SALINAN

GUBERNUR JAWA TENGAH

PERATURAN GUBERNUR JAWA TENGAH

NOMOR 25 TAHUN 2023

TENTANG

SISTEM MANAJEMEN KEAMANAN INFORMASI PEMERINTAH DAERAH

DENGAN RAHMAT TUHAN YANG MAHA ESA

GUBERNUR JAWA TENGAH,

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 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 pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b serta agar pelaksanaan Manajemen Keamanan Informasi dapat berdayaguna dan berhasilguna, perlu menetapkan Peraturan Gubernur tentang Sistem Manajemen Keamanan Informasi Pemerintah Daerah;

Mengingat :

1. Undang–Undang Nomor 10 Tahun 1950 tentang Pembentukan Provinsi Jawa Tengah (Himpunan Peraturan-Peraturan Negara Tahun 1950 Halaman 86-92);

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 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);
5. 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);
6. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
7. Peraturan Presiden Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 129);
8. 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);
9. Peraturan Gubernur Jawa Tengah Nomor 11 Tahun 2018 tentang Pedoman Pola Hubungan Komunikasi Sandi Di Lingkungan Pemerintah Provinsi Jawa Tengah (Berita Daerah Provinsi Jawa Tengah Tahun 2018 Nomor 11);
10. Peraturan Gubernur Jawa Tengah Nomor 25 Tahun 2021 tentang Penyelenggaraan Persandian Untuk Pengamanan Informasi Di Lingkungan Pemerintah Provinsi Jawa Tengah (Berita Daerah Provinsi Jawa Tengah Tahun 2021 Nomor 25);

MEMUTUSKAN :

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

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Gubernur ini yang dimaksud dengan :

1. Daerah adalah Provinsi Jawa Tengah.
2. Pemerintah Daerah adalah Gubernur sebagai unsur penyelenggara Pemerintahan Daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan daerah otonom.
3. Gubernur adalah Gubernur Jawa Tengah.
4. Sekretaris Daerah adalah Sekretaris Daerah Provinsi Jawa Tengah.
5. Perangkat Daerah adalah unsur pembantu Gubernur dan Dewan Perwakilan Rakyat Daerah dalam penyelenggaraan Urusan Pemerintahan yang menjadi kewenangan Daerah.
6. Informasi adalah keterangan, pernyataan, gagasan, dan 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 ataupun non elektronik.
7. Sistem adalah suatu kesatuan yang terdiri komponen atau elemen yang dihubungkan bersama untuk memudahkan aliran informasi, materi atau energi untuk mencapai suatu tujuan.
8. Teknologi Informasi adalah suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan/atau menyebarkan informasi.
9. Teknologi Informasi dan Komunikasi yang selanjutnya disingkat TIK adalah segala kegiatan yang terkait dengan pemrosesan, manipulasi, pengelolaan, dan pemindahan informasi antar media.
10. Komputer adalah alat untuk memproses data elektronik, mengetik, optik, atau sistem yang melaksanakan fungsi logika, algoritma, dan menyimpan data.
11. Perangkat Keras adalah semua jenis piranti atau komponen komputer yang bagian fisiknya dapat dilihat secara kasat mata dan dirasakan langsung.
12. Perangkat lunak adalah satu atau sekumpulan program komputer, prosedur, dan/atau dokumentasi yang terkait dalam pengoperasian Sistem Elektronik.

