SALINAN

GUBERNUR GORONTALO

PERATURAN GUBERNUR GORONTALO
NOMOR 16 TAHUN 2024

TENTANG

SISTEM MANAJEMEN KEAMANAN INFORMASI PEMERINTAH DAERAH

DENGAN RAHMAT TUHAN YANG MAHA ESA

GUBERNUR GORONTALO,

Menimbang :

a. bahwa dalam rangka pelaksanaan penyelenggaraan pemerintahan yang aman di lingkungan Pemerintah Daerah, diperlukan Manajemen Keamanan Informasi untuk memastikan kerahasiaan, keutuhan, dan ketersediaan terhadap aset informasi dari berbagai ancaman 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 Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik, setiap instansi Pusat dan Pemerintah Daerah harus menerapkan Keamanan Sistem Pemerintahan Berbasis Elektronik;

c. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b, perlu menetapkan Peraturan Gubernur tentang Sistem Manajemen Keamanan Informasi Pemerintah Daerah;

Mengingat :

1. Pasal 18 ayat (6) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;
2. Undang-Undang Nomor 38 Tahun 2000 tentang Pembentukan Provinsi Gorontalo;
3. 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);

4. 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);
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 238, Tambahan Lembaran Negara Republik Indonesia Nomor 6841);
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 129);
8. Peraturan Presiden Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 129);
9. 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 2018 Nomor 157);

10. 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);
11. Peraturan Daerah Provinsi Gorontalo Nomor 3 Tahun 2016 Tentang Penyelenggaraan Pemerintahan Berbasis Teknologi Informasi dan Komunikasi;

MEMUTUSKAN :

Menetapkan : PERATURAN GUBERNUR TENTANG SISTEM MANAJEMEN KEAMANAN INFORMASI PEMERINTAH DAERAH.

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Gubernur ini yang dimaksud dengan :

1. Daerah adalah Provinsi Gorontalo
2. Gubernur adalah Gubernur Gorontalo.
3. Sekretaris Daerah adalah Sekretaris Daerah Provinsi Gorontalo.
4. Pemeritnah Daerah adalah Gubernur sebagai unsur penyelenggara Pemerintahan Daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan daerah otonom.
5. Perangkat Daerah adalah unsur pembantu Gubernur dan DPRD, 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, keutuhan dan ketersediaan dari informasi.

9. Keamanan SPBE mencakup penjaminan kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan (nonrepudiation) sumber daya terkait data dan informasi, Infrastruktur SPBE, dan Aplikasi SPBE.
10. Kerahasiaan adalah sesuai dengan konsep hukum tentang kerahasian (confidentiality) atas informasi dan komunikasi secara Elektronik.
11. Keutuhan adalah sesuai dengan konsep hukum tentang keutuhan (integrity) atas Informasi Elektronik.
12. Ketersediaan adalah sesuai dengan konsep hukum tentang ketersediaan (availability) atas Informasi Elektronik.
13. Manajemen Keamanan SPBE adalah serangkaian proses untuk mencapai penerapan keamanan SPBE yang efektif, efisien, dan berkesinambungan, serta mendukung layanan SPBE yang berkualitas.
14. Aplikasi SPBE adalah satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas atau fungsi Layanan SPBE.
15. Infrastruktur SPBE adalah semua perangkat keras, perangkat lunak, dan fasilitas yang menjadi penunjang utama untuk menjalankan system, aplikasi, komunikasi data, pengolahan dan penyimpanan data, perangkat integrase/penghubung, dan perangkat Elektronik lainnya.
16. Insiden Siber adalah satu atau serangkaian kejadian yang mengganggu atau mengancam berjalannya Sistem Elektronik.
17. Tim Tanggap Insiden Siber (CSIRT) adalah tim yang dibentuk yang bertanggung jawab menangani Insiden Siber dalam ruang lingkup yang ditentukan terhadapnya.

Pasal 2

(1) Peraturan Gubernur ini dimaksudkan sebagai pedoman dalam menerapkan sistem manajemen keamanan informasi secara terpadu di lingkungan Pemerintah Daerah.
(2) Penerapan sistem manajemen keamanan informasi sebagaimana dimaksud pada ayat (1) bertujuan untuk

memastikan kerahasiaan, keutuhan dan ketersediaan terhadap aset informasi Pemerintah Darah dari berbagai ancaman Keamanan Informasi.

