GUBERNUR MALUKU

PERATURAN GUBERNUR MALUKU
NOMOR 20 TAHUN 2023

TENTANG

MANAJEMEN KEAMANAN INFORMASI
SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

DENGAN RAHMAT TUHAN YANG MAHA ESA

GUBERNUR MALUKU,

Menimbang :

a. bahwa dalam rangka mewujudkan penyelenggaraan pemerintahan secara elektronik yang aman di lingkungan Pemerintah Provinsi Maluku perlu melakukan pengelolaan keamanan informasi;

b. bahwa berdasarkan ketentuan dalam Pasal 41 ayat (1) Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik jo Pasal 2 Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manejemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik, 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 di lingkungan Pemerintah Provinsi Maluku 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 Republik 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 diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251, Tambahan Lembaran Negara Republik Indonesia Nomor 5952);
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 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 Peraturan Pemerintah Pengganti Undang-Undang Nomor 2 Tahun 2022 tentang Cipta Kerja (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 238, Tambahan Lembaran Negara Republik Indonesia Nomor 6841);
5. Undang-Undang Nomor 13 Tahun 2023 tentang Provinsi Maluku (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 60, Tambahan Lembaran Negara Republik Indonesia Nomor 6869);
6. 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);
7. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
8. 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);
9. 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);

10. Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi SPBE dan Standar Teknis dan Prosedur Keamanan SPBE (Berita Negara Republik Indonesia Tahun 2021 Nomor 541);

M E M U T U S K A N :

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 Maluku.
2. Pemerintah Daerah adalah Gubernur sebagai unsur penyelenggara Pemerintahan Daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan daerah otonom.
3. Gubernur adalah Gubernur Maluku.
4. Perangkat Daerah adalah unsur pembantu Gubernur dan Dewan Perwakilan Rakyat Daerah dalam penyelenggaraan urusan pemerintahan yang menjadi kewenangan Daerah.
5. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada pengguna SPBE.
6. Teknologi Informasi dan Komunikasi yang selanjutnya disingkat TIK adalah segala kegiatan yang terkait dengan pemprosesan, manipulasi, pengelolaan, dan pemindahan informasi antar media.
7. Keamanan Informasi adalah suatu kondisi untuk melindungi aset yang dimiliki organisasi dari berbagai ancaman pihak internal maupun eksternal untuk menjamin kelanjutan proses bisnis, mengurangi resiko bisnis, serta terjaganya aspek kerahasiaan, keutuhan dan ketersediaan dari informasi.
8. Keamanan SPBE mencakup penjaminan kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan *(nonrepudiation)* sumber daya terkait data dan informasi, Infrastruktur SPBE, dan Aplikasi SPBE.
9. Kerahasiaan adalah sesuai dengan konsep hukum tentang kerahasiaan *(confidentiality)* atas informasi dan komunikasi secara elektronik.

10. Keutuhan adalah sesuai dengan konsep hukum tentang keutuhan *(integrity)* atas Informasi Elektronik.
11. Ketersediaan adalah sesuai dengan konsep hukum tentang ketersediaan *(availability)* atas Informasi Elektronik.
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 *integrase*/penghubung, dan perangkat Elektronik lainnya.

Pasal 2

(1) Maksud pembentukan Peraturan Gubernur ini sebagai pedoman dalam melaksanakan serangkaian proses manajemen keamanan informasi SPBE pemerintahan di lingkungan Pemerintah Daerah.
(2) Pembentukan Peraturan Gubernur ini bertujuan sebagai pedoman pengelolaan Manajemen Keamanan Informasi SPBE secara terpadu untuk memastikan terjaganya kerahasiaan, keutuhan, keaslian dan ketersediaan.

Pasal 3

Ruang lingkup pengaturan dalam Peraturan Gubernur ini meliputi:

a. kebijakan internal manajemen keamanan informasi SPBE;dan
b. pengendalian teknis keamanan.