13. Sistem manajemen adalah sekumpulan kebijakan, proses, dan prosedur yang digunakan oleh organisasi atau institusi untuk memastikan bahwa sistem dapat memenuhi tugas yang diperlukan untuk mencapai tujuannya.
14. Keamanan Informasi adalah terjaganya kerahasiaan, keaslian, keutuhan, ketersediaan, dan kenirsangkalan informasi.
15. Manajemen Informasi adalah pengumpulan, penyimpanan, pengelolaan, pemeliharaan, penyebaran, pengarsipan, dan penghancuran informasi.
16. Sistem Manajemen Keamanan Informasi yang selanjutnya disingkat SMKI adalah sistem manajemen yang meliputi kebijakan, organisasi, perencanaan, penanggung jawab, proses, dan sumber daya yang mengacu pada pendekatan risiko bisnis untuk menetapkan, mengimplementasikan, mengoperasikan, memonitoring, mengevaluasi, mengelola, dan meningkatkan keamanan informasi.
17. Aset informasi adalah unit informasi yang dapat dipahami, dibagi, dilindungi, dan dimanfaatkan secara efektif.
18. Penyimpanan informasi adalah suatu proses menyimpan informasi dengan menggunakan media baik elektronik maupun non-elektronik.
19. Pusat Data (*Data Center*) adalah suatu fasilitas untuk menempatkan sistem komputer dan perangkat-perangkat terkait, seperti sistem komunikasi data dan penyimpanan data.
20. Akses adalah kegiatan melakukan interaksi dengan Sistem Elektronik dalam jaringan.
21. Perangkat Non Elektronik adalah adalah peralatan yang digunakan untuk mengelola informasi nonelektronik.
22. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada Pengguna SPBE.
23. Aplikasi SPBE adalah satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas atau fungsi Layanan SPBE.
24. 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.

BAB II
MAKSUD DAN TUJUAN

Pasal 2

(1) Peraturan Gubernur ini dimaksudkan sebagai pedoman dalam menerapkan SMKI secara terpadu di lingkungan Pemerintah Daerah.

(2) Penerapan SMKI sebagaimana dimaksud pada ayat (1) bertujuan untuk memastikan kerahasiaan, keutuhan dan ketersediaan terhadap aset informasi Pemerintah Daerah dari berbagai ancaman Keamanan Informasi.

Pasal 3

Ruang lingkup penerapan SMKI secara terpadu sebagaimana dimaksud dalam Pasal 2 ayat (1) meliputi proses :

a. penetapan cakupan;
b. penetapan penanggung jawab;
c. perencanaan;
d. dukungan pengoperasian;
e. prosedur pengendalian; dan
f. evaluasi kinerja, monitoring, dan perbaikan berkelanjutan.

BAB III
PENETAPAN CAKUPAN

Pasal 4

(1) Penetapan cakupan sebagaimana dimaksud dalam Pasal 3 huruf a meliputi aset :
    a. Data dan Informasi;
    b. Pengelolaan Informasi; dan
    c. Penyimpanan Informasi.

(2) Aset sebagaimana dimaksud pada ayat (1) merupakan aset milik Pemerintah Daerah yang wajib diamankan dalam SMKI.

Pasal 5

Data dan Informasi sebagaimana dimaksud dalam Pasal 4 ayat (1) huruf a merupakan data dan informasi dalam bentuk :

a. elektronik, meliputi informasi tercetak, tertulis dan tersimpan dalam bentuk elektronik seperti *database*, pada *file* di dalam komputer, ditampilkan pada *website*, layar komputer dan dikirimkan melalui jaringan telekomunikasi;

b. nonelektronik, meliputi informasi yang tercetak, tertulis dan tersimpan dalam bentuk fisik seperti di atas kertas, papan tulis, spanduk atau di dalam buku dan dokumen.

Pasal 6

Pengelolaan Informasi sebagaimana dimaksud dalam Pasal 4 ayat (1) huruf b meliputi :

a. Aplikasi SPBE;
b. Infrastruktur SPBE; dan
c. Perangkat Non Elektronik.

Pasal 7

Penyimpanan Informasi sebagaimana dimaksud dalam Pasal 4 ayat (1) huruf c menggunakan media :

a. elektronik, meliputi antara lain *hard di*sk, *flash d*isk, kartu memori, dan perangkat elektronik penyimpanan lainnya; dan
b. nonelektronik, meliputi antara lain lemari, rak, laci, *filing cabinet*, dan perangkat non elektronik penyimpanan lain-lain.

