RANCANGAN

PERATURAN WALI KOTA YOGYAKARTA

NOMOR TAHUN 2025

TENTANG

SISTEM MANAJEMEN KEAMANAN INFORMASI

DENGAN RAHMAT TUHAN YANG MAHA ESA

WALI KOTA YOGYAKARTA,

Menimbang :

a. bahwa sistem manajemen keamanan Informasi diperlukan untuk menunjang keamanan Informasi sebagai aset strategis Pemerintah Daerah serta mendukung tata kelola teknologi Informasi yang andal dalam mewujudkan keamanan siber secara menyeluruh;

b. bahwa dalam rangka melindungi kerahasiaan, keutuhan, dan ketersediaan aset Informasi Daerah dari berbagai ancaman keamanan Informasi baik dari dalam maupun luar, perlu melakukan penyelenggaraan keamanan Informasi;

c. bahwa Peraturan Wali Kota Yogyakarta Nomor 113 Tahun 2019 tentang Sistem Manajemen Keamanan Informasi sudah tidak sesuai dengan kebutuhan masyarakat dan dinamika peraturan perundang-undangan, sehingga perlu dicabut dan diganti;

d. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b, dan huruf c, perlu menetapkan Peraturan Wali Kota tentang Sistem Manajemen Keamanan Informasi;

Mengingat :

1. Pasal 18 ayat (6) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;

2. 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);

3. Undang-Undang Nomor 121 Tahun 2024 tentang Kota Yogyakarta di Daerah Istimewa Yogyakarta (Lembaran Negara Republik Indonesia Tahun 2024 Nomor 307, Tambahan Lembaran Negara Republik Indonesia Nomor 7058);

MEMUTUSKAN:

Menetapkan : PERATURAN WALI KOTA TENTANG SISTEM MANAJEMEN KEAMANAN INFORMASI.

BAB I

KETENTUAN UMUM

Pasal 1

Dalam Peraturan Wali Kota ini yang dimaksud dengan:

1. Sistem Manajemen Keamanan Informasi yang selanjutnya disingkat SMKI adalah sistem manajemen untuk membangun, mengimplementasikan, mengoperasikan, memonitor, meninjau, memelihara dan meningkatkan keamanan informasi berdasarkan pendekatan risiko.
2. Keamanan Informasi adalah terjaganya kerahasiaan, keaslian, keutuhan, ketersedian, dan kenirsangkalan informasi.
3. Teknologi Informasi dan Komunikasi selanjutnya disebut TIK adalah terminologi yang mencakup seluruh peralatan teknis untuk memproses dan menyampaikan informasi.
4. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi elektronik.
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. Data adalah tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange*, surat elektronik/*electronic mail*, telegram, teleks, *telecopy* atau sejenisnya, huruf, tanda, angka, kode akses, simbol, atau perforasi.
7. Informasi adalah satu atau sekumpulan data, termasuk tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto, *electronic data interchange*, surat elektronik/*electronic mail*, telegram, teleks, *telecopy* atau sejenisnya, huruf, tanda, angka, kode akses, simbol, atau perforasi yang telah diolah yang memiliki arti atau dapat dipahami oleh orang yang mampu memahaminya.
8. Aplikasi adalah satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas atau fungsi layanan.
9. Infrastruktur 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.
10. Aplikasi SPBE adalah satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas atau fungsi layanan SPBE.

