang kendali untuk melakukan fungsi pemantauan dan pengendalian?

Aktivitas 3	Manajemen Operasi
1	Apakah sudah disediakan manual operasi umum yang mencakup seluruh persyaratan operasi Pusat Data?
2	Apakah seluruh perangkat utama seperti pengkondisi udara, UPS, generator, dan lain sebagainya sudah terdapat dalam pencatatan aset?
3	Apakah seluruh konfigurasi dan prosedur operasi termasuk di dalamnya: Perubahan konfigurasi dan Set-point default sudah didokumentasikan?
4	Apakah sudah memiliki informasi dokumentasi lokasi yang meliputi bangunan/lantai, lokasi rak, denah rak dan interkonektivitas dan logik dari peralatan?
5	Apakah sudah tersedia daftar kontak tersedia yang mencatat seluruh staf Pusat Data, fungsi dan kontak rinci, pemasok, perusahaan pemeliharaan dan layanan darurat?
6	Apakah sudah tersedia perencanaan tertulis yang mudah diakses untuk menjelaskan secara rinci status alarm dan bagaimana gangguan sistem ditangani oleh staf Pusat Data?
Aktivitas 4	Pusat Pemulihan Bencana
1	Apakah penyelenggara Pusat Data sudah memiliki Pusat Pemulihan Bencana?
2	Apakah penempatan fasilitas Pusat Pemulihan Bencana sudah mempertimbangkan hal hal seperti : jarak terhadap lokasi Pusat Data yang meminimalkan risiko, biaya yang layak dan memenuhi Service Level Agreement (SLA) yang disyaratkan?
3	Apakah Penyelenggara Pusat Data sudah memiliki Rencana Kelangsungan Bisnis (Business Continuity Plan/ BCP) untuk mempertahankan kelangsungan fungsi bisnis saat gangguan terjadi dan sesudahnya?
4	Apakah Penyelenggara Pusat Data sudah memiliki Rencana Pemulihan Bencana (Disaster Recovery Planning/ DRP) untuk memperbaiki operabilitas sistem target, aplikasi, dan fasilitas computer di lokasi alternatif dalam kondisi darurat?
Aktivitas 5	Infrastruktur
1	Apakah Penyelenggara Pusat Data sudah menerapkan manajemen fasilitas pusat data seperti menyusun daftar perangkat/fasilitas, manajemen perawatan fasilitas, menyusun kontrak perawatan, memastikan ketersedian dokumen manajemen dan pelaporan perawatan?
2	Apakah Penyelenggara Pusat Data sudah menerapkan manajemen konfigurasi pusat data?
Aktivitas 6	Manajemen SDM pusat data
1	Apakah Penyelenggara Pusat Data sudah memiliki sistem manajemen untuk mengelola kompetensi sumberdaya manusia dan tenaga ahli rangka memastikan tersedianya layanan pusat data yang berkualitas?
2	Apakah Penyelenggara Pusat Data sudah memiliki program pelatihan karyawan sesuai dengan rencana peningkatan karir dan kompetensinya meliputi peraturan dan regulasi, keselamatan kerja, pengetahuan dan keterampilan dalam bidang tertentu, etika kerja, penanggulangan kondisi darurat dan prosedur standar operasi?

