SALINAN

WALI KOTA YOGYAKARTA
DAERAH ISTIMEWA YOGYAKARTA

PERATURAN WALI KOTA YOGYAKARTA
NOMOR 64 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 12 Desember 2025

WALI KOTA YOGYAKARTA,

ttd

HASTO WARDOYO

Diundangkan di Yogyakarta
pada tanggal 12 Desember 2025

SEKRETARIS DAERAH KOTA YOGYAKARTA,

ttd

AMAN YURIADIJAYA

BERITA DAERAH KOTA YOGYAKARTA TAHUN 2025 NOMOR 64

LAMPIRAN

PERATURAN WALI KOTA YOGYAKARTA

NOMOR 64 TAHUN 2025

TENTANG

SISTEM MANAJEMEN KEAMANAN INFORMASI

KEBIJAKAN SISTEM MANAJEMEN KEAMANAN INFORMASI

A. Kebijakan Umum SMKI

Kebijakan umum SMKI di lingkungan Pemerintah Daerah adalah sebagai berikut:

1. Informasi merupakan salah satu aset utama dalam bisnis yang diselenggarakan oleh Pemerintah Daerah. Oleh karena itu, kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*) Informasi perlu dikelola sehingga keamanannya dapat terjaga;
2. penerapan SMKI di lingkungan Pemerintah Daerah mengacu pada standar ISO/IEC 27001:2022 dan ketentuan peraturan perundang-undangan;
3. manajemen puncak Pemerintah Daerah menunjukkan kepemimpinan dan komitmen untuk menerapkan SMKI di organisasi;
4. kebijakan Keamanan Informasi harus dikomunikasikan ke seluruh pegawai dan pihak ketiga terkait melalui media komunikasi yang ada agar dipahami dengan mudah dan dipatuhi;
5. Pemerintah Daerah akan selalu berusaha meningkatkan kepedulian, pengetahuan, dan keterampilan tentang Keamanan Informasi bagi karyawan internal maupun pihak eksternal yang terkait;
6. Pemerintah Daerah melaksanakan kajian dan mengelola Risiko terkait Keamanan Informasi berdasarkan kerentanan (*vulnerability*) dan ancaman (*threat*) yang ada pada setiap aset maupun proses;
7. dalam hal terdapat kerentanan dan ancaman yang berpotensi mengganggu Keamanan Informasi, semua pihak yang berkepentingan melaporkan kepada *Chief Information Security Officer* atau anggota Tim SMKI;
8. seluruh pimpinan di semua tingkatan bertanggung jawab memantau dan mengevaluasi efektivitas penerapan kebijakan ini di seluruh unit kerja/bagian di bawah pengawasannya;
9. seluruh pegawai bertanggung jawab untuk menjaga dan melindungi keamanan aset Informasi serta mematuhi kebijakan dan prosedur Keamanan Informasi yang telah ditetapkan;
10. setiap pelanggaran terhadap kebijakan ini dan kebijakan lain yang terkait akan dikenai sanksi administratif seperti pencabutan hak akses sistem Informasi dan/atau tindakan pendisiplinan lain sesuai ketentuan peraturan perundang-undangan; dan
11. Pemerintah Daerah berkomitmen untuk terus melakukan perbaikan berkelanjutan terhadap implementasi SMKI.

Kebijakan dan prosedur yang bersifat lebih teknis akan dibuat secara terpisah dan ditetapkan dengan merujuk pada prinsip yang ditetapkan dalam pernyataan kebijakan ini.

B. Ruang Lingkup

1. Data dan Informasi SPBE

   Data dan Informasi SPBE adalah segala bentuk Data dan Informasi yang dikelola dalam penyelenggaraan SPBE, yang terdiri atas:

   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; dan/atau

   b. non-elektronik, meliputi Informasi yang tercetak, tertulis dan tersimpan dalam bentuk fisik seperti di atas kertas, papan tulis, spanduk atau di dalam buku dan dokumen.

2. Aplikasi SPBE

   Ruang lingkup Aplikasi SPBE meliputi seluruh Aplikasi yang dimiliki, dikembangkan, digunakan, atau dioperasikan oleh Pemerintah Daerah, baik secara mandiri maupun terintegrasi dengan instansi pusat, melalui pemanfaatan Aplikasi khusus untuk mendukung penyelenggaraan pemerintahan berbasis elektronik.

   Aplikasi khusus merupakan Aplikasi yang dikembangkan dan digunakan oleh Pemerintah Daerah sesuai dengan kebutuhan spesifik tugas dan fungsinya. Aplikasi ini dapat digunakan secara internal oleh satu Perangkat Daerah atau oleh beberapa Perangkat Daerah dalam satu Pemerintah Daerah.

   Contoh: SIMPEG daerah, sistem Informasi perizinan daerah, dan/atau Aplikasi layanan bantuan sosial.

3. Infrastruktur SPBE

   Infrastruktur SPBE merupakan bagian penting dalam penyelenggaraan SPBE, karena berperan menjaga keberlangsungan layanan digital pemerintahan agar dapat berjalan secara optimal.

   Pada tingkat Pemerintah Daerah, Infrastruktur mencakup:

   a. jaringan intra Pemerintah Daerah, yang mendukung pertukaran Data internal antar unit organisasi secara aman dan efisien; dan

   b. sistem penghubung layanan Pemerintah Daerah, yang digunakan untuk interkoneksi dan integrasi layanan SPBE antar instansi sesuai dengan prinsip interoperabilitas.

4. Sumber Daya Manusia SPBE

   Sumber daya manusia SPBE Pemerintah Daerah harus memiliki kompetensi teknis yang sesuai dengan kebutuhan pelaksanaan Keamanan Informasi dalam penyelenggaraan SPBE, meliputi:

   a. keamanan Infrastruktur SPBE, yaitu kemampuan dalam merancang, mengelola, dan melindungi Infrastruktur TIK yang digunakan oleh Pemerintah Daerah; dan

b. keamanan Aplikasi, yaitu kemampuan untuk memastikan keamanan pada seluruh siklus hidup Aplikasi, mulai dari tahap perancangan, pengembangan, pengujian, hingga pemeliharaan Aplikasi yang digunakan dalam penyelenggaraan SPBE.