BAB II

KEBIJAKAN INTERNAL MANAJEMEN KEAMANAN INFORMASI SPBE

Bagian Kesatu

Umum

Pasal 4

Kebijakan Manajemen Keamanan Informasi SPBE sebagaimana dimaksud dalam Pasal 3 huruf a 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;
c. aset Infrastruktur SPBE;dan
d. kebijakan Keamanan Informasi SPBE yang telah dimiliki.
(2) Penetapan ruang lingkup sebagaimana dimaksud pada ayat (1) merupakan aset Pemerintah Daerah yang harus diamankan dalam SPBE.

Bagian Ketiga
Penetapan Penanggung jawab

Pasal 6

(1) Penetapan penanggung jawab sebagaimana dimaksud dalam Pasal 4 huruf b dilaksanakan oleh Gubernur.
(2) Penanggung jawab sebagaimana dimaksud pada ayat (1) dijabat oleh Sekretaris Daerah.
(3) Dalam melaksanakan tugas sebagai penanggung jawab keamanan SPBE, Sekretaris Daerah disebut sebagai koordinator SPBE.

Pasal 7

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

(2) Pelaksana teknis Keamanan SPBE sebagaimana dimaksud pada ayat (1) terdiri atas:
a. penjabat pimpinan tinggi pratama yang melaksanakan tugas dan fungsi dibidang keamanan teknologi, informasi dan komunikasi;dan
b. pejabat pimpinan tinggi atau pejabat administrator yang membawahi, membangun, memelihara dan/atau mengembangkan Aplikasi SPBE.

Pasal 8

(1) Pejabat pimpinan tinggi pratama dimaksud dalam pasal 7 ayat (2) huruf a bertugas memastikan pelaksanaan manajemen keamanan informasi SPBE di lingkungan Pemerintah Daerah yang meliputi:

a. memastikan penerapan standar teknis dan prosedur Keamanan SPBE;

b. merumuskan, mengkoordinasikan dan melaksanakan program kerja dan anggaran Keamanan SPBE;dan

c. melaporkan pelaksanaan manajemen Keamanan Informasi SPBE dan penerapan standar teknis dan prosedur keamanan SPBE kepada coordinator SPBE Pemerintah Daerah.

(2) Pejabat pimpinan tinggi atau pejabat administrator sebagaimana dimaksud dalam Pasal 7 ayat (2) huruf b bertugas:

a. menerapkan standar teknis dan prosedur keamanan aplikasi di unit kerja masing-masing;

b. memastikan seluruh pembangunan atau pengembangan Aplikasi dan Infrastruktur SPBE yang dilakukan oleh pihak ke tiga memenuhi standar teknis dan prosedur Keamanan SPBE yang telah ditetapkan;

c. memastikan keberlangsungan proses bisnis SPBE;dan

d. berkoordinasi dengan pejabat pimpinan tinggi pratama yang melaksanakan tugas dan fungsi dibidang keamanan teknologi, informasi dan komunikasi pada Instansi Pusat dan Pemerintah Daerah masing-masing terkait perumusan program kerja dan anggaran Keamanan SPBE.

Bagian Keempat

Perencanaan

Pasal 9

(1) Perencanaan sebagaimana dimaksud dalam Pasal 4 huruf c ditetapkan oleh tim pelaksanan teknis Kemanan SPBE.

(2) Perencanaan sebagaimana dimaksud pada ayat (1) dilakukan dengan merumuskan:

a. program kerja Kemanan 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 dimaskud pada ayat (1) dilakukan dengan meningkatkan kapasitas terhadap:
a. sumber daya manusia Keamanan SPBE;dan
b. anggaran keamanan SPBE.
(3) Koordinator SPBE melalui dukungan pengoperasian memastikan pelaksanaan manajemen keamanan informasi SPBE diberikan alokasi sumber daya yang sesuai dengan peraturan perundang-undangan.