BAB IV
PENETAPAN PENANGGUNG JAWAB

Pasal 8

(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) Dalam melaksanakan tugas sebagai penanggung jawab Keamanan Informasi, Sekretaris Daerah membentuk Tim Keamanan Informasi yang ditetapkan melalui keputusan.
(4) Ketua Tim Keamanan Informasi sebagaimana dimaksud pada ayat (3) dijabat oleh Kepala Perangkat Daerah yang membidangi urusan Persandian dan Keamanan Informasi.
(5) Tim Keamanan Informasi sebagaimana dimaksud pada ayat (3) berwenang :
    a. menetapkan Standar Operasional Prosedur Pengendalian Keamanan Informasi Pemerintah Daerah;
    b. merumuskan, mengoordinasikan, dan melaksanakan program kerja dan anggaran Keamanan Informasi;
    c. memutuskan, merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK dalam bentuk dokumen *business continuity* dan *disaster recovery plans*;
    d. melakukan evaluasi kinerja penyelenggaraan Keamanan Informasi;

e. memastikan penerapan standar teknis dan prosedur pengendalian Keamanan Informasi pada seluruh Perangkat Daerah; dan

f. 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.

BAB V
PERENCANAAN

Pasal 9

(1) Perencanaan sebagaimana dimaksud dalam Pasal 3 huruf c ditetapkan oleh Ketua Tim Keamanan Informasi.

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

a. program kerja Keamanan Informasi; dan

b. target *output/outcome* program kerja Keamanan Informasi.

(3) Program kerja Keamanan Informasi sebagaimana dimaksud pada ayat (2) huruf a paling sedikit meliputi :

a. edukasi kesadaran Keamanan Informasi;

b. penilaian kerentanan Keamanan Informasi;

c. peningkatan Keamanan Informasi;

d. penanganan insiden Keamanan Informasi; dan

e. audit Keamanan Informasi.

(4) Target *output/outcome* program kerja Keamanan Informasi sebagaimana dimaksud pada ayat (2) huruf b ditetapkan berdasarkan ketentuan prioritas setiap tahunnya.

BAB VI
DUKUNGAN PENGOPERASIAN

Pasal 10

(1) Dukungan pengoperasian sebagaimana dimaksud dalam Pasal 3 huruf d dilakukan oleh Ketua Tim Keamanan Informasi dan Kepala Perangkat Daerah.

(2) Dukungan pengoperasian sebagaimana dimaksud pada ayat (1) dilakukan dengan meningkatkan kapasitas terhadap :

a. sumber daya manusia Keamanan Informasi;

b. teknologi Keamanan Informasi; dan

c. anggaran Keamanan Informasi.

Pasal 11

(1) Sumber daya manusia Keamanan Informasi sebagaimana dimaksud dalam Pasal 10 ayat (2) huruf a, paling sedikit memiliki kompetensi :
    a. keamanan infrastruktur teknologi, informasi dan komunikasi; dan
    b. keamanan aplikasi.
(2) Untuk memenuhi kompetensi sebagaimana dimaksud pada ayat (1), paling sedikit didukung dengan kegiatan:
    a. pelatihan dan/atau sertifikasi kompetensi keamanan infrastruktur teknologi dan keamanan aplikasi; dan
    b. bimbingan teknis mengenai standar Keamanan SPBE.

Pasal 12

Teknologi Keamanan Informasi sebagaimana dimaksud dalam Pasal 10 ayat (2) huruf b wajib tersedia sesuai kebutuhan dan berdasarkan tingkat urgensi dari setiap Perangkat Daerah.