11. 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.
12. Risiko adalah segala kejadian dalam setiap aktivitas yang mungkin timbul karena faktor ketidakpastian, yang mengandung potensi untuk menghambat pencapaian sasaran kinerja dari layanan Sistem Elektronik.
13. Manajemen Risiko adalah aktivitas terkoordinasi untuk identifikasi, penilaian, dan penentuan prioritas Risiko yang kemudian akan dikelola, dipantau, dan dikontrol untuk mengurangi dampak dan/atau kemungkinan terjadinya Risiko tersebut.
14. *Risk Treatment Plan* atau Rencana Tindak Lanjut Risiko yang selanjutnya disebut RTL adalah respon yang direncanakan manajemen untuk menindaklanjuti hasil evaluasi Risiko, seperti *mitigate*/*reduce*, *avoid*, *share*/transfer atau *accept*.
15. Audit Teknologi Informasi dan Komunikasi yang selanjutnya disebut Audit TIK adalah proses yang sistematis untuk memperoleh dan mengevaluasi bukti secara objektif terhadap aset TIK dengan tujuan untuk menetapkan tingkat kesesuaian antara TIK dengan kriteria dan/atau standar yang telah ditetapkan.
16. Audit Keamanan Informasi adalah Audit TIK cakupan Keamanan Informasi.
17. Auditor Keamanan Informasi adalah orang yang memiliki kompetensi untuk melakukan Audit Keamanan Informasi.
18. Audit Internal Keamanan Informasi adalah Audit Keamanan Informasi yang dilaksanakan oleh Auditor Keamanan Informasi internal Pemerintah Daerah.
19. Audit Eksternal Keamanan Informasi adalah Audit Keamanan Informasi yang dilaksanakan oleh Auditor Keamanan Informasi eksternal Pemerintah Daerah yang memiliki sertifikasi sebagai Auditor Keamanan Informasi.
20. Sertifikat Elektronik adalah sertifikat yang bersifat elektronik yang memuat tanda tangan elektronik dan identitas yang menunjukkan status subjek hukum para pihak dalam transaksi elektronik yang dikeluarkan oleh Penyelenggara sertifikasi elektronik.
21. Insiden Siber adalah satu atau serangkaian kejadian yang mengganggu atau mengancam keamanan informasi antara lain namun tidak terbatas pada *web defacement, malware* (*virus, worm, trojan backdoor dan ransomware), unauthorized access, data breach, dan Distributed Denial of Service* (DDoS).
22. Tim Tanggap Insiden Siber adalah sekelompok orang yang bertanggung jawab menangani Insiden Siber dalam ruang lingkup yang ditentukan terhadapnya.
23. Tim Pengelola Sistem Manajemen Keamanan Informasi yang selanjutnya disebut Tim SMKI adalah sekelompok orang yang bertanggung jawab untuk menyusun, mengomunikasikan, memastikan, dan memantau penyelenggaraan SMKI di Pemerintah Daerah.
24. Wali Kota adalah Wali Kota Yogyakarta.
25. Sekretaris Daerah adalah Sekretaris Daerah Kota Yogyakarta sekaligus sebagai Koordinator SPBE Pemerintah Kota Yogyakarta.

26. Pemerintah Daerah adalah Wali Kota sebagai unsur penyelenggara pemerintahan daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan daerah otonom.
27. Perangkat Daerah adalah unsur pembantu Wali Kota dan Dewan Perwakilan Rakyat Daerah dalam penyelenggaraan urusan Pemerintahan yang menjadi kewenangan Daerah.
28. Daerah adalah Kota Yogyakarta.

Pasal 2

(1) Maksud disusunnya Peraturan Wali Kota ini sebagai pedoman dalam penyelenggaraan SMKI.
(2) Tujuan disusunnya Peraturan Wali Kota ini untuk:
    a. menjaga kerahasiaan, keutuhan, dan ketersediaan Informasi; dan
    b. meminimalkan dampak Risiko Keamanan Informasi.

BAB II

KEBIJAKAN SISTEM MANAJEMEN KEAMANAN INFORMASI

Pasal 3

Pemerintah Daerah melaksanakan SMKI melalui kebijakan:

a. umum; dan
b. khusus.

Pasal 4

Ketentuan mengenai kebijakan umum SMKI sebagaimana dimaksud dalam Pasal 3 huruf a tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Peraturan Wali Kota ini.