3	Apakah Penyelenggara Pusat Data sudah menetapkan kebijakan dan mekanisme kerja untuk mengukur kinerja sumber daya manusia yang meliputi kompetensi yang diperlukan, rencana peningkatan, dan sasaran yang terukur?
Aktivitas 7	Monitoring, pelaporan dan pengendalian
1	Apakah Penyelenggara Pusat Data sudah menerapkan monitoring, pelaporan dan pengendalian?
Aktivitas 8	Manajemen layanan pusat data
1	Apakah Penyelenggara Pusat Data sudah menerapkan manajemen dokumen kelayakan?
2	Apakah Penyelenggara Pusat Data sudah menerapkan manajemen keselamatan kerja untuk karyawan, tamu pengguna layanan pusat data dan pengguna layanan pusat data yang menetap dan berada di lingkungan gedung pusat data pada saat kejadian insiden?
3	Apakah Penyelenggara Pusat Data sudah menerapkan manajemen proyek?
Tahapan 4	Pemeliharaan
Aktivitas 1	Pemeliharaan
1	Apakah setiap staf Pusat Data dan/atau kontraktor yang bertugas dalam pemeliharaan memiliki kompetensi yang sesuai?
2	Apakah setiap peralatan yang membutuhkan pemeliharaan sudah memiliki daftar dan catatan pemeliharaan yang merinci peralatan, tanggal pemeliharaan, hasil dan kontak rinci?
3	Apakah sudah mendeskripsikan siklus hidup peralatan dan perangkat (identifikasi garansi/lifetime, perjanjian pemeliharaan dan laporan kinerja peralatan)?
4	Apakah sudah memiliki SOP pemeliharaan komponen dan penggantian suku cadang sesuai standard?
5	Apakah sudah menyusun laporan perencanaan dan penjadwalan pemeliharaaan komponen Pusat Data?
Aktivitas 2	Manajemen Konfigurasi Perangkat Keras/MKP (Hardware Configuration Management)
1	Apakah sudah ditentukan apa saja yang menjadi lingkup manajemen konfigurasi perangkat keras?
2	Bagaimana cara mengelola konfigurasi perangkat keras?
3	Apa saja aktivitas yang dilakukan pada proses manajemen konfigurasi perangkat keras?
4	Apakah sudah memiliki jadwal untuk melakukan proses manajemen konfigurasi perangkat keras?
5	Apakah sudah memiliki sumberdaya untuk melakukan proses manajemen konfigurasi perangkat keras?
Aktivitas 3	Pemantauan
1	Apakah Pusat Data sudah memiliki kajian analisa risiko yang meliputi risiko yang mungkin terjadi, dampak, dan strategi mengurangi risiko yang dipantau terus menerus?
2	Apakah seluruh perangkat kritis seperti status UPS, kondisi gangguan, dan lain-lain sudah dipantau secara kontinyu?

3	Apakah Pusat Data memiliki sistem monitoring lingkungan Pusat Data (environtment monitoring system) yang meliputi antara lain monitoring temperatur, kelembapan, asap, kebakaran, kebocoran air, dan tegangan listrik?
4	Apakah Penyelenggara Pusat Data sudah membuat laporan pemantauan yang meliputi tren laju pemanfaatan sumber daya listrik, pendingin, rak server, rekaman alarm dan kejadian per periode?
5	Apakah efisiensi energi sudah dimonitor secara berkala sekurang-kurangnya 2 (dua) kali dalam 1 (satu) tahun dengan menggunakan acuan pengukuran power usage effectiveness (PUE)?

2. Jaringan Intra Pemerintah

Tahapan 1	Perencanaan
Aktivitas 1	Kebutuhan Bisnis (Business Requirement)
1	Apakah jaringan dapat menyampaikan solusi yang diperlukan untuk kebutuhan layanan SPBE?
2	Apakah sudah dijelaskan secara rinci apa yang dibutuhkan pengguna dan perannya dalam proses perencanaan jaringan?
3	Apakah sudah dijelaskan ruang lingkup jaringan yang direncanakan yang mencakup kebutuhan fungsional dan non-fungsional?
Aktivitas 2	Kebutuhan Jaringan (Network Requirement)
1	Apa saja proses-proses / fungsi / layanan yang dapat dilakukan oleh jaringan?
2	Apa sajakah kemampuan kerja yang dapat dicapai dan dilakukan oleh jaringan?
3	Apakah terdapat batasan khusus yang harus ada dalam rancangan jaringan?
Aktivitas 3	Rancangan Jaringan (Network Design)
1	Apa saja persiapan yang dilakukan dalam melakukan perancangan jaringan?
2	Apakah sudah dilakukan analisis lingkungan dalam melakukan perancangan jaringan?
3	Bagaimana dan seberapa besar cakupan dari jaringan yang akan dirancang?
Tahapan 2	Pengembangan
Aktivitas 1	Implementasi Jaringan (Network implementation)
1	Apa sajakah metode-metode pengembangan yang digunakan dalam pengembangan jaringan?
2	Apakah sudah menyusun konfigurasi jaringan?
3	Apakah sudah menyusun Diagram LAN/ Pengkabelan terkait pengembangan jaringan?
Aktivitas 2	Instalasi (Installation)
1	Apakah telah menyusun prosedur untuk instalasi jaringan?
2	Apakah telah menyusun dan menetapkan personel untuk instalasi jaringan?
3	Apakah telah menyusun rencana pelatihan personil yang akan menginstalasi jaringan?
4	Apakah telah menyusun jadwal untuk instalasi jaringan?
5	Apakah telah menyiapkan fasilitas yang dibutuhkan untuk instalasi jaringan?
Aktivitas 3	Pengujian (Testing)
1	Apakah telah menyusun dokumen Rencana Pengujian dalam rangka pengembangan dan pengujian jaringan?
2	Apakah telah menyusun dokumen Rancangan Pengujian dalam rangka pengembangan dan pengujian jaringan?

