BERITA DAERAH PROVINSI NUSA TENGGARA BARAT
NOMOR 12 TAHUN 2025

PERATURAN GUBERNUR NUSA TENGGARA BARAT

NOMOR 11 TAHUN 2025

TENTANG

MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

DENGAN RAHMAT TUHAN YANG MAHA ESA

GUBERNUR NUSA TENGGARA BARAT,

Menimbang :

a. bahwa untuk untuk memastikan kerahasiaan, keutuhan, ketersediaan, dan keamanan Informasi Sistem Pemerintahan Berbasis Elektronik, perlu dilakukan penataan manajemen keamanan informasi yang baik dan terintegrasi;

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 Manajemen 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 untuk memberikan arah, landasan, dan kepastian hukum dalam melindungi data dan informasi elektronik, aplikasi dan infrastruktur sistem pemerintahan berbasis elektronik dilingkungan Pemerintah Provinsi Nusa Tenggara Barat dari segala jenis gangguan sebagai akibat informasi elektronik dan transaksi elektronik, perlu pengaturan mengenai manajemen keamanan informasi sistem pemerintahan berbasis elektronik;

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 Repubik Indonesia Tahun 1945;

2. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843) sebagaimana telah beberapa kali diubah terakhir dengan 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);
3. 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);
4. Undang-Undang Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-Undangan (Lembaran Negara Republik Indonesia Tahun 2011 Nomor 82, Tambahan Lembaran Negara Republik Indonesia Nomor 5234) sebagaimana telah beberapa kali diubah terakhir dengan Undang Nomor 13 Tahun 2022 tentang Perubahan Kedua atas Undang-Undang Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-Undangan (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 143, Tambahan Lembaran Negara Republik Indonesia Nomor 6801);
5. 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 beberapa kali diubah terakhir dengan Undang-Undang Nomor 6 Tahun 2023 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 2 Tahun 2022 tentang Cipta Kerja menjadi Undang-Undang (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 41, Tambahan Lembaran Negara Republik Indonesia Nomor 6856);
6. Undang-Undang Nomor 20 Tahun 2022 tentang Provinsi Nusa Tenggara Barat (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 163, Tambahan Lembaran Negara Republik Indonesia Nomor 6809);
7. 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);
8. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
9. Peraturan Presiden Nomor 132 Tahun 2022 tentang Arsitektur Sistem Pemerintahan Berbasis Elektronik Nasional (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 233);

10. Peraturan Presiden Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 129);
11. Peraturan Menteri Dalam Negeri Nomor 80 Tahun 2015 tentang Pembentukan Produk Hukum Daerah (Berita Negara Republik Indonesia Tahun 2015 Nomor 2036) sebagaimana telah diubah dengan Peraturan Menteri Dalam Negeri Nomor 120 Tahun 2018 tentang Perubahan atas Peraturan Menteri Dalam Negeri Nomor 80 Tahun 2015 Tentang Pembentukan Produk Hukum Daerah (Berita Negara Republik Indonesia Tahun 2019 Nomor 157);
12. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 5 Tahun 2020 tentang Pedoman Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2020 Nomor 261);
13. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 59 Tahun 2020 tentang Pemantauan dan Evaluasi Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2020 Nomor 994);
14. Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi (Berita Negara Republik Indonesia Tahun 2016 Nomor 551);
15. Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian untuk Pengamanan Informasi di Pemerintah Daerah (Berita Negara Republik Indonesia Tahun 2019 Nomor 1054);
16. Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2021 Nomor 541);
17. Peraturan Badan Siber dan Sandi Negara Nomor 1 Tahun 2024 tentang Pengelolaan Insiden Siber (Berita Negara Republik Indonesia Tahun 2024 Nomor 43);
18. Peraturan Daerah Nomor 4 Tahun 2014 tentang Penyelenggaraan Komunikasi dan Informatika (Lembaran Daerah Provinsi Nusa Tenggara Barat Tahun 2014 Nomor 4) sebagaimana telah diubah dengan Peraturan Daerah Nomor 4 Tahun 2021 tentang Perubahan atas Peraturan Daerah Nomor 4 Tahun 2014 tentang Penyelenggaraan Komunikasi dan Informatika (Lembaran Daerah Provinsi Nusa Tenggara Barat Tahun 2021 Nomor 4, Tambahan Lembaran Daerah Provinsi Nusa Tenggara Barat Nomor 173);