Pasal 13

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

BAB VII
PROSEDUR PENGENDALIAN

Pasal 14

(1) Prosedur pengendalian Keamanan Informasi sebagaimana dimaksud dalam Pasal 3 huruf e ditetapkan oleh Ketua Tim Keamanan Informasi.
(2) Prosedur pengendalian Keamanan Informasi 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 pembangunan dan pengembangan aplikasi SPBE;
    e. keamanan sumber daya manusia;
    f. pengelolaan aset;
    g. keamanan fisik dan lingkungan;
    h. keamanan operasional;
    i. keamanan komunikasi;

j. keamanan dalam proses akuisisi, pengembangan dan pemeliharaan sistem informasi;
k. kebijakan terhadap pihak ketiga;
l. penanganan insiden Keamanan Informasi;
m. kelangsungan bisnis atau layanan TIK (*business continuity*);
n. perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plans*);
o. audit internal keamanan SPBE;
p. kepatuhan Keamanan Informasi; dan/atau
q. pelindungan Data dan Privasi.

(3) Prosedur pengendalian Keamanan Informasi sebagaimana dimaksud pada ayat (2) selanjutnya ditetapkan dalam bentuk surat edaran atau kebijakan teknis lainnya oleh Ketua Tim Keamanan Informasi.

Pasal 15

(1) Perangkat Daerah wajib melaksanakan ketentuan surat edaran atau kebijakan teknis lainnya terkait prosedur pengendalian Keamanan Informasi sebagaimana dimaksud dalam Pasal 14 ayat (3) untuk mendukung penerapan SMKI di setiap Perangkat Daerah.

(2) Pelaksanaan ketentuan sebagaimana dimaksud pada ayat (1) dalam rangka memastikan penerapan SMKI dilakukan sesuai ketentuan peraturan perundang-undangan.

BAB VIII
EVALUASI KINERJA, MONITORING, DAN PERBAIKAN BERKELANJUTAN

Pasal 16

Perangkat Daerah wajib melaksanakan evaluasi, monitoring, dan perbaikan berkelanjutan terhadap SMKI.

Pasal 17

Perangkat Daerah wajib melakukan kegiatan pemantauan dan tindakan koreksi penyimpangan terhadap SMKI yang meliputi :

a. kegiatan pemantauan secara terus menerus; dan
b. pelaksanaan fungsi Pemeriksaan Intern yang efektif dan menyeluruh.

Pasal 18

(1) Perangkat Daerah wajib menindaklanjuti hasil audit, umpan balik, maupun evaluasi terhadap pengendalian SMKI yang dilakukan untuk meningkatkan efektivitas SMKI secara berkesinambungan melalui perbaikan terhadap akibat penyimpangan kegiatan Keamanan Informasi.

(2) Hasil dari tindakan perbaikan dan peningkatan sebagaimana dimaksud pada ayat (1) wajib dilaporkan kepada Ketua Tim Keamanan Informasi dan didokumentasikan sebagai bagian dari proses *lesson learned*.

Pasal 19

(1) Apabila terjadi kebocoran informasi pada Perangkat Daerah yang berdampak sangat luas, maka Ketua Tim Keamanan Informasi dapat menunjuk Auditor independen untuk melakukan investigasi yang diperlukan.

(2) Perangkat Daerah wajib menyediakan akses kepada Auditor Independen sebagaimana dimaksud pada ayat (1) untuk melakukan audit seluruh aspek terkait penyelenggaraan teknologi untuk Keamanan Informasi.

BAB IX
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 Jawa Tengah.

Ditetapkan di Semarang
pada tanggal 24 Juli 2023

GUBERNUR JAWA TENGAH,

ttd

GANJAR PRANOWO

Diundangkan di Semarang
pada tanggal 24 Juli 2023

SEKRETARIS DAERAH PROVINSI
JAWA TENGAH,

ttd

SUMARNO

BERITA DAERAH PROVINSI JAWA TENGAH TAHUN 2023 NOMOR 25

Salinan sesuai dengan aslinya
KEPALA BIRO HUKUM

Ditandatangani secara elektronik oleh:

IWANUDDIN ISKANDAR
Pembina Utama Muda
NIP. 19711207 199503 1 003