WALI KOTA BOGOR
PROVINSI JAWA BARAT

PERATURAN WALI KOTA BOGOR
NOMOR 23 TAHUN 2021

TENTANG

SISTEM MANAJEMEN KEAMANAN INFORMASI

DENGAN RAHMAT TUHAN YANG MAHA ESA

WALI KOTA BOGOR,

Menimbang : a. bahwa dalam rangka melindungi kerahasiaan, keutuhan, dan ketersediaan aset informasi di lingkungan Pemerintah Daerah Kota Bogor dari berbagai ancaman keamanan informasi baik dari dalam maupun luar, perlu melakukan pengelolaan keamanan informasi;

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

Mengingat : 1. Undang-Undang Nomor 28 Tahun 1999 tentang Penyelenggaraan Negara yang Bersih dan Bebas dari Korupsi, Kolusi dan Nepotisme (Lembaran Negara Republik Indonesia Tahun 1999 Nomor 75, Tambahan Lembaran Negara Republik Indonesia Nomor 3851);

2. Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi (Lembaran Negara Republik Indonesia Tahun 1999 Nomor 154, Tambahan Lembaran Negara Republik Indonesia Nomor 3881);

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 25 Tahun 2009 tentang Pelayanan Publik (Lembaran Negara Republik Indonesia Tahun 2009 Nomor 112, Tambahan Lembaran Negara Republik Indonesia Nomor 5038);
6. Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 244, Tambahan Lembaran Negara Republik Indonesia Nomor 5587) sebagaimana telah beberapa kali diubah terakhir dengan Undang-Undang Nomor 9 Tahun 2015 tentang Perubahan Kedua atas Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2015 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 5679);
7. Undang-Undang Nomor 30 Tahun 2014 tentang Administrasi Pemerintahan (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 292, Tambahan Lembaran Negara Republik Indonesia Nomor 5601);
8. Peraturan Pemerintah Nomor 61 Tahun 2010 tentang Pelaksanaan Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (Lembaran Negara Republik Indonesia Tahun 2010 Nomor 99, Tambahan Lembaran Negara Republik Indonesia Nomor 5149);
9. Peraturan Pemerintah Nomor 96 Tahun 2012 tentang Pelaksanaan Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik (Lembaran Negara Republik Indonesia Tahun 2012 Nomor 215, Tambahan Lembaran Negara Republik Indonesia Nomor 5357);
10. 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);
11. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 6 Tahun 2011 tentang Pedoman Umum Tata Naskah Dinas Elektronik di Lingkungan Instansi Pemerintah;
12. 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);
13. Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi (Berita Negara Republik Indonesia Tahun 2016 Nomor 551);
14. Peraturan Daerah Provinsi Jawa Barat Nomor 29 Tahun 2010 tentang Penyelenggaraan Komunikasi dan Informatika (Lembaran Daerah Provinsi Jawa Barat Tahun 2010 Nomor 29 Seri E, Tambahan Lembaran Daerah Nomor 92);

15. Peraturan Daerah Kota Bogor Nomor 7 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Kota Bogor (Lembaran Daerah Kota Bogor Tahun 2016 Nomor 1 Seri D) sebagaimana telah beberapa kali diubah terakhir dengan Peraturan Daerah Kota Bogor Nomor 5 Tahun 2020 tentang Perubahan Kedua atas Peraturan Daerah Kota Bogor Nomor 7 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Kota Bogor (Lembaran Daerah Kota Bogor Tahun 2020 Nomor 1 Seri D);
16. Peraturan Daerah Kota Bogor Nomor 8 Tahun 2017 tentang Penyelenggaraan Urusan Pemerintahan Daerah (Lembaran Daerah Kota Bogor Tahun 2017 Nomor 5 Seri E);
17. Peraturan Daerah Kota Bogor Nomor 9 Tahun 2018 tentang Penyelenggaraan Informatika dan Komunikasi (Lembaran Daerah Kota Bogor Tahun 2018 Nomor 5 Seri E);
18. Peraturan Wali Kota Bogor Nomor 135 Tahun 2019 tentang Pedoman Tata Naskah Dinas Elektronik di Lingkungan Pemerintah Daerah Kota Bogor (Berita Daerah Tahun 2019 Nomor 96 Seri E);
19. Peraturan Wali Kota Bogor Nomor 17 Tahun 2021 tentang Kedudukan, Susunan Organisasi, Tugas dan Fungsi serta Tata Kerja Perangkat Daerah di Lingkungan Pemerintah Kota Bogor (Berita Daerah Kota Bogor Tahun 2021 Nomor 17);