19. Peraturan Daerah Nomor 3 Tahun 2018 tentang Tata Kelola Pemerintahan Berbasis Sistem Elektronik (Lembaran Daerah Provinsi Nusa Tenggara Barat Tahun 2018 Nomor 3);
20. Peraturan Gubernur Nomor 31 Tahun 2024 tentang Penyelenggaran Sistem Pemerintahan Berbasis Elektronik di Lingkungan Pemerintah Daerah Provinsi Nusa Tenggara Barat (Berita Daerah Provinsi Nusa Tenggara Barat Tahun 2024 Nomor 31);

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. Daerah adalah Provinsi Nusa Tenggara Barat.
2. Pemerintah Daerah adalah Gubernur sebagai unsur penyelenggara Pemerintahan Daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan daerah otonom.
3. Gubernur adalah Gubernur Nusa Tenggara Barat.
4. Sekretaris Daerah adalah Sekretaris Daerah Provinsi Nusa Tenggara Barat.
5. Perangkat Daerah adalah unsur pembantu Gubernur dan Dewan Perwakilan Rakyat Daerah dalam Penyelenggaraan Urusan Pemerintahan yang menjadi kewenangan Daerah.
6. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada pengguna SPBE.
7. Teknologi Informasi dan Komunikasi yang selanjutnya disingkat TIK adalah segala kegiatan yang terkait dengan pemrosesan, manipulasi, pengelolaan, dan pemindahan informasi antar media.
8. 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 (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*) dari informasi.
9. Manajemen Keamanan Informasi adalah serangkaian proses yang meliputi penetapan ruang lingkup, penetapan penanggung jawab, perencanaan, dukungan pengoperasian, evaluasi kinerja, dan perbaikan berkelanjutan terhadap keamanan informasi dalam SPBE.

10. Keamanan SPBE adalah pengendalian keamanan yang terpadu dalam SPBE.
11. Insiden Keamanan Informasi adalah serangkaian prosedur dan langkah yang diambil oleh suatu organisasi untuk mengidentifikasi, menganalisis, dan menangani insiden keamanan siber.
12. Manajemen Keamanan SPBE adalah serangkaian proses untuk mencapai penerapan keamanan SPBE yang efektif, efisien, dan berkesinambungan, serta mendukung layanan SPBE yang berkualitas.
13. Aplikasi SPBE adalah satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas atau fungsi Layanan SPBE.
14. 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.

Pasal 2

(1) Peraturan Gubernur ini dimaksudkan sebagai pedoman kebijakan internal manajemen keamanan informasi SPBE.

(2) Peraturan Gubernur ini bertujuan untuk:
   a. menguatkan kebijakan internal manajemen keamanan informasi SPBE;
   b. memberikan arah, landasan, dan kepastian hukum dalam melindungi data dan informasi elektronik, aplikasi dan infrastruktur Sistem Pemerintahan Berbasis Elektronik; dan
   c. memastikan kerahasiaan, keutuhan, ketersediaan, dan keamanan Informasi Sistem Pemerintahan Berbasis Elektronik.