3	Apakah telah menyusun dokumen Prosedur Pengujian dalam rangka pengembangan dan pengujian jaringan?
4	Apakah telah menyusun dokumen Laporan Pengujian dalam rangka pengembangan dan pengujian jaringan?
Tahapan 3	Pengoperasian
Aktivitas 1	Utilisasi/ Kinerja Jaringan (Network utilization/performance)
1	Apakah telah menyusun dan menyediakan pedoman penggunaan Jaringan dan Perangkat Keras (instalasi, akses, navigasi, utilisasi dan report) dalam rangka pengoperasian jaringan?
2	Apakah telah menyusun dan menyediakan Fasilitas Bantuan yang membantu petugas dalam mengoperasikan jaringan?
Tahapan 4	Pemeliharaan
Aktivitas 1	Pemeliharaan Jaringan (Network Maintenance)
1	Apakah telah menentukan ruang lingkup tanggung jawab pemeliharaan jaringan?
2	Apakah telah menentukan urutan proses pemeliharaan jaringan?
3	Apakah telah membentuk tim dan personil yang akan melakukan pemeliharaan jaringan?
Aktivitas 2	Manajemen Konfigurasi Jaringan/MKJ (Network Configuration Management)
1	Apakah sudah ditentukan apa saja yang menjadi lingkup manajemen konfigurasi jaringan?
2	Apa saja aktivitas yang dilakukan pada proses manajemen konfigurasi jaringan?
3	Apakah sudah memiliki sumberdaya untuk melakukan proses manajemen konfigurasi jaringan?

3. Sistem Penghubung Layanan

Tahapan 1	Perencanaan
Aktivitas 1	Prinsip
1	Dapat digunakan kembali (reusable) agar dapat dimanfaatkan secara berulang tanpa perlu dikembangkan lagi oleh pihak yang membutuhkan?
2	Dapat dikembangkan lebih lanjut secara mandiri dan memberi kemudahan bagi pengembangan lebih lanjut tanpa perlu melibatkan pengembang awal?
3	Dapat diperiksa (auditable) dan memiliki kemudahan bagi yang memiliki kewenangan untuk melakukan pengamatan, verifikasi, pengujian, dan pemeriksaan terhadapnya?
4	Dapat diawasi dan dinilai tingkat pemanfaatannya?
5	Dapat dibagipakaikan antar Sistem Elektronik yang berbeda karakteristik?
Aktivitas 2	Kebijakan
1	Memiliki kajian kebutuhan penerapan Sistem Penghubung sekurang-kurangnya meliputi: Dasar hukum, Pertimbangan, Pihak yang terkait, Manfaat dan Ruang lingkup?
Aktivitas 3	Organisasi
1	Memiliki satuan kerja yang bertugas untuk memastikan penerapan Sistem Penghubung?
2	Memiliki sumber daya manusia yang kompeten di bidang Sistem Penghubung?
Aktivitas 4	Teknis
1	Dikembangkan dalam bentuk antarmuka pemrograman aplikasi?
2	Memiliki kemampuan untuk menjaga keberlangsungan dan ketersediaan Interoperabilitas Data?
3	Memiliki infrastruktur yang sesuai dengan kebutuhan kapasitas dan tingkat layanan?

