GUBERNUR ACEH

PERATURAN GUBERNUR ACEH
NOMOR 46 TAHUN 2023

TENTANG

MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

DENGAN RAHMAT ALLAH YANG MAHA KUASA

GUBERNUR ACEH,

Menimbang :

a. bahwa dalam rangka penyelenggaraan pemerintahan secara elektronik yang aman pada Pemerintah Aceh, perlu adanya pedoman manajemen keamanan informasi untuk memastikan kerahasiaan, keutuhan dan ketersediaan terhadap sistem pemerintahan berbasis elektronik dari berbagai ancaman keamanan informasi;

b. bahwa untuk memberikan arah, landasan, dan kepastian hukum dalam melindungi data dan informasi elektronik, aplikasi, infrastruktur dan keberlangsungan sistem pemerintahan berbasis elektronik pada Pemerintah Aceh dari segala jenis gangguan sebagai akibat informasi elektronik dan transaksi elektronik serta untuk meminimalkan dampak resiko keamanan informasi perlu pengaturan mengenai manajemen keamanan informasi sistem pemerintahan berbasis elektronik;

c. bahwa untuk melaksanakan ketentuan Pasal 41 ayat (1) dan Pasal 48 Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik, Pasal 38 Qanun Aceh Nomor 7 Tahun 2020 tentang Sistem Informasi Aceh Terpadu serta Pasal 22 dan Pasal 24 huruf b Peraturan Gubernur Aceh Nomor 61 Tahun 2022 tentang Sistem Pemerintahan Berbasis Elektronik, perlu menyusun kebijakan terkait manajemen keamanan informasi;

d. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b dan huruf c, perlu menetapkan Peraturan Gubernur Aceh tentang Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik;

Mengingat :

1. Pasal 18 ayat (6) Undang-Undang Dasar Negara Republik Indonesia;
2. Undang-Undang Nomor 24 Tahun 1956 tentang Pembentukan Daerah Otonom Propinsi Atjeh dan Perubahan Peraturan Pembentukan Propinsi Sumatera Utara (Lembaran Negara Republik Indonesia Tahun 1956 Nomor 64, Tambahan Lembaran Negara Republik Indonesia Nomor 1103) sebagaimana telah diubah dengan Undang-Undang Nomor 4 Tahun 1974 tentang Pembentukan Kabupaten Aceh Tenggara (Lembaran Negara Republik Indonesia Tahun 1974 Nomor 32, Tambahan Lembaran Negara Republik Indonesia Nomor 3034);
3. Undang-Undang Nomor 11 Tahun 2006 tentang Pemerintahan Aceh (Lembaran Negara Republik Indonesia Tahun 2006 Nomor 62, Tambahan Lembaran Negara Republik Indonesia Nomor 4633);

4. Undang- .../2

4. 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 terakhir dengan Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 1, Tambahan Lembaran Negara Republik Indonesia Nomor 6842);
5. 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);
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 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 6841);
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 (Berita Negara Republik Indonesia Tahun 2018 Nomor 182);
9. Peraturan Presiden Nomor 82 Tahun 2022 tentang Perlindungan Infrastruktur Informasi Vital (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 129);
10. 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);
11. 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);
12. 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);
13. 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);
14. Qanun Aceh Nomor 13 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Aceh (Lembaran Aceh Tahun 2016 Nomor 16, Tambahan Lembaran Aceh Nomor 87) sebagaimana telah diubah dengan Qanun Aceh Nomor 13 Tahun 2019 tentang Perubahan Atas Qanun Aceh Nomor 13 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Aceh (Lembaran Aceh Tahun 2019 Nomor 21);
15. Qanun Aceh Nomor 7 Tahun 2020 tentang Sistem Informasi Aceh Terpadu (Lembaran Aceh Tahun 2021 Nomor 6);
16. Peraturan Gubernur Aceh Nomor 85 Tahun 2019 tentang Penyelenggaraan Persandian untuk Pengamanan Informasi di Lingkungan Pemerintah Aceh (Berita Daerah Aceh Tahun 2019 Nomor 86);
17. Peraturan Gubernur Aceh Nomor 61 Tahun 2022 tentang Sistem Pemerintahan Berbasis Elektronik (Berita Daerah Aceh Tahun 2022 Nomor 61);