Pasal 3

Ruang lingkup dalam Peraturan Gubernur ini meliputi:
a. kebijakan internal manajemen keamanan informasi SPBE;
b. pengendalian teknis keamanan;
c. penghargaan; dan
d. pembiayaan

BAB II
KEBIJAKAN INTERNAL MANAJEMEN KEAMANAN INFORMASI SPBE

Bagian Kesatu
Umum

Pasal 4

Kebijakan internal manajemen keamanan informasi SPBE meliputi:
a. penetapan ruang lingkup;

b. penetapan penanggung jawab;
c. perencanaan;
d. dukungan pengoperasian;
e. evaluasi kinerja; dan
f. perbaikan berkelanjutan terhadap keamanan informasi.

Bagian Kedua
Penetapan Ruang Lingkup

Pasal 5

(1) Penetapan ruang lingkup manajemen keamanan informasi SPBE sebagaimana dimaksud dalam Pasal 4 huruf a meliputi:
   a. data dan informasi SPBE;
   b. Aplikasi SPBE; dan
   c. Infrastruktur SPBE.

(2) Ruang lingkup sebagaimana dimaksud pada ayat (1) merupakan aset Daerah yang harus diamankan dalam SPBE.

Bagian Ketiga
Penetapan Penanggung Jawab

Pasal 6

(1) Gubernur menetapkan penanggung jawab manajemen keamanan informasi SPBE sebagaimana dimaksud dalam Pasal 4 huruf b.

(2) Penanggung jawab manajemen keamanan informasi SPBE sebagaimana dimaksud pada ayat (1), dijabat oleh Sekretaris Daerah.

(3) Selain sebagai penanggung jawab sebagaimana dimaksud pada ayat (2), Sekretaris Daerah mempunyai tugas sebagai koordinator SPBE sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 7

(1) Dalam melaksanakan tugas sebagai penanggung jawab manajemen keamanan informasi SPBE dan koordinator SPBE sebagaimana dimaksud dalam Pasal 6 ayat (3), Sekretaris Daerah menetapkan pelaksana teknis Keamanan SPBE.

(2) Pelaksana teknis Keamanan SPBE sebagai dimaksud pada ayat (1) terdiri atas:
   a. ketua tim; dan
   b. anggota tim.

(3) Ketua Tim sebagaimana dimaksud pada ayat (2) huruf a dapat dijabat oleh pimpinan Perangkat Daerah yang membidangi urusan komunikasi dan informatika.

(4) Anggota Tim sebagaimana dimaksud pada ayat (2) huruf b, dari unsur pimpinan Perangkat Daerah yang memiliki, membawahi, membangun, memelihara, dan/atau mengembangkan Aplikasi SPBE dan/atau Infrastruktur SPBE di lingkungan Pemerintah Provinsi.

Pasal 8

(1) Ketua tim sebagaimana dimaksud dalam Pasal 7 ayat (2) huruf a mempunyai tugas:
   a. menetapkan prosedur pengendalian keamanan informasi SPBE Pemerintah Provinsi Nusa Tenggara Barat;
   b. mengevaluasi penerapan prosedur pengendalian keamanan informasi SPBE di lingkungan Pemerintah Provinsi Nusa Tenggara Barat;
   c. memastikan penerapan keamanan Aplikasi SPBE dan Infrastruktur SPBE sesuai dengan standar teknis dan prosedur Keamanan SPBE yang telah ditetapkan sesuai ketentuan peraturan perundang-undangan;
   d. merumuskan, mengoordinasikan dan melaksanakan program kerja dan anggaran Keamanan SPBE;
   e. mengoordinasikan, memantau dan menerima laporan pengelolaan insiden keamanan informasi;
   f. mendokumentasikan proses pengelolaan insiden keamanan informasi;
   g. memutuskan dan merancang langkah kelangsungan layanan TIK dalam bentuk dokumen *business continuity* dan *disaster recoveryplans*; dan
   h. melaporkan pelaksanaan manajemen keamanan informasi SPBE pada koordinator SPBE.
(2) Anggota Tim sebagaimana dimaksud dalam Pasal 7 ayat (2) huruf b mempunyai tugas:
   a. mengoordinasikan dan/atau memastikan penerapan prosedur pengendalian keamanan informasi SPBE pada Perangkat Daerah masing-masing;
   b. memastikan penerapan keamanan Aplikasi SPBE dan Infrastruktur SPBE sesuai dengan standar teknis dan prosedur Keamanan SPBE yang telah ditetapkan sesuai dengan peraturan perundang-undangan;
   c. mengoordinasikan, memantau dan mengelola insiden keamanan informasi di Perangkat Daerah masing-masing;
   d. mengirim laporan pengelolaan insiden keamanan informasi kepada Ketua Tim;
   e. mendokumentasikan proses pengelolaan insiden keamanan informasi di Perangkat Daerah masing-masing;
   f. melaksanakan dan mengelola langkah kelangsungan layanan TIK yang berpedoman pada dokumen *business continuity* dan *disaster recovery plans*; dan
   g. berkoordinasi dengan ketua tim terkait penerapan keamanan Aplikasi SPBE dan Infrastruktur SPBE.