4	Memiliki panduan teknis dan panduan penggunaan Sistem Penghubung yang terpelihara dan terjaga keterkiniannya?
Tahapan 2	Pengembangan
Aktivitas 1	Implementasi
1	Apakah dalam mengembangkan Sistem Penghubung sudah memiliki metode/standard tertentu sebagai acuan?
2	Apakah sudah ada dokumentasi rancangan pengembangan Sistem Penghubung (Development Design)?
3	Apakah pengembangan Sistem Penghubung sudah memiliki rencana penerapan?
Aktivitas 2	Instalasi
1	Apakah sudah memiliki prosedur instalasi Sistem Penghubung?
2	Apakah sudah memiliki daftar personil yang bertugas melakukan instalasi Sistem Penghubung?
3	Apakah sudah memiliki rencana pelatihan terhadap personil yang melakukan instalasi Sistem Penghubung?
4	Apakah sudah memiliki jadwal instalasi Sistem Penghubung?
5	Apakah sudah memiliki daftar fasilitas yang dibutuhkan selama instalasi Sistem Penghubung?
Aktivitas 3	Pengujian
1	Apakah sudah memiliki rencana pengujian (Test Plan) terhadap Sistem Penghubung?
2	Apakah sudah memiliki rancangan pengujian (Test Design) terhadap Sistem Penghubung?
3	Apakah sudah memiliki prosedur pengujian (Test Procedures) terhadap Sistem Penghubung?
4	Apakah sudah memiliki laporan pengujian (Test Report) terhadap Sistem Penghubung?
Tahapan 3	Pengoperasian
Aktivitas 1	Penyelenggaraan
1	Sistem Penghubung dibangun dan dioperasikan oleh Penyelenggara Sistem Penghubung?
2	Sistem Penghubung dapat digunakan oleh Infrastruktur Instansi Daerah?
3	Sistem Penghubung yang digunakan oleh Infrastruktur Pemerintah Daerah sudah terhubung kedalam Jaringan Intra Pemerintah?
4	Penyelenggaraan Sistem Penghubung oleh Infrastruktur Pemerintah Daerah dilaksanakan organisasi yang membidangi urusan Komunikasi dan Informatika?
Aktivitas 2	Dokumen Mekanisme Kerja
1	Memiliki Panduan Teknis (Technical Guide) yang berisi prosedur kerja?
2	Memiliki Panduan Pengguna (User Guide) yang berisi panduan penggunaan?
Tahapan 4	Pemeliharaan
Aktivitas 1	Pemeliharaan
1	Telah menentukan ruang lingkup tanggung jawab pemeliharaan Sistem Penghubung?
2	Telah menentukan urutan proses pemeliharaan Sistem Penghubung?
3	Telah membentuk tim dan personil yang akan melakukan pemeliharaan Sistem Penghubung?

4	Telah mengalokasikan sumber daya terkait dalam rangka mendukung proses pemeliharaan Sistem Penghubung?
5	Telah melakukan Pelacakan Kinerja pada Sistem Penghubung sebagai bagian dari proses pemeliharaan?