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. Daerah Kota adalah Daerah Kota Bogor.
2. Pemerintah Daerah Kota adalah Wali Kota sebagai unsur penyelenggara pemerintahan daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan daerah otonom.
3. Wali Kota adalah Wali Kota Bogor.
4. Gubernur adalah Gubernur Jawa Barat.
5. Perangkat Daerah adalah unsur pembantu Wali Kota 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, aritmatika, dan menyimpan.
11. Perangkat lunak adalah satu atau sekumpulan program komputer, prosedur, dan/atau dokumentasi yang terkait dalam pengoperasian sistem elektronik.
12. Keamanan informasi adalah suatu kondisi dimana terjaganya aspek kerahasiaan, integritas, dan ketersediaan dari informasi.
13. 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.
14. Aset informasi adalah unit informasi yang dapat dipahami, dibagi, dilindungi, dan dimanfaatkan secara efektif.
15. Aset pengolahan adalah suatu perangkat baik elektronik maupun non-elektronik yang dapat digunakan untuk membuat dan menyunting informasi.
16. Penyimpanan informasi adalah suatu proses menyimpan informasi dengan menggunakan media baik elektronik maupun non-elektronik.
17. *Data Center* adalah suatu fasilitas untuk menempatkan sistem komputer dan perangkat-perangkat terkait, seperti sistem komunikasi data dan penyimpanan data.

Pasal 2

(1) Peraturan Wali Kota ini dibentuk sebagai pedoman pengelolaan SMKI secara terpadu untuk memastikan terjaganya kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*).

(2) Pengelolaan SMKI sebagaimana dimaksud pada ayat (1) meliputi infrastruktur komputer, jaringan, sistem informasi/aplikasi, dan sumber daya manusia.

BAB II
RUANG LINGKUP

Pasal 3

Ruang lingkup pengamanan informasi yang diatur dalam Peraturan Wali Kota ini meliputi:

a. aset informasi;
b. aset pengolahan informasi; dan
c. penyimpanan informasi.

Bagian Kesatu
Aset Informasi

Pasal 4

Aset informasi sebagaimana dimaksud dalam Pasal 3 huruf a merupakan aset dalam bentuk:

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

b. 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.

Bagian Kedua
Aset Pengolahan Informasi

Pasal 5

Aset pengolahan informasi sebagaimana dimaksud dalam Pasal 3 huruf b berupa:

a. peralatan mekanik yang digerakan dengan tangan secara manual; dan

b. peralatan elektronik yang bekerja secara elektronik penuh.

Bagian Ketiga
Penyimpanan Informasi

Pasal 6

Penyimpanan informasi sebagaimana dimaksud dalam Pasal 3 huruf c menggunakan media:

a. elektronik, meliputi antara lain *server*, *harddisk*, *flashdisk*, kartu memori, dan lain-lain; dan

b. non-elektronik, meliputi antara lain lemari, rak, laci, *filling cabinet,* dan lain-lain.

BAB III
KOORDINATOR KEAMANAN TEKNOLOGI INFORMASI

Pasal 7

(1) Untuk melakukan pengamanan informasi sebagaimana dimaksud dalam Pasal 3, setiap Perangkat Daerah memiliki koordinator keamanan teknologi informasi.

(2) Koordinator keamanan teknologi informasi sebagaimana dimaksud pada ayat (1) bertanggung jawab memastikan teknologi informasi yang digunakan mendukung proses tata kelola pemerintahan dan pencapaian tujuan organisasi.