Pasal 5

(1) Kebijakan khusus sebagaimana dimaksud dalam Pasal 3 huruf b meliputi:
    a. penetapan ruang lingkup;
    b. penetapan penanggung jawab SMKI;
    c. perencanaan;
    d. dukungan pengoperasian;
    e. kendali keamanan;
    f. Audit Keamanan Informasi; dan
    g. evaluasi kinerja dan perbaikan berkelanjutan Keamanan Informasi.
(2) Pemerintah Daerah dalam melaksanakan penetapan penanggung jawab SMKI sebagaimana dimaksud pada ayat (1) huruf b, perencanaan sebagaimana dimaksud pada ayat (1) huruf c, kendali keamanan sebagaimana dimaksud pada ayat (1) huruf e, dan evaluasi kinerja dan perbaikan berkelanjutan Keamanan Informasi sebagaimana pada ayat (1) huruf g membentuk Tim SMKI.

BAB III

PENETAPAN RUANG LINGKUP

Pasal 6

(1) Penetapan ruang lingkup manajemen Keamanan Informasi sebagaimana dimaksud dalam Pasal 5 ayat (1) huruf a meliputi:

a. Data dan Informasi SPBE;

b. Aplikasi SPBE;

c. Infrastruktur SPBE; dan

d. sumber daya manusia SPBE.

(2) Ketentuan mengenai ruang lingkup sebagaimana dimaksud pada ayat (1) tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Peraturan Wali Kota ini.

BAB IV

PENETAPAN PENANGGUNG JAWAB

Pasal 7

(1) Wali Kota menetapkan penanggung jawab SMKI sebagaimana dimaksud dalam Pasal 5 ayat (1) huruf b.

(2) Penanggung jawab SMKI sebagaimana dimaksud pada ayat (1) merupakan Sekretaris Daerah.

(3) Sekretaris Daerah sebagaimana dimaksud pada ayat (2) bertanggung jawab atas penyelenggaraan SMKI di Daerah.

(4) Sekretaris Daerah dalam penyelenggaraan SMKI di Daerah sebagaimana dimaksud pada ayat (3) dibantu oleh Tim SMKI.

(5) Penanggung jawab SMKI sebagaimana dimaksud pada ayat (1) dan Tim SMKI sebagaimana dimaksud pada ayat (4) ditetapkan dengan Keputusan Wali Kota.

BAB V

PERENCANAAN KEAMANAN INFORMASI

Bagian Kesatu

Umum

Pasal 8

(1) Pemerintah Daerah melakukan perencanaan Keamanan Informasi sebagaimana dimaksud dalam Pasal 5 ayat (1) huruf c melalui Tim SMKI.

(2) Perencanaan Keamanan Informasi sebagaimana dimaksud pada ayat (1) dilakukan melalui kegiatan:

a. melakukan Manajemen Risiko Keamanan Informasi; dan

b. menyusun program kerja Keamanan Informasi.

Bagian Kedua

Manajemen Risiko Keamanan Informasi

Pasal 9

(1) Tim SMKI melaksanakan Manajemen Risiko Keamanan Informasi sebagaimana dimaksud dalam Pasal 8 ayat (2) huruf a dengan memperhatikan berbagai Risiko yang dapat mengakibatkan terjadinya kegagalan Keamanan Informasi di Daerah.

(2) Manajemen Risiko Keamanan Informasi sebagaimana dimaksud pada ayat (1) meliputi:

a. menyusun penilaian Risiko Keamanan Informasi;

b. menyusun RTL; dan

c. melakukan sosialisasi dan komunikasi RTL.

(3) Penyusunan penilaian Risiko Keamanan Informasi sebagaimana dimaksud pada ayat (2) huruf a dilakukan melalui identifikasi:

a. ancaman;

b. kerentanan;

c. peluang; dan

d. dampak,

dalam hal terjadi Risiko.

(4) Penyusunan RTL sebagaimana dimaksud pada ayat (2) huruf b dilakukan bersama setiap Perangkat Daerah terkait.

(5) Sosialisasi dan komunikasi RTL sebagaimana dimaksud pada ayat (2) huruf c dilaksanakan bagi para pemilik Risiko.

Pasal 10

(1) Tim SMKI melakukan pengukuran Manajemen Risiko Keamanan Informasi sebagaimana dimaksud dalam Pasal 9 secara:

a. berkala; dan/atau

b. sewaktu-waktu.