II. Audit Internal TIK Aplikasi SPBE

Tahapan 1	Perencanaan
Aktivitas 1	Persyaratan Layanan (Business Requirement)
1	Apakah aplikasi dapat menyampaikan solusi yang diperlukan untuk kebutuhan layanan?
2	Apakah aplikasi dapat menjelaskan secara rinci apa yang dibutuhkan pengguna dalam proses layanan?
Aktivitas 2	Kebutuhan Perangkat Lunak (Software Requirement)
3	Apa saja proses-proses / fungsi / layanan yang dapat dilakukan oleh aplikasi?
4	Bagaimana aplikasi menggambarkan antarmuka yang dapat berinteraksi/berhubungan dengan komponen aplikasi lainnya?
5	Apa sajakah kemampuan kerja yang dapat dicapai oleh aplikasi?
6	Apakah terdapat batasan khusus yang harus ada di dalam rancangan perangkat lunak?
Aktivitas 3	Rancangan Perangkat Lunak (Software Design)
7	Bagaimana bentuk deskripsi sistem dari aplikasi?
8	Bagaimana deskripsi rancangan basisdata dari aplikasi?
9	Bagaimana bentuk arsitektur dari aplikasi sehingga dapat menggambarkan keseluruhan sistem, proses, dan layanan aplikasi?
10	Bagaimana gambaran dan karakteristik antarmuka dari aplikasi?
Tahapan 2	Pengembangan
Aktivitas 1	Implementasi Perangkat Lunak (Software Implementation)
11	Apa sajakah metode-metode pengembangan perangkat lunak yang digunakan dalam pengembangan aplikasi?
12	Apakah sudah memiliki dokumentasi dari kode-kode pengembangan perangkat lunak?
13	Apakah perangkat lunak dapat digunakan kembali secara berkesinambungan di masa yang akan datang?
14	Apakah kode sumber aplikasi dapat dimodifikasi/bersifat open source?
Aktivitas 2	Pengujian (Testing)
15	Apakah sudah memiliki rencana pengujian (Test Plan) terhadap aplikasi?
16	Apakah sudah memiliki rancangan pengujian (Test Design) terhadap aplikasi?
17	Apakah sudah memiliki rancangan atau rangkaian mengenai tindakan yang dilakukan oleh penguji/tester?
18	Apakah sudah memiliki prosedur-prosedur pengujian terhadap aplikasi?
19	Apakah sudah memiliki laporan pengujian terhadap aplikasi?
Aktivitas 3	Instalasi/Pemasangan (Installation)
20	Apakah sudah memiliki prosedur instalasi/pemasangan untuk aplikasi
21	Apakah sudah memiliki daftar personil yang bertugas untuk melakukan instalasi/pemasangan aplikasi?
22	Apakah sudah memiliki rencana pelatihan terhadap personil yang melakukan instalasi/pemasangan aplikasi?
23	Apakah sudah memiliki jadwal instalasi/pemasangan aplikasi?

24	Apakah sudah memiliki daftar fasilitas yang dibutuhkan selama instalasi/pemasangan aplikasi?
Tahapan 3	Pengoperasian
Aktivitas 1	Penggunaan Perangkat Lunak (Software Usage)
25	Apakah aplikasi sudah bisa berkolaborasi dengan aplikasi lain?
26	Apakah aplikasi merupakan perangkat lunak yang dipersiapkan untuk dapat digunakan/diaplikasikan secara umum?
27	Apakah memiliki prosedur/petunjuk/manual penggunaan aplikasi?
28	Apakah penamaan perintah-perintah dalam perangkat lunak distandardkan/dibakukan?
29	Bagaimana respon aplikasi dalam menanggapi kesalahan dan apakah memiliki solusi terhadap permasalahan tersebut?
30	Apakah memiliki/menyediakan fasilitas bantuan dan dokumentasi mengenai pertanyaan yang sering diajukan (FAQ)?
Tahapan 4	Pemeliharaan
Aktivitas 1	Pemeliharaan Perangkat Lunak (Software Maintenance)
31	Apakah sudah ditentukan lingkup apa saja yang akan dilakukan pada proses pemeliharaan aplikasi?
32	Apakah memiliki urutan/rangkaian proses pemeliharaan aplikasi?
33	Apakah sudah dibentuk tim/kelompok kerja untuk melaksanakan pemeliharaan aplikasi dengan klasifikasi tugas yang sudah ditentukan?
34	Apakah sudah ditentukan alokasi sumber daya untuk proses pemeliharaan aplikasi?
35	Apakah memiliki cara untuk dapat mengetahui, merekam, dan melacak kinerja dari aplikasi?
Aktivitas 2	Manajemen Konfigurasi Perangkat Lunak (Software Configuration Management)
36	Apakah sudah ditentukan apa saja yang menjadi lingkup manajemen konfigurasi perangkat lunak?
37	Bagaimana cara mengelola konfigurasi perangkat lunak?
38	Apa saja aktivitas yang dilakukan pada proses manajemen konfigurasi perangkat lunak?
39	Apakah sudah memiliki jadwal untuk melakukan proses manajemen konfigurasi perangkat lunak?
40	Apakah sudah memiliki sumberdaya untuk melakukan proses manajemen konfigurasi perangkat lunak?