(3) Koordinator keamanan teknologi informasi sebagaimana dimaksud pada ayat (2) memiliki wewenang:

   a. menyusun prosedur penyelenggaraan keamanan informasi yang diterapkan secara efektif baik bagi Perangkat Daerah maupun pengguna; dan

   b. melakukan evaluasi kinerja penyelenggaraan teknologi informasi.

(4) Koordinator keamanan informasi sebagaimana dimaksud pada ayat (3) dijabat oleh pejabat struktural.

BAB IV
MANAJEMEN RISIKO

Pasal 8

(1) Setiap Perangkat Daerah penyelenggara teknologi informasi wajib melakukan proses manajemen risiko dalam menerapkan SMKI.

(2) Proses manajemen risiko sebagaimana dimaksud pada ayat (1) meliputi:
   a. identifikasi;
   b. pengukuran;
   c. pemantauan; dan
   d. pengendalian atas risiko terkait penggunaan teknologi informasi.

(3) Manajemen risiko sebagaimana dimaksud pada ayat (2) mencakup:
   a. pengembangan sistem;
   b. operasional teknologi informasi;
   c. jaringan komunikasi;
   d. penggunaan perangkat komputer;
   e. pengendalian terhadap informasi; dan
   f. penggunaan pihak kedua sebagai penyedia jasa teknologi informasi.

(4) Penerapan manajemen risiko harus dilakukan secara terintegrasi pada setiap penggunaan operasional teknologi informasi terkait sistem yang digunakan.

BAB V
SUMBER DAYA

Pasal 9

(1) Pimpinan Perangkat Daerah menyediakan sumber daya yang dibutuhkan untuk membentuk, mengimplementasikan, memelihara, dan meningkatkan penerapan SMKI secara berkesinambungan.

(2) Uraian secara rinci SMKI sebagaimana dimaksud pada ayat (1) tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Peraturan Wali Kota ini.

BAB VI
STANDAR DAN PROSEDUR PENGENDALIAN

Pasal 10

(1) Setiap Perangkat Daerah harus menyusun standar dan prosedur pengendalian kegiatan teknologi informasi yang memenuhi prasyarat keamanan informasi dan untuk mengimplementasikan tindakan dalam mengelola risiko.

(2) Prasyarat keamanan informasi sebagaimana dimaksud pada ayat (1) meliputi aspek sebagai berikut:
   a. organisasi keamanan informasi;
   b. keamanan sumber daya manusia;
   c. pengelolaan aset;
   d. pengendalian akses;
   e. kriptografi;
   f. keamanan fisik dan lingkungan;
   g. keamanan operasional;
   h. keamanan komunikasi;
   i. keamanan dalam proses akuisisi, pengembangan dan pemeliharaan sistem informasi;
   i. hubungan kerja dengan pemasok (*supplier*);

j. penanganan insiden keamanan informasi;

k. kelangsungan usaha; dan

l. kepatuhan.

Pasal 11

(1) Perangkat Daerah bertanggung jawab dalam memastikan kegiatan operasional teknologi informasi yang stabil dan aman.

(2) Penyelenggaraan pemrosesan transaksi pada operasional teknologi informasi harus memenuhi prinsip kehati-hatian.

(3) Setiap Perangkat Daerah penyelenggara teknologi informasi wajib mengidentifikasi dan memantau aktivitas operasional teknologi informasi untuk memastikan efektifitas, efesiensi, dan keamanan dari aktivitas tersebut antara lain dengan:

a. menerapkan perimeter fisik dan lingkungan di area kerja dan *Data Center*;

b. mengendalikan hak akses secara memadai sesuai kewenangan yang ditetapkan;

c. menerapkan pengendalian terhadap informasi yang diproses;

d. memastikan ketersediaan dan kecukupan kapasitas layanan jaringan komunikasi baik yang dikelola secara internal maupun oleh pihak lain penyedia jasa;

e. melakukan pemantauan kegiatan operasional teknologi informasi termasuk audit *trail*; dan

f. melakukan pemantauan terhadap aplikasi yang digunakan oleh Perangkat Daerah maupun pengguna.