MEMUTUSKAN: .../3

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. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada pengguna SPBE.
2. 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.
3. Aceh adalah daerah Provinsi yang merupakan kesatuan masyarakat hukum yang bersifat istimewa dan diberi kewenangan khusus untuk mengatur dan mengurus sendiri urusan pemerintahan dan kepentingan masyarakat setempat sesuai dengan peraturan perundang-undangan dalam sistem dan prinsip Negara Kesatuan Republik Indonesia berdasarkan Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, yang dipimpin oleh Gubernur.
4. Pemerintah Aceh adalah unsur penyelenggara Pemerintahan Aceh yang terdiri atas Gubernur dan Perangkat Aceh.
5. Gubernur adalah Kepala Pemerintah Aceh.
6. Satuan Kerja Perangkat Aceh yang selanjutnya disingkat SKPA adalah organisasi perangkat daerah pada Pemerintah Aceh.
7. Aparatur Sipil Negara yang selanjutnya disingkat ASN adalah Pegawai Negeri Sipil dan pegawai pemerintah dengan perjanjian kerja yang diangkat oleh pejabat pembina kepegawaian dan diserahi tugas dalam suatu jabatan pemerintahan atau diserahi tugas negara lainnya dan digaji berdasarkan peraturan perundang-undangan.
8. Pejabat Daerah Lainnya adalah Anggota Dewan Perwakilan Rakyat Aceh, Wali Nanggroe Aceh, Majelis Permusyawaratan Ulama, Majelis Adat Aceh, Majelis Pendidikan Aceh, Badan Reintegrasi Aceh, Baitul Mal Aceh dan/atau pejabat pada lembaga keistimewaan Aceh lainnya.
9. Koordinator SPBE adalah Sekretaris Daerah Aceh.
10. Teknologi Informasi dan Komunikasi yang selanjutnya disingkat TIK adalah segala kegiatan yang terkait dengan pemrosesan, manipulasi, pengelolaan, dan pemindahan informasi antar media.
11. Keamanan SPBE adalah pengendalian keamanan yang terpadu dalam SPBE.
12. Kerahasiaan adalah sesuai dengan konsep hukum tentang kerahasiaan (*confidentiality*) atas informasi dan komunikasi secara Elektronik.
13. Keutuhan adalah sesuai dengan konsep hukum tentang keutuhan (*integrity*) atas Informasi Elektronik.
14. Ketersediaan adalah sesuai dengan konsep hukum tentang ketersediaan (*availability*) atas Informasi Elektronik.
15. Manajemen Keamanan SPBE adalah serangkaian proses untuk mencapai penerapan keamanan SPBE yang efektif, efisien, dan berkesinambungan serta mendukung layanan SPBE yang berkualitas.

16. Pengendalian .../4

16. Pengendalian teknis keamanan adalah mekanisme yang diterapkan untuk melindungi informasi dari dampak risiko yang mungkin terjadi pada perangkat lunak dan perangkat keras sistem elektronik.
17. Aplikasi SPBE adalah satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas atau fungsi Layanan SPBE.
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 *integrase*/penghubung dan perangkat Elektronik lainnya.

Pasal 2

(1) Peraturan Gubernur ini dimaksudkan sebagai kebijakan internal manajemen keamanan informasi SPBE pada Pemerintah Aceh.
(2) Ruang lingkup Peraturan Gubernur ini meliputi:
a. kebijakan internal manajemen Keamanan Informasi SPBE; dan
b. pengendalian teknis Keamanan Informasi.

BAB II

KEBIJAKAN INTERNAL MANAJEMEN KEAMANAN INFORMASI SPBE

Bagian Kesatu

Kebijakan Internal

Pasal 3

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 4

(1) Penetapan ruang lingkup manajemen Keamanan Informasi SPBE sebagaimana dimaksud dalam Pasal 3 huruf a 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 Aceh yang harus diamankan dalam SPBE.

Bagian Ketiga

Penetapan Penanggung Jawab

Pasal 5

(1) Penetapan penanggung jawab sebagaimana dimaksud dalam Pasal 3 huruf b dilaksanakan oleh Gubernur.
(2) Penanggung jawab sebagaimana dimaksud pada ayat (1) dijabat oleh Sekretaris Daerah.
(3) Sekretaris Daerah selain bertugas sebagai penanggung jawab sebagaimana dimaksud pada ayat (2) juga bertugas sebagai Koordinator SPBE sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 6 .../5

Pasal 6

(1) Dalam melaksanakan tugas sebagai penanggung jawab manajemen Keamanan Informasi SPBE, Koordinator SPBE sebagaimana dimaksud dalam Pasal 5 ayat (3) menetapkan pelaksana teknis Keamanan SPBE.

(2) Pelaksana teknis Keamanan SPBE sebagaimana dimaksud pada ayat (1) paling sedikit terdiri dari:
   a. Ketua tim;
   b. Sekretaris tim; dan
   c. Anggota tim.

(3) Ketua tim sebagaimana dimaksud pada ayat (2) huruf a dijabat oleh pimpinan SKPA yang membidangi urusan persandian dan Keamanan Informasi.