(2) Pengukuran Manajemen Risiko Keamanan Informasi secara berkala sebagaimana dimaksud pada ayat (1) huruf a dilakukan paling sedikit 1 (satu) kali dalam 1 (satu) tahun.

(3) Pengukuran Manajemen Risiko Keamanan Informasi secara sewaktu-waktu sebagaimana dimaksud pada ayat (1) huruf b dilakukan dalam hal terdapat perubahan aset atau proses bisnis yang berdampak signifikan terhadap profil Risiko yang ditetapkan.

Bagian Ketiga

Program Kerja Keamanan Informasi

Pasal 11

(1) Tim SMKI menyusun program kerja Keamanan Informasi sebagaimana dimaksud dalam Pasal 8 ayat (2) huruf b berdasarkan RTL.

(2) Program kerja Keamanan Informasi sebagaimana dimaksud pada ayat (1) paling sedikit meliputi:

a. edukasi kesadaran Keamanan Informasi;

b. penilaian kerentanan Keamanan Informasi;

c. peningkatan Keamanan Informasi;

d. penanganan Insiden Siber; dan

e. Audit Keamanan Informasi.

(3) Program kerja Keamanan Informasi sebagaimana dimaksud pada ayat (1) dituangkan dalam peta rencana Keamanan Informasi yang disusun untuk periode 5 (lima) tahunan.

(4) Program kerja Keamanan Informasi sebagaimana dimaksud pada ayat (3) disusun dengan sasaran Keamanan Informasi yang ditetapkan untuk setiap tahunnya.

(5) Peta rencana Keamanan Informasi sebagaimana dimaksud pada ayat (3) menjadi bagian dari peta rencana SPBE.

BAB VI

DUKUNGAN PENGOPERASIAN

Pasal 12

(1) Sekretaris Daerah memberikan dukungan pengoperasian Keamanan Informasi sebagaimana dimaksud dalam Pasal 5 ayat (1) huruf d.

(2) Dukungan pengoperasian Keamanan Informasi sebagaimana dimaksud pada ayat (1) berupa penyediaan:

a. sumber daya manusia Keamanan Informasi yang kompeten; dan

b. anggaran Keamanan Informasi.

(3) Penyediaan anggaran Keamanan Informasi sebagaimana dimaksud pada ayat (2) huruf b berdasarkan arsitektur dan peta rencana SPBE yang telah disusun.

BAB VII

KENDALI KEAMANAN

Pasal 13

(1) Pemerintah Daerah melaksanakan kendali keamanan SMKI sebagaimana dimaksud dalam Pasal 5 ayat (1) huruf e melalui Tim SMKI.

(2) Kendali keamanan sebagaimana dimaksud pada ayat (1) meliputi:

a. keamanan sumber daya manusia;

b. keamanan aset Informasi;

c. keamanan akses;

d. keamanan kriptografi;

e. keamanan fisik dan lingkungan;

f. keamanan operasional;

g. keamanan komunikasi;

h. keamanan pengembangan dan pemeliharaan;

i. keamanan pihak ketiga;

j. manajemen Insiden Siber;

k. manajemen keberlangsungan layanan Informasi; dan

l. pengendalian kepatuhan.

(3) Ketentuan mengenai kendali keamanan sebagaimana dimaksud pada ayat (2) tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Peraturan Wali Kota ini.

BAB VIII

AUDIT KEAMANAN INFORMASI

Pasal 14

(1) Audit Keamanan Informasi sebagaimana dimaksud dalam Pasal 5 ayat (1) huruf f dilaksanakan secara berkala untuk memastikan diterapkannya kebijakan, standar, dan prosedur Keamanan Informasi.

(2) Audit Keamanan Informasi sebagaimana dimaksud pada ayat (1) dilaksanakan melalui kegiatan:

a. Audit Internal Keamanan Informasi; dan

b. Audit Eksternal Keamanan Informasi.

(3) Audit Internal Keamanan Informasi sebagaimana dimaksud pada ayat (2) huruf a dilaksanakan oleh Aparat Pengawas Intern Pemerintah.