BAB VII
MEKANISME PENYELENGGARAAN

Pasal 12

(1) Setiap Perangkat Daerah penyelenggara teknologi informasi harus memastikan ketersediaan data dan sistem dalam rangka menjaga kelangsungan teknologi informasi melalui penyelenggaraan fasilitas *Data Center* baik dikelola oleh internal maupun oleh pihak penyedia jasa.

(2) Setiap aktivitas pada fasilitas di *Data Center* harus dapat terpantau guna menghindari kesalahan proses pada sistem dan memperhatikan aspek perlindungan terhadap data yang diproses dan lingkungan fisik.

Pasal 13

(1) Perangkat Daerah harus menerapkan prinsip pengendalian terhadap aktivitas teknologi informasi melalui proses evaluasi dan monitoring secara berkala.

(2) Setiap instansi wajib melakukan kegiatan pemantauan dan tindakan koreksi penyimpangan terhadap kontrol keamanan informasi yang meliputi:

a. kegiatan pemantauan secara terus menerus; dan

b. pelaksanaan fungsi pemeriksaan intern yang efektif dan menyeluruh.

(3) Perangkat Daerah penyelenggara teknologi informasi berdasarkan hasil audit, umpan balik, maupun evaluasi terhadap pengendalian keamanan informasi yang dilakukan, meningkatkan efektivitas sistem manajemen keamanan informasi secara berkesinambungan melalui perbaikan terhadap akibat penyimpangan kegiatan teknologi informasi.

(4) Hasil dari tindakan perbaikan dan peningkatan sebagaimana dimaksud pada ayat (3) harus dilaporkan kepada Kepala Perangkat Daerah dan didokumentasikan sebagai bagian dari proses *lesson learned* bagi Perangkat Daerah.

Pasal 14

(1) Apabila terjadi kebocoran informasi pada instansi terkait yang berdampak sangat luas, maka Pemerintah Daerah dapat menunjuk auditor independen untuk melakukan investigasi yang diperlukan.

(2) Perangkat Daerah penyelenggara teknologi informasi wajib menyediakan akses kepada auditor independen sebagaimana dimaksud pada ayat (1) untuk melakukan pemeriksaan seluruh aspek terkait penyelenggaraan teknologi informasi.

BAB VIII
KETENTUAN PENUTUP

Pasal 15

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 Bogor.

Ditetapkan di Bogor
pada tanggal 3 Mei 2021

WALI KOTA BOGOR,
Ttd.
BIMA ARYA

Diundangkan di Bogor
pada tanggal 3 Mei 2021

SEKRETARIS DAERAH KOTA BOGOR,
Ttd.
SYARIFAH SOFIAH DWIKORAWATI

BERITA DAERAH KOTA BOGOR
TAHUN 2021 NOMOR 23

Salinan sesuai dengan aslinya
KEPALA BAGIAN HUKUM
DAN HAK ASASI MANUSIA,
Ttd.
ALMA WIRANTA, S.H., M.Si. (Han)
NIP. 19800507 200312 1 003

LAMPIRAN PERATURAN WALI KOTA BOGOR

NOMOR : 23 TAHUN 2021

TANGGAL : 3 MEI 2021

TENTANG : SISTEM MANAJEMEN KEAMANAN INFORMASI.

SISTEM MANAJEMEN KEAMANAN INFORMASI

BAB I

PENDAHULUAN

A. Tujuan

Sistem Manajemen Keamanan Informasi (SMKI) ini disusun sebagai arahan dan pedoman dalam pengelolaan sistem manajemen keamanan informasi secara terpadu serta untuk pengamanan aset informasi guna memastikan terjaganya aspek kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*).