Dalam hal sumber daya manusia SPBE yang tersedia belum memiliki kompetensi yang memadai, Sekretaris Daerah selaku Koordinator SPBE melaksanakan langkah strategis sebagai berikut:

a. memfasilitasi peningkatan kompetensi melalui kegiatan pelatihan, sertifikasi profesi, dan/atau bimbingan teknis yang sesuai dengan standar kompetensi kerja nasional maupun internasional di bidang Keamanan Informasi; dan/atau

b. memfasilitasi penyelenggaraan kegiatan kesadaran Keamanan Informasi (*security awareness*) secara berkala bagi seluruh pegawai di lingkungan Pemerintah Daerah untuk menanamkan budaya Keamanan Informasi.

C. Kendali Keamanan

1. Keamanan Sumber Daya Manusia

Keamanan sumber daya manusia dilakukan untuk mengendalikan sumber daya manusia dalam melaksanakan kebijakan SMKI. Keamanan sumber daya manusia di Pemerintah Daerah dilaksanakan oleh Tim SMKI bekerja sama dengan unit kerja terkait, dengan cara sebagai berikut namun tidak terbatas pada:

a. mengomunikasikan peran dan tanggung jawab pelaksanaan kebijakan SMKI kepada seluruh pegawai dan pihak ketiga yang terlibat dalam pengelolaan dan pengamanan aset Informasi;

b. melakukan pembagian tugas dan wewenang (*segregation of duty*) untuk menghindari kesalahan atau pelanggaran;

c. melakukan pemeriksaan Data pribadi pegawai dan pihak ketiga yang terlibat dalam pengelolaan dan pengamanan aset Informasi;

d. membuat perjanjian tertulis dengan pegawai dan pihak ketiga yang terlibat dalam penggunaan dan/atau pengelolaan Informasi yang menyatakan tanggung jawab terhadap Keamanan Informasi dan sanksi atas pelanggaran Keamanan Informasi;

e. menghentikan hak penggunaan aset Informasi bagi pegawai yang sedang dalam pemeriksaan terkait dengan dugaan pelanggaran Keamanan Informasi;

f. mencabut hak akses ke aset Informasi yang dimiliki pegawai dan pihak ketiga apabila yang bersangkutan tidak lagi memiliki kepentingan terhadap aset Informasi, dimutasi, atau tidak lagi bekerja di Pemerintah Daerah;

g. membuat berita acara serah terima terkait penerimaan seluruh aset Informasi yang dipergunakan selama bekerja dan pengembalian seluruh aset Informasi bagi pegawai yang berhenti bekerja atau mutasi;

h. memberikan edukasi kesadaran Keamanan Informasi melalui kegiatan sosialisasi, bimbingan teknis, dan/atau pelatihan mengenai Keamanan Informasi yang dilaksanakan secara berkala; dan

i. memelihara catatan pelatihan, kompetensi, pengalaman, dan kualifikasi pegawai yang mengelola Keamanan Informasi.

2. Keamanan Aset Informasi

Keamanan aset Informasi dilakukan untuk mengamankan aset Informasi di Pemerintah Daerah berdasarkan tingkat kekritisannya. Keamanan aset Informasi di Pemerintah Daerah dilakukan oleh Tim SMKI bekerja sama dengan unit kerja terkait, dengan cara sebagai berikut namun tidak terbatas pada:

a. mengidentifikasi aset Informasi dan mendokumentasikannya dalam daftar inventaris aset Informasi yang memuat tingkat kekritisan dan penanggung jawab setiap aset;

b. memberikan label sesuai tingkat kekritisan;

c. menetapkan pihak yang dapat mengakses aset Informasi;

d. menetapkan aturan penggunaan aset Informasi;

e. menempatkan aset Informasi di lokasi yang aman guna mengurangi Risiko aset Informasi dapat diakses oleh pihak yang tidak berwenang;

f. penggunaan aset yang dibawa ke luar dari lingkungan pusat Data atau tempat layanan Informasi harus disetujui oleh Kepala Perangkat Daerah yang menyelenggarakan urusan pemerintahan di bidang komunikasi, informatika dan persandian;

g. perangkat penyimpanan Data yang sudah tidak digunakan lagi harus disanitasi sebelum digunakan kembali atau dimusnahkan;

h. pemusnahan perangkat penyimpanan Data harus dilakukan secara aman sesuai Prosedur Pemusnahan Perangkat Penyimpanan; dan

i. melaksanakan manajemen aset TIK sesuai dengan ketentuan manajemen aset TIK yang ditetapkan oleh kementerian yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika.

3. Keamanan Akses

Keamanan akses dilakukan untuk mengendalikan akses ke aset Informasi yaitu memastikan perangkat pengguna yang terhubung ke aset Informasi mendapatkan perlindungan keamanan dan tidak diakses oleh pihak yang tidak berhak. Keamanan akses terhadap aset Informasi di Pemerintah Daerah dilakukan oleh Tim SMKI bekerja sama dengan unit kerja terkait, dengan cara sebagai berikut namun tidak terbatas pada:

a. menyusun prosedur pengelolaan hak akses pengguna yang berisi ketentuan akses ke aset Informasi sesuai dengan kebutuhan organisasi, persyaratan keamanan, dan ketentuan peraturan perundang-undangan;

b. mengelola akses pengguna dengan cara:

1. menggunakan akun yang unik untuk setiap pengguna;

2. memeriksa tingkat akses yang diberikan sesuai dengan tujuan penggunaan;

