SALINAN

GUBERNUR SULAWESI TENGAH

PERATURAN GUBERNUR SULAWESI TENGAH

NOMOR 25 TAHUN 2023

TENTANG

MANAJEMEN KEAMANAN INFORMASI
SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

DENGAN RAHMAT TUHAN YANG MAHA ESA

GUBERNUR SULAWESI TENGAH,

Menimbang :

a. bahwa dalam rangka melindungi kerahasian keutuhan dan ketersediaan Aset Informasi di lingkungan Pemerintahan dari berbagai ancaman keamanan Informasi baik dari dalam maupun luar, perlu adanya manajeman keamanan Informasi;
b. bahwa sesuai ketentuan Pasal 41 ayat (1) Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik dan Pasal 17 ayat (1) Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajem Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis Dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik, setiap Instansi Pusat dan Pemerintah Daerah harus menerapkan Keamanan Sistem Pemerintahan Berbasis Elektronik;
c. bahwa berdasarkan ketentuan Pasal 19 ayat (1) Peraturan Gubernur Sulawesi Tengah Nomor 52 Tahun 2022 tentang Sistem Pemerintahan Berbasis Elektroni, dalam rangka perlindungan keamanan, kerahasiaan, kekinian, akurasi serta keutuhan data dan Informasi, Perangkat Daerah menyusun kebijakan keamanan Informasi;
d. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, Huruf b dan Huruf c, perlu menetapkan Peraturan Gubernur tentang Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik;

Mengingat :

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

2. 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 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 2 Tahun 2022 tentang Cipta Kerja menjadi Undang-Undang (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 41, Tambahan Lembaran Negara Republik Indonesia Nomor 6856);
3. Undang-Undang Nomor 6 Tahun 2022 tentang Provinsi Sulawesi Tengah (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 66, Tambahan Lembaran Negara Republik Indonesia Nomor 6777);
4. Peraturan Presiden Nomor 95 Tahun 2018 tentang Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
5. Peraturan Presiden Nomor 82 Tahun 2022 tentang Perlindungan Infrastruktur Informasi Vital (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 129);
6. Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Pemerintah Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2021 Nomor 541);

MEMUTUSKAN :

Menetapkan : PERATURAN GUBERNUR TENTANG MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK.

BAB I

KETENTUAN UMUM

Pasal 1

Dalam Peraturan Gubernur ini yang dimaksud dengan:

1. Informasi adalah sebuah keterangan, pernyataan, gagasan, atau tanda-tanda yang mengandung nilai, makna, dan pesan, baik data, fakta maupun penjelasannya yang dapat dilihat, didengar, dan dibaca yang disajikan dalam berbagai kemasan dan format sesuai dengan perkembangan teknologi Informasi dan komunikasi secara Elektronik.

2. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan Pemerintahan yang memanfaatkan teknologi Informasi dan komunikasi untuk memberikan layanan kepada pengguna SPBE.
3. Sistem Manajemen Keamanan Informasi yang selanjutnya disebut SMKI adalah bagian dari Sistem Manajemen secara keseluruhan berdasarkan pendekatan risiko bisnis, untuk menetapkan, menerapkan, mengoperasikan, memantau, mengkaji, meningkatkan, dan memelihara keamanan Informasi.
4. Teknologi Informasi dan Komunikasi yang selanjutnya disingkat TIK adalah segala kegiatan yang terkait dengan pemrosesan, manipulasi, pengelolaan, dan pemindahan Informasi antar media.
5. Sistem adalah kumpulan komponen atau elemen-elemen yang saling berhubungan satu sama lain untuk mencapai suatu tujuan tertentu.
6. Keamanan Informasi adalah suatu kondisi untuk melindungi Aset yang dimiliki organisasi dari berbagai ancaman pihak internal maupun eksternal untuk menjamin kelanjutan proses bisnis, mengurangi risiko bisnis, serta terjaganya aspek kerahasiaan, keutuhan dan ketersediaan dari Informasi.
7. Keamanan SPBE mencakup penjaminan kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan (*nonrepudiation*) sumber daya terkait data dan Informasi, Infrastruktur SPBE, dan Aplikasi SPBE.
8. Aset Informasi adalah unit Informasi yang dapat dipahami, dibagi, dilindungi dan dimanfaatkan secara efektif.
9. Manajemen Keamanan SPBE adalah serangkaian proses untuk mencapai penerapan keamanan SPBE yang efektif, efisien, dan berkesinambungan, serta mendukung layanan SPBE yang berkualitas.
10. Perangkat Keras adalah semua jenis piranti atau komponen Computer yang bagian fisiknya dapat dilihat secara kasat mata dan dirasakan langsung.
11. Perangkat Lunak adalah satu atau sekumpulan program komputer, prosedur, dan/atau dokumentasi yang terkait, dalam pengoperasian Sistem Elektronik.
12. Pusat Data adalah fasilitas yang digunakan untuk penempatan Sistem Elektronik dan komponen terkait lainnya untuk keperluan penempatan, penyimpanan dan pengolahan data, dan pemulihan data.
13. Kerahasiaan adalah sesuai dengan konsep hukum tentang kerahasian (*confidentiality*) atas Informasi dan komunikasi secara Elektronik.