B. Ruang Lingkup

1. Ruang lingkup kebijakan ini adalah seluruh aset informasi dan aset pemrosesan informasi yang berada di bawah pengelolaan *Data Center* Pemerintah Daerah Kota, beserta Perangkat Daerah pemilik aset terkait.
2. Aset informasi adalah aset dalam bentuk:
   a. fisik, meliputi informasi yang tercetak, tertulis, dan tersimpan dalam bentuk fisik seperti di atas kertas, papan tulis, spanduk, atau di dalam buku dan dokumen; dan
   b. 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.

C. Kebijakan

1. Perangkat Daerah berkomitmen untuk mengembangkan, mengimplementasikan, memelihara, dan meningkatkan Sistem Manajemen Keamanan Informasi (SMKI) secara berkesinambungan untuk menjamin keamanan informasi organisasi dari risiko keamanan informasi, baik dari pihak internal maupun eksternal.
2. Seluruh informasi dalam bentuk fisik maupun elektronik, yang dikomunikasikan langsung atau melalui teknologi komunikasi harus dilindungi dari kemungkinan kerusakan, kesalahan penggunaan baik secara sengaja atau tidak, dicegah dari akses oleh pengguna yang tidak berwenang dan dari ancaman terhadap kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*).
3. Perangkat Daerah berkomitmen untuk mendukung pemenuhan prasyarat internal maupun eksternal keamanan informasi Perangkat Daerah yang relevan.
4. Perangkat Daerah berkomitmen untuk mematuhi seluruh peraturan perundang-undangan, regulasi dan kewajiban kontrak yang relevan.
5. Perangkat Daerah berkomitmen untuk memastikan ketersediaan dari sumber daya yang dibutuhkan oleh SMKI di Perangkat Daerah untuk menjamin terciptanya SMKI yang efektif dan efisien.

6. Kontrol keamanan informasi beserta sasaran masing-masing kontrol ditetapkan oleh Kepala Dinas Komunikasi dan Informatika Kota Bogor secara tahunan, didasarkan atas hasil identifikasi dan analisis risiko yang sesuai dengan ruang lingkup kebijakan SMKI, serta prioritisasi dengan mempertimbangkan ketersediaan dan kemampuan sumber daya.
7. Kebijakan keamanan informasi harus dikomunikasikan ke seluruh pegawai dan pihak kedua terkait melalui media komunikasi yang ada agar dipahami dengan mudah dan dipatuhi.
8. Perangkat Daerah berkomitmen meningkatkan kepedulian (*awareness*), pengetahuan dan keterampilan tentang keamanan informasi bagi pegawai, serta mitra pihak kedua lain sejauh diperlukan.
9. Seluruh kelemahan keamanan informasi yang berpotensi atau telah mengakibatkan gangguan penggunaan TIK atau gangguan keamanan informasi harus segera dilaporkan kepada penanggung jawab TIK terkait.
10. Seluruh pimpinan di semua tingkatan bertanggung jawab menjamin kebijakan ini diterapkan di seluruh unit kerja di bawah pengawasannya.
11. Seluruh pegawai bertanggung jawab untuk menjaga dan melindungi keamanan aset informasi serta mematuhi kebijakan dan prosedur keamanan informasi yang telah ditetapkan.
12. Setiap pelanggaran terhadap kebijakan ini dapat dikenai sanksi administratif sesuai ketentuan peraturan perundang-undangan.
13. Setiap pengecualian terhadap kebijakan ini dan kebijakan turunannya harus mendapat persetujuan dari Kepala Dinas Komunikasi dan Informatika Kota Bogor.
14. Dokumen ini harus ditinjau paling sedikit 1 (satu) kali dalam 1 (satu) tahun atau apabila terdapat perubahan signifikan dalam proses bisnis organisasi untuk menjamin kesesuaian dan kecukupan dengan kondisi terkini.
15. Setiap perubahan terhadap dokumen ini harus didokumentasikan dan disetujui melalui proses manajemen perubahan.