3. membatasi dan mengendalikan penggunaan hak akses khusus (jika ada);

4. mengatur pengelolaan kata sandi pengguna sesuai dengan ketentuan pengelolaan kata sandi di Pemerintah Daerah;

5. memantau dan mengevaluasi hak akses pengguna dan penggunaannya secara berkala untuk memastikan kesesuaian status pemakaiannya;
6. memelihara catatan pengguna layanan (*user log*);
7. menonaktifkan akses pengguna yang telah berakhir penugasannya; dan
8. memantau dan mengevaluasi akun dan hak akses secara berkala paling sedikit 1 (satu) kali dalam 6 (enam) bulan;

c. mengendalikan akses ke jaringan dan layanan jaringan Informasi dengan cara;
1. menerapkan prosedur otorisasi pemberian akses ke jaringan dan layanan jaringan untuk setiap akses ke dalam jaringan internal;
2. akses ke Infrastruktur dan Aplikasi yang digunakan untuk melakukan diagnosa harus dikendali dan hanya digunakan untuk pegawai yang bertugas untuk melakukan pengujian, pemecahan masalah, serta pengembangan sistem;
3. memisahkan jaringan untuk pengguna, sistem Informasi, dan layanan Informasi;
4. memberikan akses jaringan kepada tamu hanya untuk akses terbatas dan waktu tertentu; dan
5. melakukan penghentian layanan jaringan pada area jaringan yang mengalami gangguan Keamanan Informasi;

d. mengendalikan akses ke Aplikasi dan sistem Informasi dengan cara:
1. akses terhadap Aplikasi dan sistem Informasi hanya diberikan kepada pengguna sesuai dengan peruntukannya dan dikendali dengan menggunakan sistem manajemen akses pengguna;
2. setiap pengguna wajib memiliki akun yang unik dan hanya digunakan sesuai dengan peruntukannya dan proses otorisasi pengguna wajib menggunakan teknik otentikasi yang sesuai untuk memvalidasi identitas pengguna;
3. menggunakan sistem pengelolaan kata sandi sesuai dengan ketentuan pengelolaan kata sandi di Pemerintah Daerah untuk memastikan kualitas kata sandi yang dibuat pengguna;
4. fasilitas *session time-out* wajib diaktifkan untuk menutup dan mengunci layar komputer, Aplikasi, dan koneksi jaringan apabila tidak ada aktivitas pengguna setelah periode tertentu;
5. membatasi waktu koneksi untuk sistem Informasi dan Aplikasi yang memiliki klasifikasi rahasia dan/atau sangat rahasia; dan
6. akses ke kode sumber Aplikasi dibatasi secara ketat diperuntukkan hanya bagi pihak yang sah dan berkepentingan melalui hak akses khusus;

e. mengendalikan perangkat kerja jarak jauh dengan cara menentukan parameter keamanan yang harus dipenuhi oleh perangkat kerja jarak jauh yang digunakan dalam mengakses aset Informasi, yang terdiri dari namun tidak terbatas pada:
1. *virtual private network*;
2. *secure socket layer*; dan/atau

3. *two step authentication*;

f. hak akses khusus dapat dibuat untuk mengakses sistem Informasi berklasifikasi rahasia pada sistem operasi, perangkat penyimpanan (*storage devices*), *file server*, dan Aplikasi sensitif, dengan cara:

1. mengidentifikasi hak akses khusus untuk dialokasikan kepada pengguna terkait;
2. memberikan hak akses khusus hanya kepada pengguna sesuai dengan peruntukannya berdasarkan kebutuhan dan kegiatan tertentu;
3. mengelola proses otorisasi dan catatan dari seluruh hak akses khusus; dan
4. memberikan hak akses khusus secara terpisah dari akun yang digunakan untuk kegiatan lainnya;

g. melakukan pemantauan terhadap akses ke aset Informasi meliputi:

1. kegagalan akses;
2. penggunaan hak akses tidak wajar;
3. alokasi dan penggunaan hak akses khusus;
4. penelusuran transaksi pengiriman file sistem atau dokumen tertentu yang mencurigakan; dan
5. penggunaan sumber daya sensitif;

h. menghapus akun setiap pegawai dan pihak ketiga yang tidak lagi memiliki kepentingan terhadap akses aset Informasi, dimutasi, berhenti, atau telah berakhir kontraknya.

4. Keamanan Kriptografi

Keamanan kriptografi untuk memastikan penggunaan kriptografi yang tepat untuk melindungi kerahasiaan, keutuhan, dan keotentikan Data dan Informasi rahasia dan/atau sangat rahasia yang dikelola dalam perangkat Informasi. Keamanan kriptografi untuk Informasi rahasia dan/atau sangat rahasia dilaksanakan oleh Tim SMKI bekerja sama dengan unit kerja terkait, dengan cara sebagai berikut namun tidak terbatas pada:

a. melakukan klasifikasi Informasi yang disimpan dan dikelola dalam perangkat Informasi sesuai dengan ketentuan peraturan perundang-undangan;

b. menerapkan keamanan kriptografi untuk Informasi berklasifikasi rahasia dan/atau sangat rahasia dengan cara sebagai berikut namun tidak terbatas pada:

1. menerapkan jalur komunikasi aman dengan menerapkan *secure socket layer* untuk proses otentikasi antara pengguna dengan Aplikasi berbasis *website*;
2. menjaga kerahasiaan kata sandi dan menyimpannya dalam basis Data dengan mekanisme *hash function*;
3. melindungi kerahasiaan Data dan Informasi rahasia dan/atau sangat rahasia yang dipertukarkirimkan dan disimpan dalam basis Data dengan melakukan enkripsi;

4. menerapkan otentikasi berbasis tanda tangan digital dengan menggunakan Sertifikat Elektronik yang dikeluarkan oleh pihak ketiga terpercaya; dan
5. menggunakan algoritma kriptografi, modul kriptografi, protokol kriptografi, dan kunci kriptografi sesuai dengan peraturan perundangan dan/atau rekomendasi dari lembaga yang melaksanakan tugas pemerintahan di bidang keamanan siber.