(4) Sekretaris tim sebagaimana dimaksud pada ayat (2) huruf b dijabat oleh kepala bagian yang membidangi persandian/Keamanan Informasi pada SKPA yang membidangi urusan persandian dan Keamanan Informasi.

(5) Anggota tim sebagaimana dimaksud pada ayat (2) huruf c terdiri dari seluruh pimpinan SKPA yang memiliki, membawahi, membangun, memelihara dan/atau mengembangkan data dan informasi SPBE, Aplikasi SPBE dan/atau Infrastruktur SPBE pada Pemerintah Aceh.

Pasal 7

(1) Ketua tim sebagaimana dimaksud dalam Pasal 6 ayat (2) huruf a bertugas memastikan pelaksanaan manajemen Keamanan Informasi SPBE yang meliputi:
   a. menetapkan prosedur pengendalian Keamanan Informasi SPBE;
   b. mengevaluasi penerapan prosedur pengendalian Keamanan Informasi SPBE;
   c. memastikan penerapan keamanan Aplikasi SPBE dan Infrastruktur SPBE sesuai dengan standar teknis dan prosedur Keamanan SPBE yang telah ditetapkan sesuai dengan ketentuan peraturan perundang-undangan;
   d. merumuskan, mengoordinasikan dan melaksanakan program kerja dan anggaran Keamanan SPBE;
   e. memutuskan dan merancang langkah kelangsungan layanan TIK dalam bentuk dokumen *business continuity* dan *disaster recovery plans*; dan
   f. melaporkan pelaksanaan manajemen Keamanan Informasi SPBE kepada Koordinator SPBE.

(2) Sekretaris tim sebagaimana dimaksud dalam Pasal 6 ayat (2) huruf b bertugas membantu ketua tim dalam memastikan pelaksanaan manajemen Keamanan Informasi SPBE.

(3) Anggota tim sebagaimana dimaksud dalam Pasal 6 ayat (2) huruf c bertugas:
   a. mengoordinasikan dan memastikan penerapan prosedur pengendalian Keamanan Informasi SPBE pada SKPA masing-masing;
   b. memastikan penerapan keamanan Aplikasi SPBE dan Infrastruktur SPBE sesuai dengan standar teknis dan prosedur Keamanan SPBE yang telah ditetapkan sesuai dengan ketentuan peraturan perundang-undangan;
   c. melaksanakan dan mengelola keberlangsungan layanan TIK yang berpedoman pada dokumen *business continuity* dan *disaster recovery plans*; dan
   d. berkoordinasi dengan ketua tim terkait penerapan keamanan data dan informasi SPBE, keamanan Aplikasi SPBE dan Infrastruktur SPBE.

Bagian .../6

Bagian Keempat
Perencanaan
Pasal 8

(1) Perencanaan sebagaimana dimaksud dalam Pasal 3 huruf c ditetapkan oleh ketua tim 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 paling sedikit memuat:
    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 pada Pasal 8 ayat (2) huruf b ditetapkan berdasarkan ketentuan prioritas setiap tahunnya.

Bagian Kelima
Dukungan Pengoperasian
Pasal 10

(1) Dukungan pengoperasian sebagaimana dimaksud dalam Pasal 3 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.
(3) Koordinator SPBE melalui dukungan pengoperasian memastikan pelaksanaan manajemen Keamanan Informasi SPBE mendapatkan alokasi sumber daya yang sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 11

(1) Sumber Daya Manusia Keamanan SPBE sebagaimana dimaksud dalam Pasal 10 ayat (2) huruf a paling sedikit berjumlah 5 (lima) orang.
(2) Sumber Daya Manusia sebagaimana dimaksud pada ayat (1) harus memiliki kompetensi di bidang:
    a. keamanan TIK; dan
    b. keamanan aplikasi.
(3) Untuk meningkatkan kompetensi sebagaimana dimaksud pada ayat (2), Pemerintah Aceh harus melaksanakan kegiatan:
    a. pelatihan dan/atau sertifikasi kompetensi keamanan aplikasi dan TIK; dan/atau
    b. bimbingan teknis mengenai standar teknis dan prosedur Keamanan SPBE.
(4) Peningkatan kompetensi sebagaimana dimaksud pada ayat (3) dilakukan agar Sumber Daya Manusia Keamanan SPBE memiliki kompetensi dan keahlian yang memadai dalam pelaksanaan Keamanan SPBE.

Pasal 12 .../7

Pasal 12

Teknologi Keamanan SPBE sebagaimana dimaksud dalam Pasal 10 ayat (2) huruf b harus tersedia sesuai kebutuhan dan tingkat urgensi dari setiap SKPA.