BAB II

PEDOMAN PELAKSANAAN SISTEM MANAJEMEN KEAMANAN INFORMASI

A. Tujuan

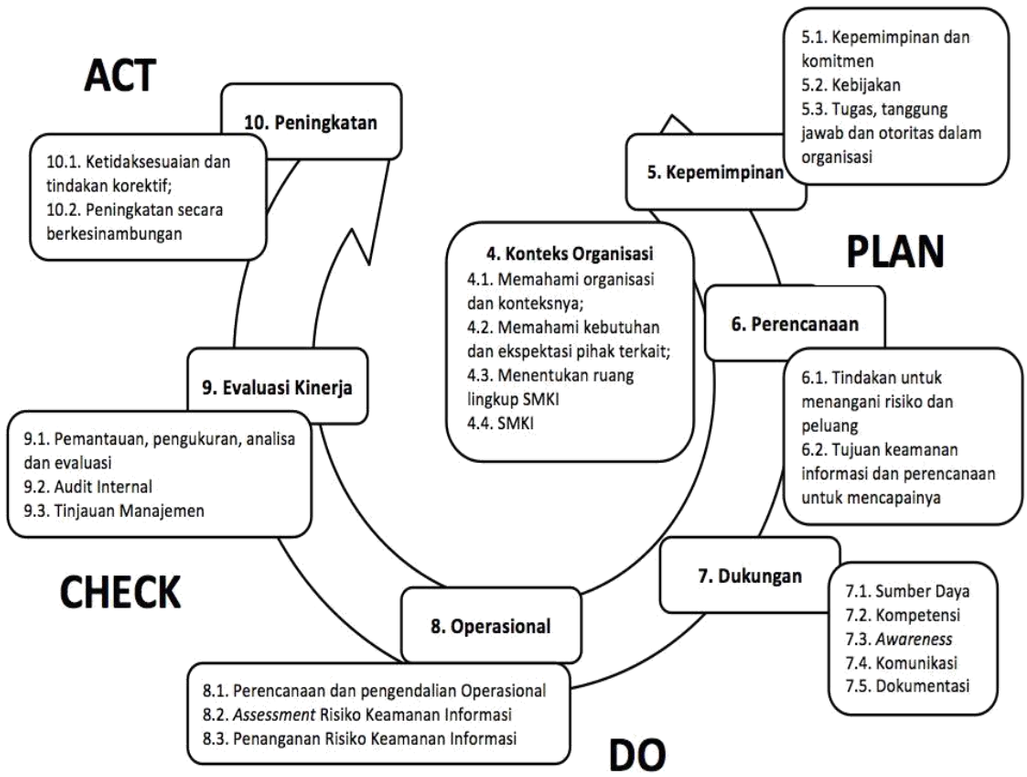
Tata kelola Sistem Manajemen Keamanan Informasi (SMKI) disusun dalam rangka untuk memastikan efektivitas dan efisiensi dari sistem manajemen keamanan informasi. Kerangka kerja ini akan menjabarkan proses-proses dan aktivitas-aktivitas yang harus dijalankan oleh Perangkat Daerah dalam rangka menetapkan, mengimplementasikan, memelihara SMKI, dan meningkatkan secara berkesinambungan.

B. Ruang Lingkup

Pedoman pelaksanaan Sistem Manajemen Keamanan Informasi yang diatur dalam Peraturan Wali Kota ini merupakan acuan bagi seluruh Perangkat Daerah di lingkungan Pemerintah Daerah Kota.

C. Kebijakan

1. Perangkat Daerah harus merencanakan suatu Sistem Manajemen Keamanan Informasi dengan mengadopsi siklus proses pada standar ISO 27001:2013. Deskripsi umum tentang siklus proses berdasarkan arahan standar ISO/IEC 27001:2013 dapat dilihat dari Gambar 1 sebagai berikut:



Gambar 1. Penggunaan siklus proses *Plan Do Check Act* dalam proses SMKI

2. Proses perencanaan dalam pengembangan Sistem Manajemen Keamanan Informasi meliputi:

   2.1 Perangkat Daerah harus menentukan konteks dan ruang lingkup SMKI organisasi dengan cara:

   a. menentukan dan secara berkala meninjau faktor serta permasalahan internal dan eksternal yang dihadapi oleh organisasi yang:

      1) relevan dengan tujuan dari Perangkat Daerah dan SMKI;

      2) mempengaruhi kemampuan Perangkat Daerah untuk mencapai tujuan SMKI yang diharapkan oleh Perangkat Daerah;

   b. menentukan dan secara berkala meninjau pihak-pihak yang terkait dengan Perangkat Daerah dan dapat mempengaruhi SMKI di Perangkat Daerah;

   c. menentukan dan secara berkala meninjau kebutuhan dan ekspektasi terkait keamanan informasi dari pihak-pihak yang terkait tersebut;

   d. menentukan dan secara berkala meninjau hubungan dan ketergantungan antar proses dan aktivitas Perangkat Daerah yang dilaksanakan oleh pihak internal maupun pihak eksternal Perangkat Daerah; dan

   e. menentukan dan secara berkala meninjau ruang lingkup dari SMKI di organisasi.

   2.2 risiko dan peluang yang relevan dengan SMKI harus secara jelas ditentukan dan ditangani untuk:

   a. memastikan bahwa SMKI mencapai tujuan yang diharapkan;

   b. mencegah atau mengurangi dampak yang tidak diinginkan; dan

   c. mencapai peningkatan yang berkesinambungan.

2.3 penentuan risiko dan peluang dilakukan dengan mempertimbangkan aspek-aspek yang telah didefinisikan dalam fase penentuan konteks dan ruang lingkup Perangkat Daerah yaitu:

a. faktor dan permasalahan internal maupun eksternal yang dihadapi Perangkat Daerah; dan

b. ekspektasi keamanan informasi dari pihak terkait Perangkat Daerah.

3. Perencanaan harus dibuat bagi risiko dan peluang yang telah ditentukan untuk:

a. menangani risiko dan peluang;

b. mengintegrasikan dan mengimplementasikan tindakan untuk menangani risiko dan peluang dengan proses SMKI; dan

c. mengevaluasi efektivitas dari tindakan yang diambil dalam rangka menangani risiko dan peluang.

4. Proses manajemen risiko dilakukan melalui proses literatif yang mencakup aktivitas *assessment* risiko, penanganan risiko, penerimaan risiko, dan pengkomunikasian risiko.

5. Seluruh manajemen risiko di organisasi harus dilakukan paling tidak 1 (satu) kali dalam 1 (satu) tahun atau apabila terdapat usulan atau telah terjadi perubahan yang relevan dan signifikan pada organisasi. Seluruh catatan (*record*) terkait dengan seluruh proses manajemen risiko harus dibuat dan dipelihara.

6. Dalam proses pemilihan dari kontrol terhadap pengendalian risiko tersebut dilakukan pada saat aktivitas penanganan risiko yang merupakan bagian dari proses manajemen risiko.

7. Pemilihan dari kontrol tersebut dapat memperhatikan kontrol keamanan informasi berdasarkan standar ISO 27001:2013 atau kontrol lainnya sesuai ketentuan peraturan perundang-undangan.

8. Dalam hal proses pendokumentasian SMKI perlu memperhatikan aspek sebagai berikut:

8.1. dokumentasi SMKI di Perangkat Daerah perlu mencakup informasi terdokumentasi yang disyaratkan oleh ISO 27001:2013 yang mencakup namun tidak terbatas pada:

a. ruang lingkup SMKI;

b. kebijakan dan tujuan keamanan informasi;

c. metodologi assessment dan penanganan risiko;

d. *statement of applicability*;

e. rencana penanganan risiko;

f. laporan *assessment* risiko;

g. pendefinisian tugas dan tanggung jawab keamanan informasi;

h. inventarisasi aset;

i. aturan terkait penggunaan aset;

j. kebijakan pengendalian akses;

k. prosedur operasional untuk manajemen teknologi informasi;

l. prinsip rekayasa sistem secara aman;

m. kebijakan keamanan terkait penyedia jasa;