14. Keutuhan adalah sesuai dengan konsep hukum tentang keutuhan (*integrity*) atas Informasi Elektronik.
15. Ketersediaan adalah sesuai dengan konsep hukum tentang ketersediaan (*availability*) atas Informasi Elektronik.
16. Aplikasi SPBE adalah satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas atau fungsi Layanan SPBE.
17. Layanan SPBE adalah keluaran yang dihasilkan oleh 1 (satu) atau beberapa fungsi aplikasi SPBE dan yang memiliki nilai manfaat.
18. Infrastruktur SPBE adalah semua Perangkat Keras, Perangkat lunak, dan fasilitas yang menjadi penunjang utama untuk menjalankan Sistem, aplikasi, komunikasi data, pengolahan dan penyimpanan data, Perangkat integrasi/penghubung, dan Perangkat Elektronik lainnya.
19. Sistem Elektronik adalah serangkaian Perangkat dan prosedur Elektronik yang berfungsi untuk mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengirimkan, dan/atau menyebarkan Informasi Elektronik.
20. Transaksi Elektronik adalah perbuatan hukum yang dilakukan dengan menggunakan komputer, jaringan komputer, dan/atau media Elektronik lainnya.
21. Informasi Elektronik adalah satu atau sekumpulan data Elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange* (EDI), surat elektronik, *telegram, teleks, telecopy* atau sejenisnya, huruf, tanda, angka, kode akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.
22. Daerah adalah Provinsi Sulawesi Tengah.
23. Pemerintah Daerah adalah Gubernur sebagai unsur penyelenggara Pemerintah Daerah yang memimpin pelaksanaan urusan Pemerintah yang menjadi kewenangan Daerah otonom.
24. Gubernur adalah Gubernur Sulawesi Tengah.
25. Sekretaris Daerah adalah Sekretaris Daerah Provinsi Sulawesi Tengah.
26. Perangkat Daerah adalah unsur pembantu kepala daerah dan Dewan Perwakilan Rakyat Daerah dalam Penyelenggaraan Urusan Pemerintahan yang menjadi kewenangan Daerah.
27. Kepala Dinas adalah Dinas Komunikasi, Informatika, Persandian dan Statistik Provinsi Sulawesi Tengah.

28. Dinas Komunikasi, Informatika, Persandian dan Statistik Provinsi Sulawesi Tengah yang selanjunya disingkat DKIPS adalah Perangkat Daerah yang menyelenggarakan urusan Pemerintahan di bidang persandian pada Dinas Komunikasi, Informatika, Persandian dan Statistik.

Pasal 2

(1) Pembentukan Peraturan Gubernur ini dimaksudkan sebagai pedoman bagi Perangkat Daerah dalam mengelola manajemen Keamanan Informasi SPBE secara terpadu dengan memastikan terjaganya aspek kerahasiaan, keutuhan dan ketersediaan pada Informasi.
(2) Proses manajemen Keamanan Informasi SPBE sebagaimana dimaksud pada ayat (1) meliputi:
    a. penetapan ruang lingkup;
    b. penetapan penanggung jawab;
    c. perencanaan;
    d. dukungan pengoperasian;
    e. standar dan prosedur pengendalian;
    f. manajemen risiko;
    g. pengelolaan pihak ketiga;
    h. evaluasi kinerja; dan
    i. perbaikan berkelanjutan.

BAB II
PENETAPAN RUANG LINGKUP

Pasal 3

(1) Penetapan ruang lingkup manajemen Keamanan Informasi SPBE meliputi:
    a. data dan Informasi SPBE;
    b. aplikasi SPBE; dan
    c. infrastruktur SPBE.
(2) Penetapan ruang lingkup sebagaimana dimaksud pada ayat (1) merupakan Aset Pemerintah Daerah yang harus diamankan dalam SPBE.