Pasal 13

Anggaran Keamanan SPBE sebagaimana dimaksud pada Pasal 10 ayat (2) huruf c disusun berdasarkan perencanaan yang telah ditetapkan sesuai dengan ketentuan peraturan perundang-undangan.

Bagian Keenam

Evaluasi Kinerja

Pasal 14

(1) Evaluasi kinerja sebagaimana dimaksud dalam Pasal 3 huruf e dilakukan oleh Koordinator SPBE.
(2) Evaluasi kinerja sebagaimana dimaksud pada ayat (1) dilakukan terhadap pelaksanaan manajemen Keamanan Informasi SPBE.
(3) Evaluasi kinerja sebagaimana dimaksud pada ayat (2) dilaksanakan dengan:
    a. menganalisis efektivitas 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 atau sewaktu-waktu jika diperlukan.

Bagian Ketujuh

Perbaikan Berkelanjutan Terhadap Keamanan Informasi

Pasal 15

(1) Perbaikan berkelanjutan sebagaimana dimaksud dalam Pasal 3 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. menindaklanjuti hasil audit Keamanan SPBE.

BAB III

PENGENDALIAN TEKNIS KEAMANAN

Bagian Kesatu

Teknis Keamanan

Pasal 16

Pengendalian teknis keamanan meliputi:
a. manajemen risiko;
b. penetapan prosedur pengendalian Keamanan Informasi SPBE; dan
c. pengelolaan pihak ketiga.

Bagian Kedua

Manajemen Resiko

Pasal 17

(1) Manajemen risiko sebagaimana dimaksud dalam Pasal 16 huruf a dilakukan oleh setiap SKPA.

(2) Pelaksanaan .../8

(2) Pelaksanaan manajemen risiko oleh SKPA dilakukan dengan menyusun daftar risiko *(risk register)* yang meliputi:
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 dilaksanakan sesuai dengan ketentuan peraturan perundang- undangan.

Bagian Ketiga

Penetapan Prosedur Pengendalian Keamanan Informasi SPBE

Pasal 18

(1) Penetapan prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud pada Pasal 16 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 informasi SPBE dengan cakupan aspek yang 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 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. 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 atau *disaster recovery plans*;
u. audit internal keamanan SPBE; dan/atau
v. aspek prosedur pengendalian keamanan informasi SPBE lainnya.

(3) Penetapan prosedur pengendalian Keamanan Informasi SPBE sebagaimana dimaksud pada ayat (2) ditetapkan dengan Keputusan Gubernur.

Pasal 19

(1) Setiap Kepala SKPA bertanggung jawab dalam memastikan kegiatan operasional teknologi informasi yang stabil dan aman dengan berpedoman pada prosedur pengendalian keamanan informasi SPBE.

(2) Setiap .../9

(2) Setiap SKPA harus melaksanakan ketentuan penetapan prosedur pengendalian Keamanan Informasi SPBE sebagaimana dimaksud pada Pasal 18 ayat (2).

Bagian Keempat
Pengelolaan Pihak Ketiga
Pasal 20

(1) Pengelolaan Manajemen Keamanan SPBE pada SKPA dapat dikelola pihak ketiga sebagaimana dimaksud dalam Pasal 16 huruf c sesuai dengan ketentuan peraturan perundang-undangan.

(2) Dalam hal pengelolaan Manajemen Keamanan SPBE dikelola oleh pihak ketiga, SKPA bertanggung jawab:

a. 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;

b. memastikan pihak ketiga memberikan akses sepenuhnya terkait pekerjaan pembangunan atau pengembangan Aplikasi SPBE dan Infrastruktur SPBE beserta kode sumbernya kepada SKPA;

c. menetapkan proses, prosedur atau rencana terdokumentasi untuk memantau layanan dan aspek keamanan informasi dalam hubungan kerjasama dengan pihak ketiga; dan

d. membuat laporan secara berkala kepada penanggung jawab SPBE mengenai pencapaian sasaran tingkat layanan atau *Service Level Agreement* (SLA) dan aspek keamanan yang diisyaratkan dalam perjanjian kontrak dengan pihak ketiga.

BAB IV
KETENTUAN PENUTUP
Pasal 21

Peraturan Gubernur ini mulai berlaku pada tanggal diundangkan.

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

Ditetapkan di Banda Aceh
pada tanggal, 22 Desember 2023
9 Jumadil Akhir 1445

Pj. GUBERNUR ACEH,

ACHMAD MARZUKI

Diundangkan di Banda Aceh
pada tanggal, 22 Desember 2023
9 Jumadil Akhir 1445

SEKRETARIS DAERAH ACEH,

BUSTAMI

BERITA DAERAH ACEH TAHUN 2023 NOMOR 46

ATE\MW\DATAWAHED\2023\DISKOMINSA\KEP.GUB\DES