Pasal 12

(1) Sumber daya manusia Keamanan SPBE sebagaimana dimaksud dalam Pasal 11 ayat (2) huruf a paling sedikit berjumlah 5 (lima) orang dengan ketentuan harus memiliki kompetensi:
a. keamanan 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 dimaskud pada ayat (2) dilakukan agar sumber daya manusia Keamanan SPBE memiliki kompetensi dan keahlian yang memadai dalam pelaksanaan Keamanan SPBE.
(4) Anggaran Keamanan SPBE sebagaimana dimaksud dalam Pasal 11 ayat (2) huruf b 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. mengidentifikasi area proses yang memiliki resiko 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; atau
    e. mendukung dan merealisasikan program audit Keamaman SPBE.
(4) Evaluasi kinerja sebagaimana dimaksud pada ayat (1) dilaksanakan paling sedikit 1 (satu) kali dalam 1 (satu) tahun.

Bagian Ketujuh
Perbaikan Berkelanjutan Terhadap Keamanan Informasi

Pasal 14

(1) Perbaikan berkelanjutan Terhadap Keamanan Informasi sebagaiman 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 sebagaiman 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
Bagian Kesatu
Umum
Pasal 15

Pengendalian teknis keamanan sebagaimana dimaksud dalam Pasal 3 huruf b meliputi:

a. manajemen risiko;
b. penetapan prpsedur pengendalian keamanan informasi SPBE;dan
c. pengelolaan pihak ketiga.

Bagian Kedua
Manejemen Resiko

Pasal 16

(1) Manajemen risiko sebagaimana dimaksud dalam Pasal 15 huruf a dilakukan oleh setiap Perangkat Daerah.
(2) Manajemen risiko sebagaimana dimaksud pada ayat (1) dilaksanakan dengan prosedur sebagai berikut:
    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
    g. rekomendasi kontrol keamanan.
(3) Prosedur pelaksanaan manajemen risiko sebagaimana dimaksud pada ayat (2) berpedoman pada ketentuan peraturan perundang-undangan.

Bagian Ketiga
Penetapan Prosedur Pengendalian Keamanan SPBE

Pasal 17

(1) Penetapan prosedur pengendalian keamanan informasi SPBE sebagaiman dimaksud pada Pasal 15 huruf b ditetapkan oleh ketua tim pelaksana teknis Keamanan SPBE.
(2) Penetapan prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud pada ayat (1) digunakan untuk mengimplentasikan manajemen keamanan informasi SPBE di lingkungan Pemerintah Daerah dengan cakupan aspek meliputi:
    a. keamanan perangkat teknologi informasi komunikasi;
    b. keamanan jaringan;
    c. keamanan pusat data;
    d. keamanan perangkat *end point*;
    e. keamanan *remote working;*
    f. keamanan penyimpanan elektronik;
    g. pengelolaan akses control;

h. pengendalian keamanan dari ancaman *virus* dan *malware*;
i. persyaratan keamanan terkait pembangunan dan pengembangan aplikasi SPBE;
j. pengelolaan akses;
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;*
t. perencanaan pemulihan bencana terhadap layanan TIK;
u. audit intenal keamanan SPBE; dan/atau
v. aspek prosedur pengendalian keamanan informasi SPBE lainnya.

(3) Penetapan prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud pada ayat (2) selanjutnya ditetapkan oleh Gubernur.

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.

Bagian Keempat
Pengelolaan Pihak Ketiga

Pasal 19

(1) Pengelolaan pihak ketiga sebagaimana dimaksud dalam Pasal 15 huruf c 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.

BAB IV
KETENTUAN PENUTUP

Pasal 20

Peraturan Gubernur ini mulai berlaku pada tanggal diundangkan.

Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Gubernur ini dengan penempatannya dalam Berita Daerah Provinsi Maluku.

Ditetapkan di Ambon
pada tanggal 14 Juli 2023

GUBERNUR MALUKU,

MURAD ISMAIL

Diundangkan di Ambon
pada tanggal 14 Juli 2023

SEKRETARIS DAERAH PROVINSI MALUKU,

SADALI IE

BERITA DAERAH PROVINSI MALUKU TAHUN 2023 NOMOR 306.