(3) Kebijakan internal manajemen keamanan informasi SPBE sebagaimana dimaksud pada ayat (1) meliputi:
   a. penetapan ruang lingkup;
   b. penetapan penanggung jawab;
   c. perencanaan;
   d. dukungan pengoperasian;
   e. evaluasi kinerja; dan
   f. perbaikan berkelanjutan terhadap keamanan informasi.

(4) Ketentuan lain untuk mendukung kebijakan internal manajemen keamanan informasi SPBE sebagaimana dimaksud pada ayat (3) dapat menerapkan pengendalian teknis keamanan yang meliputi:
   a. manajemen risiko;
   b. penetapan prosedur pengendalian keamanan informasi SPBE; dan
   c. pengelolaan pihak ketiga.

BAB II
KEBIJAKAN INTERNAL MANAJEMEN KEAMANAN INFORMASI

Pasal 3

(1) Penetapan ruang lingkup manajemen keamanan informasi SPBE sebagaimana dimaksud dalam Pasal 2 ayat (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 Provinsi yang harus diamankan dalam SPBE.

Pasal 4

(1) Gubernur menetapkan penanggung jawab manajemen keamanan informasi SPBE sebagaimana dimaksud dalam Pasal 2 ayat (3) huruf b dengan Keputusan Gubernur.

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

(3) Penanggungjawab manajemen keamanan informasi dalam melaksanakan tugasnya dibantu oleh Tim Kerja Keamanan SPBE.

Pasal 5

(1) Tim Kerja Keamanan SPBE sebagai dimaksud pada Pasal 4 ayat (3) terdiri atas :
   a. Ketua Tim; dan
   b. Anggota Tim.

(2) Ketua Tim sebagaimana dimaksud pada ayat (1) huruf a dijabat oleh pimpinan Perangkat Daerah yang membidangi urusan komunikasi dan informatika.

(3) Anggota Tim sebagaimana dimaksud pada ayat (1) huruf b terdiri dari seluruh unsur pelaksana SPBE yang memiliki kompetensi teknis dalam Keamanan SPBE.

(4) Tim Kerja Keamanan SPBE sebagaimana dimaksud pada ayat (1) ditetapkan dengan Keputusan Gubernur.

Pasal 6

(1) Ketua Tim sebagaimana dimaksud dalam Pasal 5 ayat (1) huruf a mempunyai tugas:
   a. menetapkan prosedur pengendalian keamanan informasi SPBE Pemerintah Provinsi;
   b. mengevaluasi penerapan prosedur pengendalian keamanan informasi SPBE di lingkungan Pemerintah Provinsi;
   c. memastikan penerapan keamanan Aplikasi SPBE dan Infrastruktur SPBE sesuai dengan standar teknis dan prosedur Keamanan SPBE yang telah ditetapkan sesuai dengan 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 recovery plans; dan
h. melaporkan pelaksanaan manajemen keamanan informasi SPBE pada koordinator SPBE.

(2) Anggota Tim sebagaimana dimaksud dalam Pasal 5 ayat (1) huruf b mempunyai tugas:
a. mengoordinasikan dan/atau memastikan penerapan prosedur pengendalian keamanan informasi SPBE pada Perangkat Daerah;
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;
d. mengirim laporan pengelolaan insiden keamanan informasi kepada Ketua Tim;
e. mendokumentasikan proses pengelolaan insiden keamanan informasi di Perangkat Daerah;
f. Melakukan koordinasi dan tindak lanjut pengamanan atas Insiden Siber bersama Tim Tanggap Insiden Siber (CSIRT)
g. melaksanakan dan mengelola langkah kelangsungan layanan TIK yang berpedoman pada dokumen business continuity dan disaster recovery plans; dan
h. berkoordinasi dengan Ketua Tim terkait penerapan keamanan Aplikasi SPBE dan Infrastruktur SPBE.

Pasal 7

(1) Perencanaan sebagaimana dimaksud dalam Pasal 2 ayat (3) huruf c dilakukan oleh Tim Kerja 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 8

(1) Program Kerja Keamanan SPBE sebagaimana dimaksud dalam Pasal 7 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 7 ayat (2) huruf b ditetapkan berdasarkan ketentuan prioritas setiap tahunnya.