5. Keamanan Fisik dan Lingkungan

Keamanan fisik dan lingkungan dilakukan untuk memberikan pelindungan, pemeliharaan, keamanan, dan ketersediaan aset Informasi. Keamanan fisik dan lingkungan dilaksanakan oleh Tim SMKI bekerja sama dengan unit kerja terkait, dengan cara sebagai berikut namun tidak terbatas pada:

a. menyimpan Infrastruktur di ruangan khusus yang dilindungi dengan pengamanan fisik yang memadai antara lain namun tidak terbatas pada:
   1. pintu dengan kendali akses;
   2. kamera pengawas;
   3. pendeteksi asap;
   4. sistem pemadam kebakaran; dan
   5. perangkat pemutus aliran listrik;
b. akses ke pusat Data dan/atau area kerja layanan Informasi yang berisi Data dan/atau Informasi rahasia dan/atau sangat rahasia harus dibatasi dan hanya diberikan kepada pegawai yang memiliki akses;
c. pihak ketiga yang memasuki pusat Data dan/atau area kerja layanan Informasi yang berisikan Data dan/atau Informasi rahasia dan/atau sangat rahasia harus didampingi oleh pegawai yang ditugaskan sepanjang waktu kunjungan;
d. makanan dan minuman dilarang untuk dibawa masuk ke atau dikonsumsi di dalam ruang server pusat Data;
e. semua area yang digunakan untuk menyimpan aset Informasi merupakan area bebas rokok;
f. batas minimum dan maksimum suhu dan kelembaban di dalam ruang server pusat Data harus memenuhi standar yang disyaratkan pabrikan perangkat dan senantiasa dilakukan pengawasan terhadap kondisi suhu dan kelembaban;
g. pengamanan area pusat Data dan area kerja layanan Informasi dilakukan sesuai prosedur keamanan area;
h. pengamanan kantor, ruangan, dan fasilitas kerja sesuai dengan peraturan dan standar keamanan dan keselamatan kerja, termasuk *clear screen policy* dan *clean desk policy*;
i. Infrastruktur yang digunakan untuk menjalankan Aplikasi dipelihara sesuai dengan buku petunjuk;

j. dalam hal pemeliharaan Infrastruktur tidak dapat dilakukan di tempat, maka pemindahan Infrastruktur dilakukan berdasarkan persetujuan Kepala Perangkat Daerah yang menyelenggarakan urusan pemerintahan di bidang komunikasi, informatika dan persandian;

k. dalam hal pemindahan Infrastruktur terdapat Data dan/atau Informasi berklasifikasi rahasia dan/atau sangat rahasia yang tersimpan pada perangkat tersebut, maka Data dan/atau Informasi berklasifikasi rahasia dan/atau sangat rahasia tersebut harus dipindahkan terlebih dahulu ke dalam media penyimpanan lain;

l. dalam hal pemeliharaan dilakukan oleh pihak ketiga, maka pelaksanaannya dilakukan dengan membuat perjanjian kerja sama yang paling sedikit memuat perjanjian menjaga kerahasiaan, pemeliharaan yang disediakan, dan tingkat kinerja yang harus dipenuhi pihak ketiga;

m. Infrastruktur beserta perangkat pemulihan dan media penyimpanan Data cadangan wajib diletakkan di tempat yang aman dengan struktur yang memadai untuk menghindari kerusakan dari hama (misal: tikus, semut dan rayap) dan bencana (misal: banjir dan gempa);

n. semua Infrastruktur harus mendapatkan pasokan daya yang sesuai dengan spesifikasi yang diisyaratkan oleh pabrikan Infrastruktur;

o. pasokan listrik yang digunakan untuk mengoperasikan Infrastruktur harus mempunyai sumber alternatif dengan daya dan jangka waktu ketersediaan atau jangka waktu pengoperasian yang cukup, yang paling sedikit mencakup generator listrik dan *uniterruptable power supply* dengan daya yang cukup dan dengan konfigurasi yang dapat memindahkan pasokan listrik tanpa gangguan terhadap Infrastruktur;

p. bahan berbahaya atau mudah terbakar di lingkungan Pemerintah Daerah wajib disimpan pada jarak yang aman dari pusat Data dan area kerja layanan Informasi;

q. perangkat pemadam kebakaran wajib disediakan, dipelihara, dan diletakkan di tempat yang mudah dijangkau;

r. Infrastruktur diletakkan pada lokasi yang meminimalisasi akses pihak yang tidak berwenang;

s. Infrastruktur yang menangani Informasi sensitif diposisikan dan dibatasi sudut pandangnya untuk mengurangi Risiko Informasi dilihat oleh pihak tidak berwenang;

t. perlindungan petir harus diterapkan untuk semua bangunan, jalur komunikasi dan listrik; dan

u. pengamanan kabel di pusat Data dan/atau area kerja layanan Informasi dilakukan dengan mengikuti standar mekanikal/elektrikal pusat Data yang berlaku.