Bagian Keempat
Perencanaan

Pasal 9

(1) Perencanaan sebagaimana dimaksud dalam Pasal 4 huruf c dilakukan oleh pelaksana teknis Keamanan SPBE.

(2) Perancanaan sebagaimana dimaksud pada ayat (1) dilakukan dengan merumuskan:
   a. program kerja Keamanan SPBE; dan
   b. target realisasi program kerja Keamanan SPBE.

Pasal 10

(1) Program kerja Keamanan SPBE sebagaimana dimaksud dalam Pasal 9 ayat (2) huruf a paling sedikit meliputi:
   a. edukasi kesadaran Keamanan SPBE;
   b. penilaian kerentanan Keamanan SPBE;
   c. peningkatan Keamanan SPBE;
   d. penanganan insiden Keamanan SPBE; dan
   e. audit Keamanan SPBE.

(2) Target realisasi program kerja Keamanan SPBE sebagaimana dimaksud dalam Pasal 9 ayat (2) huruf b ditetapkan berdasarkan ketentuan prioritas setiap tahunnya.

Bagian Kelima
Dukungan Pengoperasian

Pasal 11

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

(2) Dukungan pengoperasian sebagaimana dimaksud pada ayat (1) dilakukan dengan meningkatkan kapasitas terhadap:
   a. sumber daya manusia Keamanan SPBE;
   b. teknologi keamanan SPBE; dan
   c. anggaran keamanan SPBE.

Pasal 12

(1) Sumber daya manusia Keamanan SPBE sebagaimana dimaksud dalam Pasal 11 ayat (2) huruf a dengan ketentuan harus memiliki kompetensi:
   a. Keamanan Infrastruktur TIK; dan
   b. Keamanan aplikasi.

(2) Untuk memenuhi kompetensi sebagaimana dimaksud pada ayat (1), paling sedikit harus adanya dukungan kegiatan:
   a. pelatihan dan/atau sertifikasi kompetensi keamanan aplikasi dan TIK; dan/atau
   b. bimbingan teknis mengenai standar teknis dan prosedur 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 Keamanan SPBE.

(4) Teknologi keamanan informasi sebagaimana dimaksud dalam Pasal 11 ayat (2) huruf b harus tersedia sesuai kebutuhan dan tingkat urgensi dari setiap Perangkat Daerah.

(5) Anggaran Keamanan SPBE sebagaimana dimaksud dalam Pasal 11 ayat (2) huruf c disusun berdasarkan perencanaan yang telah ditetapkan sesuai dengan ketentuan peraturan perundang-undangan.

Bagian Keenam
Evaluasi Kinerja

Pasal 13

(1) Evaluasi kinerja sebagaimana dimaksud dalam Pasal 4 huruf e dilakukan oleh koordinator SPBE.

(2) Evaluasi kinerja sebagaimana dimaksud pada ayat (1) dilakukan terhadap pelaksanaan manajemen keamanan informasi SPBE di lingkungan Pemerintah Daerah.