(4) Audit Eksternal Keamanan Informasi sebagaimana dimaksud pada ayat (2) huruf b dilaksanakan oleh pihak ketiga sesuai dengan ketentuan peraturan perundang-undangan.

(5) Ketentuan mengenai tata cara Audit Internal Keamanan Informasi sebagaimana dimaksud pada ayat (3) tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Peraturan Wali Kota ini.

BAB IX

EVALUASI KINERJA DAN PERBAIKAN BERKELANJUTAN KEAMANAN INFORMASI

Pasal 15

(1) Sekretaris Daerah dengan dibantu Tim SMKI melakukan evaluasi kinerja Keamanan Informasi sebagaimana dimaksud dalam Pasal 5 ayat (1) huruf g berdasarkan:

a. peta rencana;

b. sasaran Keamanan Informasi; dan

c. hasil Audit Keamanan Informasi.

(2) Evaluasi kinerja Keamanan Informasi sebagaimana dimaksud pada ayat (1) dilaksanakan paling sedikit 1 (satu) kali dalam 1 (satu) tahun dalam bentuk tinjauan manajemen.

(3) Tinjauan manajemen sebagaimana dimaksud pada ayat (2) dilakukan untuk memastikan pencapaian target Keamanan Informasi yang telah direncanakan.

(4) Hasil evaluasi kinerja Keamanan Informasi sebagaimana dimaksud pada ayat (2) didokumentasikan untuk digunakan sebagai bahan evaluasi kinerja Keamanan Informasi berikutnya.

(5) Ketentuan mengenai tata cara evaluasi kinerja Keamanan Informasi sebagaimana dimaksud pada ayat (2) tercantum Lampiran yang merupakan bagian tidak terpisahkan dari Peraturan Wali Kota ini.

Pasal 16

(1) Perangkat Daerah atau unit kerja pemilik aset Informasi bertanggung jawab melaksanakan perbaikan berkelanjutan sebagai tindak lanjut dari hasil evaluasi kinerja Keamanan Informasi sebagaimana dimaksud dalam Pasal 15 ayat (4).

(2) Perbaikan berkelanjutan sebagaimana dimaksud pada ayat (1) paling sedikit dilakukan melalui:

a. mengatasi permasalahan dalam pelaksanaan Keamanan Informasi; dan

b. memperbaiki pelaksanaan Keamanan Informasi secara berkala.

(3) Tindakan perbaikan berkelanjutan yang telah dilakukan sebagaimana dimaksud pada ayat (2) didokumentasikan dan dilaporkan kepada Tim SMKI untuk digunakan sebagai bahan evaluasi kinerja Keamanan Informasi.

(4) Format tindakan perbaikan sebagaimana dimaksud pada ayat (3) tercantum Lampiran yang merupakan bagian tidak terpisahkan dari Peraturan Wali Kota ini.

BAB X

PENDANAAN

Pasal 17

Pendanaan SMKI bersumber dari:

a. anggaran pendapatan dan belanja Daerah; dan/atau

b. sumber lain yang sah dan tidak mengikat.

BAB XI

KETENTUAN PENUTUP

Pasal 18

Pada saat Peraturan Wali Kota ini mulai berlaku, Peraturan Wali Kota Yogyakarta Nomor 113 Tahun 2019 tentang Sistem Manajemen Keamanan Informasi (Berita Daerah Kota Yogyakarta Tahun 2019 Nomor 113), dicabut dan dinyatakan tidak berlaku.

Pasal 19

Peraturan Wali Kota ini mulai berlaku pada tanggal diundangkan.

Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Wali Kota ini dengan penempatannya dalam Berita Daerah Kota Yogyakarta.

Ditetapkan di Yogyakarta
pada tanggal

WALI KOTA YOGYAKARTA,

HASTO WARDOYO

Diundangkan di Yogyakarta
pada tanggal

SEKRETARIS DAERAH KOTA YOGYAKARTA,

AMAN YURIADIJAYA

BERITA DAERAH KOTA YOGYAKARTA TAHUN 2025 NOMOR