6. Keamanan Operasional

Keamanan operasional dilakukan untuk memastikan implementasi, operasional, dan pemeliharaan yang aman dari aset Informasi, pengelolaan layanan oleh pihak ketiga, meminimalkan Risiko kegagalan, dan melindungi keutuhan dan ketersediaan aset Informasi. Keamanan operasional di Pemerintah Daerah dilakukan oleh Tim SMKI bekerja sama dengan unit kerja terkait, dengan cara sebagai berikut namun tidak terbatas pada:

a. mendokumentasikan, memelihara, dan menyediakan prosedur penggunaan perangkat Informasi sesuai dengan peruntukannya;

b. perubahan pada aset Informasi yang dapat mempengaruhi Keamanan Informasi harus didokumentasikan dan dikendalikan dengan memperhatikan Manajemen Risiko dan persetujuan dari pemilik aset Informasi;

c. menetapkan kriteria penerimaan untuk sistem Informasi baru, pemutakhiran dan versi baru serta melakukan pengujian sebelum penerimaan;

d. memantau penggunaan aset Informasi yang dimiliki dan membuat proyeksi kebutuhan ke depan untuk menjamin ketersediaan aset Informasi yang dibutuhkan. Untuk aset Informasi yang kritikal harus senantiasa dimonitor dan dievaluasi kapasitas dan ketersediaannya;

e. melakukan pemisahan akses terhadap Informasi yang memiliki klasifikasi rahasia dan/atau sangat rahasia (seorang pegawai dihindari memiliki akses terhadap seluruh aset Informasi dan perangkat pengolahnya);

f. memisahkan lingkungan pengembangan, pengujian, dan operasional untuk mengurangi Risiko perubahan atau akses oleh pihak yang tidak berhak terhadap sistem operasional;

g. menerapkan sistem pendeteksian, pencegahan, dan pemulihan sebagai bentuk perlindungan terhadap ancaman *malware*;

h. perlindungan dilakukan dengan cara pemasangan paling sedikit meliputi:

   1. perangkat *firewall*;
   2. perangkat *intrusion prevention system*;
   3. perangkat antivirus;
   4. perangkat manajemen akses pengguna; dan
   5. perangkat monitoring/pendukung lainnya sesuai perkembangan teknologi Keamanan Informasi;

i. melakukan pembuatan *backup* Informasi dan Aplikasi yang berada di pusat Data dan/atau area kerja layanan Informasi secara berkala sesuai dengan prosedur *backup* di Pemerintah Daerah;

j. salinan cadangan Data/Informasi, Aplikasi, dan *image sistem* harus diambil dan diuji secara berkala;

k. mencatat (*logging*) setiap aktivitas administrator, aktivitas pengguna, peristiwa kegagalan, dan kejadian keamanan serta disimpan dalam periode tertentu;

l. melindungi sistem pencatatan (*log*) dari pemalsuan dan akses yang tidak berwenang;

m. melakukan penilaian kerentanan terhadap perangkat Informasi (*vulnerability assessment*) secara berkala dan melakukan tindakan perlindungan terhadap kerentanan dan/atau ancaman yang teridentifikasi;

n. menerapkan pencatatan kesalahan untuk dianalisis dan diambil tindak pengamanan yang tepat;

o. memastikan semua perangkat pengolah Informasi yang tersambung dengan jaringan telah disinkronisasi dengan sumber waktu yang akurat dan disepakati; dan

p. menerapkan audit terhadap *log* yang mencatat aktivitas pengguna dan kejadian Keamanan Informasi dalam kurun waktu tertentu untuk membantu investigasi di masa mendatang, antara lain:

   1. kegagalan akses;
   2. penggunaan hak akses tidak wajar;
   3. alokasi dan penggunaan hak akses khusus;
   4. penelusuran transaksi pengiriman file sistem atau dokumen tertentu yang mencurigakan; dan
   5. penggunaan sumber daya sensitif.

7. Keamanan Komunikasi

   Keamanan komunikasi dilakukan untuk memastikan keamanan pertukaran Informasi melalui jaringan komunikasi. Keamanan komunikasi di Pemerintah Daerah dilakukan oleh Tim SMKI bekerja sama dengan unit kerja terkait, dengan cara sebagai berikut namun tidak terbatas pada:

   a. Tim SMKI mengidentifikasi fitur keamanan layanan, tingkat layanan, dan kebutuhan pengelolaan dalam kesepakatan penyediaan layanan jaringan termasuk layanan jaringan yang disediakan oleh pihak ketiga;

   b. dalam hal pihak ketiga diizinkan mengakses ke jaringan, maka dilakukan pemantauan serta pencatatan kegiatan selama menggunakan jaringan;

   c. melindungi jaringan dari pihak yang tidak berhak mengakses, paling sedikit dengan cara:

      1. mendokumentasikan arsitektur jaringan yang meliputi seluruh komponen Infrastruktur dan Aplikasi jaringan;
      2. menerapkan teknologi keamanan jaringan berbasis enkripsi dan otentikasi (termasuk Sertifikat Elektronik);
      3. menerapkan pemisahan jaringan untuk kelompok pengguna, layanan Informasi, dan sistem Informasi;
      4. menerapkan parameter teknis yang diperlukan untuk koneksi aman dengan layanan jaringan; dan
      5. menerapkan prosedur penggunaan layanan jaringan yang membatasi akses ke layanan jaringan atau Aplikasi;

   d. menerapkan mekanisme kriptografi untuk melindungi Informasi yang terdapat dalam Aplikasi yang melewati jaringan publik dari upaya pengungkapan, modifikasi, dan perusakan;

e. melakukan pendeteksian dan perlindungan terhadap kode berbahaya (*malicious code*) yang disisipkan pada file yang dikirim melalui Sistem Elektronik;

f. memberikan perlindungan kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan untuk Informasi elektronik berklasifikasi rahasia dan/atau sangat rahasia; dan

g. menetapkan Prosedur Pertukaran Informasi yang mengatur sistem dan keamanan yang digunakan untuk pertukaran Informasi.