III. Audit Internal TIK Keamanan SPBE

1. Audit Keamanan Pusat Data SPBE

PERENCANAAN	
1	identifikasi keamanan lokasi dan lingkungan pusat data telah dilakukan
2	identifikasi keamanan jalur kabel jaringan data telah dilakukan
3	identifikasi keamanan jalur kabel listrik dan sistem kelistrikan pusat data telah dilakukan
4	identifikasi keamanan sistem pengendalian kebakaran telah dilakukan
5	identifikasi keamanan akses fisik gedung dan perimeter pusat data telah dilakukan
PENGEMBANGAN	
1	persyaratan untuk pengembangan pusat data dan berbagai fasilitas penunjangnya telah ditetapkan dan diterapkan.
2	perubahan dan penyesuaian atas desain pusat data telah dikendalikan dengan menggunakan prosedur pengendalian perubahan yang formal.
3	kegiatan pengembangan pusat data telah diawasi dan dipantau pihak organisasi

4	pengujian keamanan saat pengembangan pusat data telah dilakukan.
OPEPRASIONAL	
1	pengunjung yang akan memasuki area pusat data telah dikendalikan dengan mendapatkan ijin masuk dari penyelenggara pusat data.
2	untuk memasuki area pusat data telah menggunakan sistem pengendali akses berupa kartu akses elektronik, biometrik atau pemindai jari.
3	mobilisasi (keluar/masuk) perangkat pada pusat data telah dikendalikan dengan surat ijin masuk/keluar barang, dilakukan melalui area bongkar muat dan melalui pemeriksaan fisik atas penerimaan dan pengiriman barang di pusat data.
PEMANTAUAN	
1	pemantauan terhadap akses personil dan pengunjung pusat data telah dilakukan
2	pemantauan terhadap akses masuk dan keluar barang pada pusat data telah dilakukan
3	pemantauan terhadap kondisi lingkungan pusat data telah dilakukan mencakup suhu ruangan pusat data, kelembaban ruangan, kebocoran air, sistem pemantauan kebakaran dari sensor panas dan sensor asap, ketersediaan pasokan listrik dan penggunaan daya listrik.

2. Audit Keamanan Jaringan Intra

PERENCANAAN	
1	kebijakan tentang perencanaan, pengembangan, operasional, dan pemantauan keamanan JI;
2	identifikasi, penetapan peran, tanggung jawab, dan kewenangan dari pihak-pihak yang terkait dengan keamanan JI;
3	pengendalian atas pembuatan, perubahan, dan penyimpanan dokumentasi kebijakan, standar, prosedur, desain arsitektur teknis, serta informasi lainnya terkait JI.
PENGEMBANG	
1	1) pengendalian keamanan secara mendalam (defense in depth) terhadap ancaman keamanan dari internal maupun eksternal JI.
2	3) standar spesifikasi dan konfigurasi teknis terkait desain, perangkat jaringan dan perangkat keamanan jaringan terkait JIP.
3	4) pengendalian keamanan terhadap ancaman malware dan intrusion yang berasal dari internal maupun eksternal JIP.
4	pengendalian keamanan terkait JI terhadap berbagai kebutuhan bisnis, sekurang-kurangnya meliputi:
	a) keamanan akses jarak jauh (remote/VPN).
	b) keamanan akses jaringan ke instansi lain.
	c) keamanan akses jaringan ke internet.
	d) keamanan akses jaringan nirkabel
OPERASIONAL	
1	kebijakan terkait operasional keamanan JI bagi pengguna yang mencakup ketentuan akses JI, ketentuan penggunaan JI yang aman, dan konsekuensi pelanggaran dan penyalahgunaan JI telah dilaksanakan.
2	pengendalian integritas konfigurasi yang dapat mencegah adanya perubahan yang tidak sah terhadap konfigurasi perangkat terkait JI
3	pemeliharaan perangkat terkait keamanan JI secara berkala untuk preventif maupun korektif.