Pasal 9

(1) Dalam hal pelaksanaan Program Kerja Keamanan SPBE sebagaimana dimaksud dalam Pasal 7 ayat (2) huruf a, Gubernur menetapkan Tim Tanggap Insiden Siber.
(2) Tim Tanggap Insiden Siber sebagai dimaksud pada ayat (1) terdiri atas:
a. penanggungjawab tim;
b. ketua tim; dan
c. anggota tim.
(3) Penanggungjawab Tim sebagaimana dimaksud pada ayat (2) huruf a, dijabat oleh Sekretaris Daerah Provinsi;
(4) Ketua Tim sebagaimana dimaksud pada ayat (2) huruf b dijabat oleh pimpinan Perangkat Daerah yang membidangi urusan komunikasi dan informatika.
(5) Anggota Tim sebagaimana dimaksud pada ayat (2) huruf b terdiri dari terdiri dari berbagai unsur pelaksana SPBE yang memiliki kompetensi dalam penanganan Insiden Siber.

Pasal 10

(1) Dukungan pengoperasian sebagaimana dimaksud dalam Pasal 2 ayat (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.

Pasal 11

(1) Sumber Daya Manusia Keamanan SPBE sebagaimana dimaksud dalam Pasal 10 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 10 ayat (2) huruf b harus tersedia sesuai kebutuhan dan tingkat urgensi dari setiap Perangkat Daerah.

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

Pasal 12

(1) Evaluasi kinerja sebagaimana dimaksud dalam Pasal 2 ayat (3) huruf e dilakukan oleh koordinator SPBE.

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

(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, Badan Siber dan Sandi Negara dan Instansi terkait.

Pasal 13

(1) Perbaikan berkelanjutan sebagaimana dimaksud dalam Pasal 2 ayat (3) huruf f dilakukan oleh Tim Kerja 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 14

(1) Manajemen risiko sebagaimana dimaksud dalam Pasal 2 ayat (4) huruf a dilakukan oleh setiap Perangkat Daerah.

(2) Setiap Perangkat Daerah menyusun daftar risiko (risk register) dengan ketentuan subtansi paling sedikit 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/atau
   g. rekomendasi kontrol keamanan.

(3) Prosedur pelaksanaan manajemen risiko mengacu sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 15

(1) Penetapan prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud dalam Pasal 2 ayat (4) huruf b disusun oleh Tim Kerja 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 dengan cakupan aspek dapat 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. 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) dijadikan Pedoman Pelaksanaan dan ditetapkan dengan Keputusan Gubernur.

Pasal 16

(1) Setiap Perangkat Daerah harus melaksanakan ketentuan penetapan prosedur pengendalian keamanan informasi SPBE sebagaimana dimaksud dalam Pasal 15 ayat (1).
(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 17

(1) Pengelolaan pihak ketiga sebagaimana dimaksud dalam Pasal 2 ayat (4) 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 harus menetapkan proses, prosedur atau rencana terdokumentasi untuk memantau layanan dan aspek keamanan informasi dalam hubungan kerja sama dengan pihak ketiga.

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

BAB IV
PENDANAAN

Pasal 18

Pendanaan penyelenggaraan Manajemen Kemanan Informasi SPBE bersumber pada:

a. Anggaran Pendapatan dan Belanja Daerah Provinsi; dan
b. sumber pendanaan lain yang sah dan tidak mengikat sesuai dengan ketentuan peraturan perundang-undangan.

BAB V
KETENTUAN PENUTUP

Pasal 19

Peraturan Gubernur ini mulai berlaku pada tanggal diundangkan.

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

Ditetapkan di Gorontalo
pada tanggal 19 Juli 2024
Pj. GUBERNUR GORONTALO,

ttd

RUDY SALAHUDDIN

Diundangkan di Gorontalo
pada tanggal 19 Juli 2024
SEKRETARIS DAERAH PROVINSI GORONTALO,

ttd

SOFIAN IBRAHIM

BERITA DAERAH PROVINSI GORONTALO TAHUN 2024 NOMOR 16

Salinan sesuai dengan aslinya
Kepala Biro Hukum
Setda Provinsi Gorontalo,

Mohamad Trizal Entengo, S.H., M.H.
Pembina Utama Muda (VI/c)
NIP. 19700115 199803 1 011