8. Keamanan Pengembangan dan Pemeliharaan

Keamanan pengembangan dan pemeliharaan sistem dilakukan untuk memastikan bahwa Keamanan Informasi merupakan bagian yang terintegrasi dalam daur hidup aset Informasi untuk mencegah terjadinya kesalahan, eksploitasi, modifikasi, dan perusakan aset Informasi oleh pihak yang tidak berwenang. Keamanan pengembangan dan pemeliharaan di Pemerintah Daerah dilakukan oleh Tim SMKI bekerja sama dengan unit kerja terkait, dengan cara sebagai berikut namun tidak terbatas pada:

a. lingkungan pengembangan, pengujian, dan operasional Aplikasi harus dipisahkan baik secara fisik, *logic*, maupun aksesnya;

b. menjaga agar lingkungan pengembangan tidak boleh diakses dari sistem operasional layanan;

c. mengupayakan lingkungan pengujian sama dengan lingkungan operasional layanan;

d. memilih Data uji dengan hati-hati, melindungi, dan mengendalikannya;

e. mengawasi dan memantau aktivitas pembangunan/pengembangan Aplikasi dan Infrastruktur yang dialihdayakan pada pihak ketiga;

f. memastikan bahwa dalam proses perencanaan dan pembangunan/pengembangan Aplikasi dan Infrastruktur termasuk yang dilakukan oleh pihak ketiga, telah memasukkan fitur keamanan dalam spesifikasi Aplikasi dan Infrastruktur yang dibangun/dikembangkan;

g. fitur keamanan yang dimasukkan harus sesuai dengan standar keamanan yang relevan dan paling sedikit memenuhi standar yang ditetapkan oleh lembaga yang melaksanakan tugas pemerintahan di bidang keamanan siber, yang meliputi:

   1. standar keamanan Data dan Informasi;
   2. standar keamanan Aplikasi;
   3. standar keamanan pusat Data;
   4. standar keamanan sistem penghubung layanan; dan
   5. standar keamanan jaringan intra;

h. melaksanakan uji kelaikan Aplikasi sebelum Aplikasi digunakan dan sewaktu-waktu sesuai kebutuhan, yang mencakup aspek:

   1. uji fungsi, dilakukan untuk memastikan Aplikasi yang dibangun dan/atau dikembangkan telah memenuhi fungsi sesuai dengan dokumentasi terkait;

2. uji integrasi, dilakukan untuk yang memastikan Aplikasi yang dibangun dan/atau dikembangkan telah memenuhi kebutuhan dan persyaratan integrasi dengan Aplikasi, Data, serta komponen lain yang terkait;
3. uji beban, dilakukan untuk yang memastikan Aplikasi yang dibangun dan/atau dikembangkan dapat berfungsi sebagaimana mestinya menghadapi beban kerja yang dikenakan terhadapnya; dan
4. uji keamanan, dilakukan untuk memastikan Aplikasi yang dibangun dan/atau dikembangkan dapat menjaga keamanan Data dan Informasi yang terkait dengannya;

i. uji kelaikan pada aspek uji fungsi, uji integrasi, dan uji beban dapat menggunakan pedoman/instrumen pengukuran yang ditetapkan oleh kementerian yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika;

j. uji kelaikan pada aspek uji keamanan dapat menggunakan pedoman/instrumen pengukuran yang ditetapkan oleh lembaga yang melaksanakan tugas pemerintahan di bidang keamanan siber; dan

k. pelaksanaan pembangunan dan pengembangan Aplikasi dilakukan sesuai dengan standar teknis dan prosedur pembangunan dan pengembangan Aplikasi yang ditetapkan oleh kementerian yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika.

9. Keamanan Pihak Ketiga

Keamanan pihak ketiga dilakukan untuk memastikan perlindungan dari aset Informasi yang dapat diakses oleh pihak ketiga. Keamanan pihak ketiga di Pemerintah Daerah dilakukan oleh Tim SMKI bekerja sama dengan unit kerja terkait, dengan cara sebagai berikut namun tidak terbatas pada:

a. melakukan pemeriksaan latar belakang pihak ketiga dengan tetap memperhatikan privasi dan perlindungan Data pribadi;

b. membuat dan meninjau ulang secara berkala perjanjian keamanan dengan pihak ketiga yang terlibat dalam penggunaan dan/atau pengelolaan aset Informasi yang menyatakan tanggung jawab terhadap keamanan aset Informasi. Perjanjian keamanan sebagaimana dimaksud dibuat secara tertulis paling sedikit memuat:

1. perlindungan atas Informasi rahasia dan/atau sangat rahasia dan hak kekayaan intelektual setiap pihak;
2. dalam hal aset Informasi disediakan oleh pihak ketiga, maka adanya jaminan bahwa tidak terdapat *malicious code* dan *backdoor*;
3. hak untuk melakukan audit dan memantau kegiatan yang melibatkan Informasi rahasia dan/atau sangat rahasia;
4. pengawasan atas akses terhadap aset Informasi yang diberikan pada pihak ketiga;
5. pelaporan terhadap penyingkapan yang dilakukan secara tidak sah atau pelanggaran terhadap kerahasiaan;
6. syarat untuk Informasi yang akan dikembalikan atau dimusnahkan pada saat penghentian perjanjian;

7. penggunaan jalur komunikasi yang aman untuk perpindahan Informasi antara Pemerintah Daerah dengan pihak ketiga; dan
8. dalam hal pihak ketiga tidak lagi menjadi bagian dalam pengelolaan aset Informasi, maka aset Informasi yang dikuasainya diserahkan kembali kepada Tim SMKI;

c. memastikan secara berkala bahwa pengendalian Keamanan Informasi, definisi layanan, dan tingkat layanan yang termuat dalam kesepakatan penyediaan layanan, telah diterapkan, dioperasikan, dan dipelihara oleh pihak ketiga;

d. memastikan *service level agreement* pihak ketiga telah mengatur ketersediaan layanan dan penyelesaian insiden keamanan;

e. melakukan pemantauan terhadap kinerja penyediaan layanan, laporan, dan catatan yang disediakan oleh pihak ketiga secara berkala;

f. memperhatikan tingkat kekritisan, proses yang terkait dan hasil penilaian ulang Risiko layanan apabila terjadi perubahan pada layanan yang disediakan oleh pihak ketiga;

g. mencatat peristiwa keamanan, masalah operasional, kegagalan, dan gangguan yang terkait dengan layanan yang diberikan oleh pihak ketiga;

h. memberikan Informasi tentang gangguan keamanan dan mengkaji Informasi bersama pihak ketiga;

i. mencabut hak akses terhadap akses Informasi yang dimiliki pihak ketiga apabila yang bersangkutan tidak lagi bekerja di Pemerintah Daerah;

j. membuat berita acara serah terima terkait mengembalikan seluruh aset Informasi yang dipergunakan selama bekerja bagi pihak ketiga yang berakhir masa kontraknya; dan

k. memastikan pihak ketiga dan tamu yang memasuki lingkungan pusat Data, dan tempat layanan Informasi harus mematuhi standar keamanan fisik dan lingkungan.