4	pengendalian keberlangsungan keamanan JI, mencakup sekurang-kurangnya pencadangan konfigurasi dan perangkat terkait JI.
PEMANTAUAN	
1	identifikasi perangkat jaringan dan keamanan jaringan terkait JI yang dilakukan pemantauan.
2	identifikasi jenis informasi minimum yang harus terdapat dalam audit log pada perangkat jaringan dan keamanan jaringan terkait JI.
3	penerapan audit log yang mencatat informasi dan kejadian yang terkait dengan keamanan JI, yang sekurang-kurangnya meliputi:
	a) waktu, sumber, dan tujuan
	b) ancaman dan/atau kejadian keamanan yang berasal dari internal maupun eksternal
	c) aktivitas-aktivitas anomali di luar kondisi normal operasional.
4	pelaporan hasil pemantauan keamanan JI secara berkala dan terdokumentasi.

3. Audit Keamanan Sistem Layanan Penghubung

PERENCANAAN	
1	Kebijakan tentang keamanan dalam perencanaan, pengembangan, implementasi dan operasional, serta pemantauan dan pemeliharaan aplikasi yang terdokumentasi;
2	Identifikasi, penetapan peran, tanggung jawab, dan kewenangan dari pihak-pihak yang terkait dengan keamanan aplikasi;
4	Identifikasi standar kebutuhan dan persyaratan minimum keamanan aplikasi yang, sekurang-kurangnya meliputi:
	a) Kebutuhan kerahasiaan dan privasi
	b) Kebutuhan integritas
	c) Kebutuhan ketersediaan dan kontinuitas
	d) Kebutuhan otentikasi
	e) Kebutuhan otorisasi
	f) Kebutuhan akuntabilitas dan *non-repudiation*
	g) Kebutuhan peraturan, regulasi hukum dan perundang-undangan yang berlaku
5	Identifikasi kendali keamanan tambahan, jika aplikasi dikembangkan oleh pihak ketiga, meliputi:
	a) hak kekayaan intelektual, kepemilikan aplikasi dan kode sumber asli
	b) penyimpanan kode sumber asli berdasarkan hak kepemilikan
	c) kebijakan, prosedur, dan standar terkait keamanan aplikasi pada pihak ketiga
	d) hak untuk melakukan verifikasi dan validasi kendali keamanan pada aplikasi, termasuk melakukan reviu kode sumber apabila diperlukan
	e) komitmen dan *Service Level Agreement* (SLA) terkait penyelesaian jika terdapat error, bug, atau permasalahan dan insiden terkait keamanan aplikasi
	f) jaminan tidak terdapat *malicious code* dan *backdoor*
	g) perjanjian kerahasiaan
PENGEMBANGAN	
1	penyimpanan dan pengelolaan tiap versi kode sumber secara aman (secure repository & version control).
2	pemisahan lingkungan pengembangan dari lingkungan produksi.

3	memastikan seluruh proses pengujian terdokumentasi dengan baik.
IMPLEMENTASI DAN OPERASIONAL	
1	identifikasi standar konfigurasi keamanan dan penguatan keamanan (security hardening), sekurang-kurangnya meliputi:
	a) konfigurasi penguatan keamanan sistem operasi.
	b) perubahan akun, password dan konfigurasi *default.*
	c) penonaktifan fungsi debug..
	d) penyesuaian dan pembatasan hak akses sesuai kebutuhan lingkungan produksi.
	e) penghapusan informasi sensitif pada kode sumber dan konfigurasi (*hardcoded & plaintext sensitive information*).
	f) penghapusan dan/atau penyesuaian akun, konfigurasi, dan data yang dihasilkan pada tahap pengembangan.
PEMELIHARAAN DAN PEMANTAUAN	
1	Penerapan dan pemantauan audit log yang mencatat informasi dan kejadian yang terkait dengan keamanan aplikasi , yang sekurang-kurangnya meliputi:
	a) waktu, sumber, dan tujuan;
	b) ancaman dan/atau kejadian keamanan yang berasal dari internal maupun eksternal;
	c) aktivitas-aktivitas anomali di luar kondisi normal operasional.
2	peninjauan ulang secara berkala terhadap aktivitas pengguna, khususnya pengguna dengan hak akses administratif (administrator/super user)
3	pemantauan terhadap kerentanan pada komponen perangkat lunak dan aplikasi serta tindak lanjutnya (patching)