Pasal 4

(1) Data dan Informasi sebagaimana dimaksud dalam Pasal 3 ayat (1) huruf a merupakan data dan Informasi dalam bentuk Elektronik meliputi satu atau sekumpulan data Elektronik, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, Pertukaran Data Elekronik, surat Elektronik, huruf, tanda, angka, kode akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.

(2) Aplikasi SPBE dan infrastruktur SPBE sebagaimana dimaksud dalam Pasal 3 ayat (1) huruf b dan huruf c yang saling terintegrasi merupakan Sistem Elektronik.

BAB III
PENETAPAN PENANGGUNG JAWAB

Pasal 5

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

Pasal 6

(1) Dalam melaksanakan tugas sebagai penanggung jawab Keamanan Informasi, koordinator SPBE sebagaimana dimaksud dalam Pasal 5 ayat (3) menetapkan pelaksana teknis Keamanan SPBE.
(2) Pelaksana teknis keamanan SPBE sebagaimana dimaksud pada ayat (1) terdiri atas:
    a. ketua tim; dan
    b. anggota tim.
(3) Ketua tim sebagaimana dimaksud pada ayat (2) huruf a dijabat oleh Kepala Dinas.
(4) Anggota tim sebagaimana dimaksud pada ayat (2) huruf b terdiri dari seluruh Pimpinan Perangkat Daerah lainnya pada Pemerintah Daerah.

Pasal 7

(1) Ketua Tim sebagaimana dimaksud dalam Pasal 6 ayat (2) huruf a mempunyai tugas memastikan pelaksanaan Manajemen Keamanan Informasi SPBE di lingkungan Pemerintah Daerah yang meliputi:
    a. menetapkan standar operasional prosedur pengendalian Keamanan Informasi Pemerintah Daerah;
    b. memastikan penerapan standar teknis dan prosedur pengendalian keamanan Informasi di lingkungan Pemerintah Daerah;
    c. merumuskan, mengoordinasikan, dan melaksanakan program kerja dan anggaran Keamanan SPBE;
    d. memutuskan dan merancang langkah kelangsungan layanan TIK dalam bentuk dokumen keberlangsungan bisnis dan perencanaan pengelolaan bencana;

e. melaporkan pelaksanaan Manajemen Keamanan Informasi dan Penerapan Standar Teknis dan Prosedur pengendalian Keamanan Informasi pada koordinator SPBE; dan
f. mengevaluasi penerapan prosedur pengendalian keamanan Informasi SPBE di lingkungan Provinsi Sulawesi Tengah.

(2) Anggota tim sebagaimana dimaksud dalam Pasal 6 ayat (2) huruf b mempunyai tugas:
a. mengoordinasikan dan/atau memastikan dan prosedur pengendalian keamanan Daerah masing-masing;
b. melaksanakan dan mengelola langkah kelangsungan layanan TIK yang berpedoman pada dokumen *business continuity* dan perencanaan pengelolaan bencana;
c. berkoordinasi dengan ketua tim terkait standar teknis dan prosedur pengendalian keamanan Informasi dan standar teknis dan prosedur Keamanan SPBE; dan
d. memastikan penerapan keamanan Aplikasi SPBE dan Infrastruktur SPBE sesuai dengan standar teknis dan prosedur Keamanan SPBE yang telah ditetapkan sesuai dengan peraturan perundang-undangan.

BAB IV
PERENCANAAN

Pasal 8

(1) Perencanaan sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf c ditetapkan oleh pelaksana teknis Keamanan SPBE.
(2) Perencanaan sebagaimana dimaksud pada ayat (1) dilakukan dengan merumuskan:
a. program kerja Keamanan SPBE; dan
b. target realisasi program kerja Keamanan SPBE.

Pasal 9

(1) Program kerja Keamanan SPBE sebagaimana dimaksud dalam Pasal 8 ayat (2) huruf a minimal 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.
(2) Target realisasi program kerja Keamanan SPBE sebagaimana dimaksud dalam Pasal 8 ayat (2) huruf b ditetapkan berdasarkan ketentuan prioritas setiap tahunnya.

BAB V
DUKUNGAN PENGOPERASIAN

Pasal 10

(1) Dukungan pengoperasian sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf d dilakukan oleh koordinator SPBE.
(2) Koordinator SPBE memastikan pelaksanaan pengamanan Informasi diberikan alokasi sumber daya yang sesuai untuk mengelola dan menjamin kepatuhan program keamanan Informasi.
(3) Dukungan pengoperasian sebagaimana dimaksud pada ayat (1) dilakukan dengan meningkatkan kapasitas terhadap:
    a. sumber daya manusia Keamanan SPBE;
    b. teknologi keamanan SPBE; dan
    c. anggaran keamanan SPBE.