10. Manajemen Insiden Siber

Manajemen Insiden Siber dilaksanakan untuk mengendalikan Insiden Siber. Manajemen Insiden Siber di Pemerintah Daerah dilakukan oleh Tim SMKI bekerja sama dengan unit kerja terkait, dengan cara sebagai berikut namun tidak terbatas pada:

a. membentuk Tim Tanggap Insiden Siber yang bertugas melakukan pencegahan dan penanganan Insiden Siber yang terjadi di Pemerintah Daerah;

b. Tim Tanggap Insiden Siber melakukan tindakan pencegahan Insiden Siber paling sedikit meliputi:

1. melakukan penilaian kerentanan dan/atau *penetration testing* untuk menemukan celah keamanan pada aset Informasi;
2. mengimplementasikan alat monitoring keamanan berupa *security information and event management*; dan
3. melakukan monitoring dan pendeteksian serangan terhadap aset Informasi;

c. dalam hal terjadi Insiden Siber, Tim Tanggap Insiden Siber melaksanakan prosedur penanganan Insiden Siber paling sedikit meliputi:

1. menerima laporan dan mencatat Insiden Siber;
2. melakukan triase Insiden Siber;
3. mengidentifikasi sumber serangan;
4. menganalisis Informasi yang berkaitan dengan Insiden Siber;
5. memprioritaskan penanganan insiden berdasarkan tingkat dampak;
6. memelihara artefak digital untuk keperluan investigasi;
7. menyusun laporan penanganan Insiden Siber; dan
8. mengevaluasi dan memperbaiki standar, prosedur, dan kendali-kendali Keamanan Informasi agar Insiden Siber serupa tidak terulang kembali di masa mendatang;

d. menyusun berbagai macam skenario penanganan Insiden Siber;

e. melakukan simulasi secara berkala skenario penanganan Insiden Siber yang telah disusun;

f. memberikan pelatihan terhadap sumber daya manusia yang terlibat pada penanganan Insiden Siber sesuai skenario yang disusun;

g. menjalankan program kesadaran ancaman dan penanganan Insiden Siber, serta ajakan peran aktif pada seluruh pegawai;

h. memastikan tersedianya kontak pelaporan Insiden Siber yang dapat diakses oleh seluruh pegawai di Pemerintah Daerah termasuk oleh pihak ketiga; dan

i. melakukan pengukuran tingkat kematangan penanganan Insiden Siber secara berkala yang sesuai dengan lembaga yang melaksanakan tugas pemerintahan di bidang keamanan siber.

11. Manajemen Keberlangsungan Layanan Informasi

Manajemen keberlangsungan layanan Informasi dilakukan untuk menjamin ketersediaan layanan Informasi pada saat terjadi keadaan darurat. Manajemen keberlangsungan layanan Informasi dilakukan oleh Tim SMKI bekerja sama dengan unit kerja terkait, dengan cara sebagai berikut namun tidak terbatas pada:

a. melakukan identifikasi Risiko terhadap keberlangsungan layanan Informasi;

b. menyusun dan menerapkan rencana keberlangsungan layanan Informasi (*business continuity planning*) untuk menjaga dan mengembalikan operasional aset Informasi dalam jangka waktu yang disepakati dan tingkat keberlangsungan yang dibutuhkan, yang paling sedikit meliputi:

1. prosedur keberlangsungan layanan Informasi pada saat keadaan darurat, Manajemen Risiko, analisis dampak kegiatan, pengembalian kondisi sebelum terjadi gangguan peralihan kondisi normal, dan uji coba keberlangsungan kegiatan;
2. penetapan peran dan penanggung jawab pegawai yang terlibat dalam pelaksanaan keberlangsungan layanan Informasi; dan

3. pelaksanaan sosialisasi dan pelatihan keberlangsungan layanan Informasi;

c. dalam hal Aplikasi merupakan Aplikasi umum dan/atau Sistem Elektronik berkategori strategis, maka harus memiliki redundansi yang cukup untuk memenuhi ketersediaan layanan Informasi;

d. melakukan uji coba rencana keberlangsungan layanan Informasi secara berkala; dan

e. pelaksanaan pengelolaan layanan dilakukan sesuai dengan pedoman manajemen layanan SPBE yang ditetapkan oleh kementerian yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika.