4. Audit Keamanan Aplikasi

PERENCANAAN	
1	Kebijakan tentang keamanan dalam perencanaan, pengembangan, implementasi dan operasional, serta pemantauan dan pemeliharaan aplikasi yang terdokumentasi
2	Identifikasi, penetapan peran, tanggung jawab, dan kewenangan dari pihak-pihak yang terkait dengan keamanan aplikasi
3	Identifikasi standar kebutuhan dan persyaratan minimum keamanan aplikasi, meliputi:
	a) Kebutuhan kerahasiaan dan privasi
	b) Kebutuhan integritas
	c) Kebutuhan ketersediaan dan kontinuitas
	d) Kebutuhan otentikasi
	e) Kebutuhan otorisasi
	f) Kebutuhan akuntabilitas dan *non-repudiation*
	g) Kebutuhan peraturan, regulasi hukum dan perundang-undangan yang berlaku
4	Identifikasi kendali keamanan tambahan, jika aplikasi dikembangkan oleh pihak ketiga, meliputi:
	a) Hak kekayaan intelektual, kepemilikan aplikasi dan kode sumber asli
	b) Penyimpanan kode sumber asli berdasarkan hak kepemilikan
	c) Kualifikasi kapabilitas personil terkait keamanan aplikasi
	d) Komitmen dan *Service Level Agreement* (SLA) terkait penyelesaian jika terdapat error, bug, atau permasalahan dan insiden terkait keamanan aplikasi
	e) Jaminan tidak terdapat *malicious code* dan *backdoor*
	f) perjanjian kerahasiaan

PENGEMBANGAN	
1	Penyimpanan dan pengelolaan tiap versi kode sumber secara aman (*secure repository & version control*).
2	Pemisahan lingkungan pengembangan dari lingkungan produksi.
3	Memastikan seluruh proses pengujian terdokumentasi dengan baik.
IMPLEMENTASI DAN OPERASIONAL	
1	Identifikasi standar konfigurasi keamanan dan penguatan keamanan (security hardening), meliputi:
	a) Konfigurasi penguatan keamanan sistem operasi
	b) Perubahan akun, password dan konfigurasi *default*
	c) Penonaktifan fungsi debug
	d) Penyesuaian dan pembatasan hak akses sesuai kebutuhan lingkungan produksi
	e) penghapusan informasi sensitif pada kode sumber dan konfigurasi (*hardcoded & plaintext sensitive information*)
	f) penghapusan dan/atau penyesuaian akun, konfigurasi, dan data yang dihasilkan pada tahap pengembangan
PEMELIHARAAN DAN PEMANTAUAN	
1	Penerapan dan pemantauan audit log yang mencatat informasi dan kejadian yang terkait dengan keamanan aplikasi , yang sekurang-kurangnya meliputi:
	a) Waktu, sumber, dan tujuan;
	b) Ancaman dan/atau kejadian keamanan yang berasal dari internal maupun eksternal;
	c) Aktivitas-aktivitas anomali di luar kondisi normal operasional.
2	peninjauan ulang secara berkala terhadap aktivitas pengguna, khususnya pengguna dengan hak akses administratif (*administrator/ super user*)
3	pemantauan terhadap kerentanan pada komponen perangkat lunak dan aplikasi serta tindak lanjutnya (*patching*)

BUPATI POLEWALI MANDAR

ttd

ANDI IBRAHIM MASDAR

Salinan Sesuai Dengan Aslinya
Polewali 17 Juni 2021

Plt.KEPALA BAGIAN HUKUM,

ABDUL JALAL,SH,MM
Pangkat : Pembina Utama Muda
NIP : 19681118 199803 1 007