Pasal 11

(1) Sumber daya manusia Keamanan SPBE sebagaimana dimaksud dalam Pasal 10 ayat (3) huruf a harus memiliki kompetensi:
    a. keamanan infrastruktur teknologi, Informasi dan komunikasi; dan
    b. keamanan aplikasi.
(2) Untuk memenuhi kompetensi sebagaimana dimaksud pada ayat (1), minimal didukungan dengan kegiatan:
    a. pelatihan dan atau sertifikasi kompetensi keamanan infrastruktur teknologi, Informasi dan komunikasi dan keamanan aplikasi; dan
    b. bimbingan teknis mengenai standar Keamanan SPBE.
(3) Pemenuhan kompetensi sebagaimana dimaksud pada ayat (2) dilakukan agar sumber daya manusia Keamanan SPBE memiliki kompetensi dan keahlian yang memadai dalam pelaksanaan pengamanan Informasi
(4) Teknologi keamanan SPBE sebagaimana dimaksud dalam Pasal 10 ayat (3) huruf b harus tersedia sesuai kebutuhan dan tingkat urgensi dari setiap Perangkat Daerah.
(5) Anggaran Keamanan SPBE sebagaimana dimaksud dalam Pasal 10 ayat (3) huruf c disusun berdasarkan perencanaan yang telah ditetapkan sesuai dengan ketentuan peraturan perundang-undangan.

BAB VI
STANDAR DAN PROSEDUR PENGENDALIAN

Pasal 12

(1) Standar dan prosedur pengendalian Keamanan Informasi sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf e ditetapkan oleh ketua tim pelaksana teknis Keamanan SPBE.

(2) Standar dan prosedur pengendalian Keamanan SPBE sebagaimana dimaksud pada ayat (1) digunakan untuk mengimplementasikan SMKI di lingkungan Pemerintah Daerah dengan persyaratan aspek meliputi:
   a. keamanan Perangkat teknologi Informasi;
   b. keamanan jaringan;
   c. keamanan pusat data;
   d. keamanan Perangkat *end point*;
   e. keamanan *remote working*;
   f. keamanan penyimpanan Elektronik;
   g. pengelolaan akses kontrol;
   h. pengendalian keamanan dari ancaman virus dan *malware;*
   i. persyaratan keamanan terkait pembangunan dan pengembangan Aplikasi SPBE;
   j. pengelolaan Aset;
   k. keamanan migrasi data;
   l. konfigurasi Perangkat IT *Security*;
   m. perlindungan data pribadi;
   n. Penerapan kriptografi;
   o. keamanan fisik dan lingkungan;
   p. keamanan operasional;
   q. keamanan komunikasi;
   r. keamanan dalam proses akuisisi, pengembangan dan pemeliharaan Sistem Informasi;
   s. pengendalian keamanan Informasi terhadap pihak ketiga;
   t. penanganan insiden keamanan Informasi;
   u. kebijakan terhadap pihak ketiga;
   v. kelangsungan bisnis atau layanan TIK;
   w. perencanaan pemulihan bencana terhadap layanan TIK;
   x. audit internal Keamanan SPBE;
   y. aspek prosedur pengendalian keamanan Informasi SPBE lainnya; dan/atau
   z. kepatuhan Keamanan SPBE.

(3) Standar dan prosedur pengendalian keamanan SPBE sebagaimana dimaksud pada ayat (2) selanjutnya ditetapkan dalam bentuk surat edaran atau kebijakan teknis lainnya.

Pasal 13

(1) Setiap Perangkat Daerah harus melaksanakan ketentuan penetapan standar dan prosedur pengendalian Keamanan Informasi SPBE sebagaimana dimaksud dalam Pasal 12 ayat (2).

(2) Setiap Perangkat Daerah bertanggung jawab dalam memastikan kegiatan operasional teknologi Informasi yang stabil dan aman dengan berpedoman pada prosedur pengendalian Keamanan Informasi SPBE.