12. Pengendalian Kepatuhan

Pengendalian kepatuhan dilaksanakan untuk memastikan kepatuhan pegawai dan pihak ketiga dalam melaksanakan Keamanan Informasi sesuai dengan ketentuan peraturan perundang-undangan, kontrak dan keselarasan dengan kebijakan Keamanan Informasi yang berlaku di Pemerintah Daerah. Pengendalian kepatuhan Keamanan Informasi di Pemerintah Daerah dilakukan oleh Tim SMKI bekerja sama dengan unit kerja terkait, dengan cara sebagai berikut namun tidak terbatas pada:

a. mengidentifikasi, mendokumentasikan, mereviu, dan memelihara regulasi, standar, dan prosedur Keamanan Informasi;

b. memeriksa kepatuhan seluruh pegawai dan pihak ketiga terhadap regulasi, standar, dan prosedur Keamanan Informasi;

c. mendapatkan Aplikasi hanya melalui sumber yang dikenal dan memiliki reputasi baik untuk memastikan tidak ada pelanggaran hak cipta;

d. memeriksa kepatuhan penggunaan lisensi Aplikasi dan menerapkan pengendalian untuk memastikan jumlah pengguna tidak melampaui lisensi yang dimiliki;

e. memelihara bukti kepemilikan lisensi, *master disk*, buku manual, dan lain sebagainya;

f. melakukan pemeriksaan bahwa tidak ada produk bajakan yang terinstal (pelanggaran hak kekayaan intelektual) di Pemerintah Daerah;

g. memastikan rekaman terlindungi dari kehilangan, kerusakan, pemalsuan, akses tidak sah, dan rilis tidak sah sesuai dengan persyaratan peraturan perundang-undangan, kontraktual, dan bisnis;

h. memastikan pengamanan privasi dan Data pribadi yang dapat diidentifikasikan sesuai dengan persyaratan ketentuan peraturan perundang-undangan;

i. memastikan kesesuaian penerapan kriptografi dengan ketentuan peraturan perundang-undangan; dan

j. mereviu sistem Informasi secara berkala agar sesuai dengan kebijakan dan standar Keamanan Informasi di Pemerintah Daerah.

D. Tata Cara Audit Internal Keamanan Informasi

Pelaksanaan Audit Internal Keamanan Informasi dilaksanakan dengan ketentuan sebagai berikut:

1. Aparat Pengawas Intern Pemerintah merencanakan, menetapkan, dan menjalankan program audit sesuai dengan pedoman Audit Internal Keamanan Informasi;
2. program audit minimal mencakup frekuensi, metode, kriteria, lingkup, tanggung jawab, dan pelaporan audit, serta mempertimbangkan pentingnya proses yang sedang berjalan dan hasil audit sebelumnya;
3. Audit Internal Keamanan Informasi dilaksanakan paling sedikit 1 (satu) kali dalam 2 (dua) tahun dan dimasukkan dalam peta rencana SPBE Pemerintah Daerah;
4. Audit Internal Keamanan Informasi dilaksanakan oleh Auditor yang memiliki kompetensi memadai dan memiliki objektivitas serta imparsialitas (ketidakberpihakan) dalam melaksanakan Audit Internal Keamanan Informasi;
5. setiap temuan audit harus dicatat secara formal oleh Auditor dan diberikan kepada Auditee;
6. Auditee harus melakukan perbaikan terhadap setiap temuan yang diberikan oleh Auditor dalam jangka waktu yang disepakati;
7. laporan hasil audit Keamanan Informasi dilaporkan kepada Tim SMKI dan Koordinator SPBE sebagai bahan evaluasi penerapan kebijakan SMKI;
8. menyimpan dan mendokumentasikan proses dan hasil audit internal sebagai alat bukti dari program audit; dan
9. pelaksanaan Audit Internal Keamanan Informasi dapat menggunakan instrumen penilaian Audit Keamanan SPBE yang ditetapkan oleh Kepala lembaga yang melaksanakan tugas pemerintahan di bidang keamanan siber.

E. Tata Cara Evaluasi Kinerja Keamanan Informasi

Pelaksanaan evaluasi kinerja Keamanan Informasi secara berkala oleh Koordinator SPBE bersama Tim SMKI untuk memastikan pencapaian sasaran dan efektivitas penerapan SMKI di lingkungan Pemerintah Daerah, dengan ketentuan sebagai berikut namun tidak terbatas pada:

1. mengidentifikasi area proses yang memiliki Risiko tinggi terhadap keberhasilan pelaksanaan Keamanan Informasi;
2. menetapkan indikator kinerja pada setiap area proses;
3. memformulasi pelaksanaan Keamanan Informasi dengan mengukur secara kuantitatif kinerja yang diharapkan;
4. melakukan evaluasi terhadap penyelenggaraan atau pelaksanaan SMKI;
5. menganalisis efektivitas pelaksanaan Keamanan Informasi; dan
6. mendukung dan merealisasikan program Audit Keamanan Informasi.

| | Format Tindakan Perbaikan | No. | FORM/SMKI/010 |
|---|---|---|---|
| | | Tanggal Efektif | 24 Juli 2023 |
| | | Versi | 1.0 |

F. Format Tindakan Perbaikan

No : .....
Bidang/Area : .....
Tanggal : .....
Diajukan kepada : .....
Dilaporkan oleh : .....

| Sumber Ketidaksesuaian | | | |
|---|---|---|---|
| | Audit Internal | | Laporan Insiden |
| | Audit Eksternal | | Usulan / Saran |
| | Pengukuran dan pemantauan | | Lain-lain:..... |

| Deskripsi Masalah/Potensial Masalah:<br>..... | | | |
|---|---|---|---|
| Status Temuan: ( Major / Minor / OFI )* | | | |
| Akar Masalah:<br>..... | | | |
| No | Koreksi *(perbaikan seketika)* | PIC | Batas Waktu |
| 1 | ..... | ..... | ..... |
| No | Tindakan Korektif (*supaya ketidaksesuaian tidak terjadi kembali*) | PIC | Batas Waktu |
| 1 | ..... | ..... | ..... |
| Verifikasi: | ( Close / Open )* | Tanggal: ..... | |
| Catatan:<br>..... | | | |

| Diverifikasi Oleh:<br>Auditor | Diverifikasi Oleh:<br>Atasan Terkait | Diverifikasi Oleh:<br>CISO |
|---|---|---|
| (.....) | (.....) | (.....) |

Catatan: Kolom auditor hanya perlu diisi untuk kegiatan audit

*Pilih salah satu/coret yang tidak perlu

WALI KOTA YOGYAKARTA,

ttd

HASTO WARDOYO