(3) Evaluasi kinerja sebagaimana dimaksud pada ayat (2) dilaksanakan dengan:
   a. menganalisis efektifitas pelaksanaan Keamanan SPBE; atau
   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.

(5) Laporan hasil evaluasi kinerja sebagaimana yang dimaksud pada ayat (1) dilaporkan kepada Gubernur, BSSN dan instansi terkait.

Bagian Ketujuh
Perbaikan Berkelanjutan Terhadap
Keamanan Informasi

Pasal 14

(1) Perbaikan berkelanjutan sebagaimana dimaksud dalam Pasal 4 huruf f dilakukan oleh pelaksana teknis Keamanan SPBE.

(2) Perbaikan berkelanjutan sebagaimana dimaksud pada ayat (1) merupakan tindak lanjut dari hasil evaluasi kinerja.

(3) Perbaikan berkelanjutan sebagaimana dimaksud pada ayat (1) dilakukan dengan:
   a. mengatasi permasalahan dalam pelaksanaan Keamanan SPBE;
   b. memperbaiki pelaksanaan Keamanan SPBE secara periodik; dan
   c. tindak lanjut hasil audit Keamanan SPBE.

BAB III
PENGENDALIAN TEKNIS KEAMANAN

Pasal 15

(1) Pengendalian teknis keamanan dapat diterapkan untuk mendukung kebijakan internal manajemen keamanan informasi SPBE.

(2) Pengendalian teknis keamanan sebagaimana dimaksud pada ayat (1) meliputi:
   a. manajemen risiko;
   b. penetapan prosedur pengendalian keamanan informasi SPBE; dan
   c. pengelolaan pihak ketiga.

Pasal 16

(1) Manajemen risiko sebagaimana dimaksud dalam Pasal 15 ayat (2) huruf a dilakukan oleh setiap Perangkat Daerah.

(2) Setiap Perangkat Daerah menyusun daftar risiko (*riskregister*) dengan ketentuan susbtansi, paling sedikit memuat:
   a. inventarisasi aset SPBE;
   b. identifikasi ancaman dan kerentanan keamanan terhadap aset SPBE;
   c. penilaian risiko keamanan terhadap aset SPBE;
   d. penentuan prioritas risiko;
   e. analisa dampak jika terjadi risiko;
   f. analisa kontrol keamanan yang bisa diterapkan; dan/atau
   g. rekomendasi kontrol keamanan.

(3) Prosedur pelaksanaan manajemen risiko sebagaimana dimaksud pada ayat (1), dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 17

(1) Penetapan prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud dalam Pasal 15 ayat (2) huruf b ditetapkan oleh ketua tim pelaksana teknis Keamanan SPBE.

(2) Penetapan prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud pada ayat (1) digunakan untuk mengimplementasikan manajemen keamanan;

(3) Pengendalian keamanan informasi SPBE di lingkungan Pemerintah Provinsi Nusa Tenggara Barat dengan cakupan aspek dapat meliputi:
   a. keamanan perangkat teknologi informasi komunikasi;
   b. keamanan jaringan;
   c. keamanan pusat data;
   d. keamanan perangkat *endpoint;*
   e. keamanan *remote working;*

f. keamanan penyimpanan elektronik;
g. pengelolaan akses kontrol;
h. pengendalian keamanan dari ancaman *virus* dan *malware;*
i. persayaratan keamanan terkait pembangunan dan pengembangan aplikasi SPBE;
j. pengelolaan aset;
k. keamanan migrasi data;
l. konfigurasi perangkat IT *Security*;
m. perlindungan data pribadi;
n. keamanan komunikasi;
o. keamanan dalam proses akuisisi, pengembangan dan pemeliharaan sistem informasi;
p. pengendalian keamanan informasi terhadap pihak ketiga;
q. penerapan kriptografi;
r. penanganan insiden keamanan informasi;
s. kelangsungan bisnis atau layanan TIK (*business continuity*);
t. perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plans*);
u. audit internal keamanan SPBE; dan/atau
v. aspek prosedur pengendalian keamanan informasi SPBE lainnya.