BAB VII
MANAJEMEN RISIKO

Pasal 14

(1) Manajemen risiko sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf f dilakukan oleh setiap Perangkat Daerah untuk menjamin keberlangsungan SPBE dengan meminimalkan dampak risiko dalam SPBE.
(2) Setiap Perangkat Daerah harus menerapkan prosedur pelaksanaan manajemen risiko meliputi:
    a. komunikasi dan konsultasi;
    b. Penetapan konteks risiko SPBE:
        1. inventarisasi Informasi umum;
        2. identifikasi sasaran SPBE;
        3. penentuan struktur pelaksana Manajemen Risiko SPBE;
        4. identifikasi pemangku kepentingan;
        5. identifikasi peraturan perundang-undangan;
        6. penetapan kategori risiko SPBE;
        7. penetapan area dampak risiko SPBE;
        8. penetapan kriteria risiko SPBE;
        9. matrik analisis risiko SPBE dan level risiko SPBE; dan
        10. selera risiko SPBE;
    c. penilaian risiko SPBE:
        1. identifikasi risiko SPBE;
        2. analisis risiko SPBE; dan
        3. evaluasi risiko SPBE;
    d. penanganan risiko SPBE:
        1. prioritas risiko;
        2. rencana penanganan risiko SPBE; dan
        3. risiko residual;
    e. pemantauan dan reviu;
    f. pencatatan dan pelaporan;
    g. dokumen manajemen risiko SPBE;
        1. pakta intergritas manajemen risiko SPBE
        2. dokumen proses risiko SPBE; dan
        3. dokumen proses pengendalian risiko SPBE.

(3) Perangkat Daerah dalam menerapkan prosedur manajemen risiko di lingkungan kerjanya masing-masing dapat berkoordinasi dengan pelaksana teknis Keamanan Informasi.

BAB VIII
PENGELOLAAN PIHAK KETIGA

Pasal 15

(1) Pengelolaan pihak ketiga sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf g dilakukan oleh setiap Perangkat Daerah.
(2) Perangkat Daerah harus memastikan seluruh pembangunan atau pengembangan Aplikasi SPBE dan Infrastruktur SPBE yang dilakukan oleh pihak ketiga memenuhi standar teknis dan prosedur Keamanan SPBE yang telah ditetapkan.
(3) Perangkat daerah harus memastikan pihak ketiga memberikan akses sepenuhnya terkait pekerjaan pembangunan atau pengembangan Aplikasi SPBE dan Infrastruktur SPBE beserta kode sumbernya.
(4) Perangkat Daerah harus menetapkan proses, prosedur atau rencana terdokumentasi untuk memantau layanan dan aspek keamanan Informasi dalam hubungan kerjasama dengan pihak ketiga.
(5) Perangkat Daerah harus membuat laporan secara berkala tentang pencapaian Sasaran Tingkat Layanan dan aspek keamanan yang disyaratkan dalam perjanjian kontrak dengan pihak ketiga.
(6) Perangkat daerah dalam melaksanakan pengelolaan pihak ketiga di lingkungan kerjanya masing-masing dapat berkoordinasi kepada pelaksana teknik Keamanan Informasi.

BAB IX
EVALUASI KINERJA

Pasal 16

(1) Evaluasi kinerja sebagaimana dimaksud dalam Pasal 2 ayat (2) huruf h dilakukan oleh koordinator SPBE.
(2) Evaluasi kinerja sebagaimana dimaksud pada ayat (1) dilakukan terhadap pelaksanaan Keamanan SPBE.
(3) Evaluasi kinerja sebagaimana dimaksud pada ayat (2) dilaksanakan dengan:
    a. menganalisis efektifitas pelaksanaa keamanan SPBE; dan
    b. mendukung dan merealisasikan program audit Keamanan SPBE.

(4) Evaluasi kinerja sebagaimana dimaksud pada ayat (1) dilaksanakan paling sedikit 1 (satu) kali dalam 1 (satu) tahun.

BAB X
PERBAIKAN BERKELANJUTAN

Pasal 17

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

BAB XI
KETENTUAN PENUTUP

Pasal 18

Peraturan Gubernur ini mulai berlaku pada tanggal diundangkan.

Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Gubemur ini dengan penempatannya dalam Berita Daerah Provinsi Sulawesi Tengah.

Ditetapkan di Palu
pada tanggal 13 September 2023
GUBERNUR SULAWESI TENGAH,

ttd

RUSDI MASTURA

Diundangkan di Palu
pada tanggal 13 September 2023
SEKRETARIS DAERAH PROVINSI
SULAWESI TENGAH,

ttd

NOVALINA

BERITA DAERAH PROVINSI SULAWESI TENGAH TAHUN 2023 NOMOR 889

Salinan sesuai dengan aslinya
KEPALA BIRO HUKUM,

ADIMAN, SH.,M.SI
Pembina Tingkat I, IV/b
Nip. 19740610 200003 1 007