(4) Penetapan prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud pada ayat (2) ditetapkan oleh koordinator SPBE.

Pasal 18

(1) Setiap Perangkat Daerah harus melaksanakan ketentuan penetapan prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud dalam Pasal 17 ayat (3).

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

Pasal 19

(1) Pengelolaan pihak ketiga sebagaimana dimaksud dalam Pasal 15 ayat (2) huruf c dilakukan oleh setiap Perangkat Daerah.

(2) Perangkat Daerah sebagaimana dimaksud pada ayat (1) harus memastikan seluruh pembangunan atau pengembangan Aplikasi SPBE dan Infrastruktur SPBE yang dilakukan oleh pihak ketiga:

a. memenuhi standar teknis dan prosedur Keamanan SPBE yang telah ditetapkan;
b. memberikan akses sepenuhnya terkait pekerjaan pembangunan atau pengembangan Aplikasi SPBE dan Infrastruktur SPBE beserta kode sumbernya.

(3) Perangkat Daerah menetapkan proses, prosedur atau rencana terdokumentasi untuk memantau layanan dan aspek keamanan informasi dalam hubungan kerjasama dengan pihak ketiga.

(4) Perangkat Daerah membuat laporan secara berkala tentang pencapaian sasaran tingkat layanan (SLA) dan aspek keamanan yang disyaratkan dalam perjanjian kontrak dengan pihak ketiga.

BAB IV
PENGHARGAAN

Pasal 20

(1) Gubernur memberikan penghargaan kepada Perangkat Daerah dan Pemerintah Kabupaten/Kota yang melaksanakan manajemen kemanan informasi SPBE dengan baik.

(2) Penghargaan sebagaimana dimaksud pada ayat (1) didasarkan pada kriteria penilaian dalam bentuk pemeringkatan yang merupakan hasil dari:
   a. monitoring dan evaluasi; dan
   b. penilaian Ahli.

(3) Pemeringkatan sebagaimana dimaksud pada ayat (2), diberikan kategori predikat:
   a. Sangat Baik;
   b. Baik;
   c. Cukup; dan
   d. Kurang Baik.

(4) Kriteria penilaian dan bentuk penghargaan sebagaimana dimaksud pada ayat (2), disusun dan ditetapkan oleh Perangkat Daerah yang membidangi urusan Komunikasi Informatika dan Statistik.

BAB V
PENDANAAN

Pasal 21

Pembiayaan penyelenggaraan Manajemen Kemanan Informasi SPBE bersumber dari:

a. Anggaran Pendapatan dan Belanja Daerah Provinsi; dan

b. sumber pendapatan lainnya yang sah dan tidak mengikat sesuai dengan ketentuan peraturan perundang-undangan.

BAB VI
KETENTUAN PENUTUP

Pasal 22

Peraturan Gubernur ini mulai berlaku pada tanggal diundangkan. Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Gubernur ini dengan penempatannya dalam Berita Daerah Provinsi Nusa Tenggara Barat.

Ditetapkan di Mataram
pada tanggal 26 Juni 2025

GUBERNUR NUSA TENGGARA BARAT,

ttd

LALU MUHAMAD IQBAL

Diundangkan di Mataram
pada tanggal 26 Juni 2025

Plh. SEKRETARIS DAERAH
PROVINSI NUSA TENGGARA BARAT,

ttd

LALU MOH. FAOZAL

BERITA DAERAH PROVINSI NUSA TENGGARA BARAT TAHUN 2025 NOMOR 12

Salinan sesuai dengan aslinya
KEPALA BIRO HUKUM,

LALU RUDY GUNAWAN
NIP. 19700527 199603 1 002