n. prosedur pengelolaan insiden;

o. prosedur keberlanjutan bisnis*;*

p. prasyarat hukum, regulasi, dan kontraktual;

q. catatan terkait pelatihan, kemampuan, pengalaman, dan kualifikasi;

r. hasil pemantauan dan pengukuran SMKI;

s. program audit internal;

t. hasil audit internal;

u. hasil dari tinjauan manajemen;

v. hasil dari tindakan korektif;

w. *log* dari aktifitas pengguna, pengecualiaan, dan kejadian keamanan; dan

x. informasi terdokumentasi yang dibutuhkan untuk menjamin efektifitas dari SMKI.

8.2. dokumen yang relevan dengan SMKI dan berasal dari pihak eksternal seperti dokumen peraturan perundang-undangan harus di identifikasi dan dikendalikan juga;

8.3. terkait proses peninjauan dan pembaruan dokumentasi hal-hal berikut berlaku:

a. semua dokumentasi SMKI harus ditinjau paling sedikit 1 (satu) kali dalam 1 (satu) tahun atau apabila terdapat perubahan dalam SMKI dan/atau organisasi untuk menjamin kesesuaian dan kecukupannya dengan kondisi terkini SMKI dan keamanan informasi di organisasi;

b. peninjauan harus dilakukan oleh pemilik dari dokumentasi dan dapat melibatkan pihak-pihak yang terkait dengan dokumentasi dan/atau proses yang relevan dengan dokumentasi tersebut; dan

c. setiap pembaruan terhadap dokumentasi SMKI sebagai hasil dari peninjauan dokumentasi harus disetujui oleh manajemen yang relevan di Perangkat Daerah;

8.4 terkait proses salinan, distribusi, dan retensi dokumentasi hal-hal berikut berlaku:

a. salinan dari dokumentasi SMKI harus didistribusikan kepada pihak internal yang terkait untuk memastikan operasional SMKI secara efektif;

b. akses ke dokumentasi SMKI untuk pihak internal akan diberikan berdasarkan kebutuhan pengguna untuk mengakses dokumentasi tersebut (*need to know basis*);

c. pihak eksternal yang memerlukan akses kepada dokumentasi SMKI akan diberikan akses hanya setelah kontrol keamanan informasi yang memadai telah diimplementasikan. Hal ini mencakup namun tidak terbatas pada akses *read only* atau perjanjian kerahasiaan;

d. daftar distribusi harus ditetapkan dan dipelihara untuk mengendalikan distribusi dari dokumentasi SMKI; dan

e. kecuali diputuskan berbeda, seluruh dokumen SMKI memiliki masa retensi selama 10 (sepuluh) tahun.

9. Instansi harus mempertimbangkan penyediaan sumber daya dalam melaksanakan SMKI yang mencakup:

9.1. ketersediaan sumber daya yang dibutuhkan bagi pelaksanaan SMKI perusahan secara efektif dan efisien sangatlah penting. Oleh karena itu perencanaan yang baik sangatlah penting untuk memastikan ketersediaan sumber daya yang tepat pada waktu yang tepat pula;

9.2. sumber daya yang dibutuhkan oleh SMKI mencakup sumber daya dengan kompetensi dan pemahaman yang memadai, dokumentasi, proses dan solusi teknis, baik berupa perangkat keras maupun perangkat lunak;

9.3. perencanaan sumber daya SMKI dapat dilakukan bersamaan dengan proses perencanaan dan penyusunan anggaran tahunan organisasi; dan

9.4. pelatihan dan program peningkatan kesadaran terkait dengan SMKI dan keamanan informasi organisasi akan dilakukan secara berkala bagi seluruh pengguna sistem informasi organisasi. Program pelatihan dan peningkatan kesadaran tersebut akan dirancang sesuai dengan fungsi dan tanggung jawab pengguna.

10. Komunikasi yang relevan dengan SMKI, baik internal maupun eksternal, harus dikendalikan dan dikoordinasikan untuk memastikan:

    a. efektivitas alur pertukaran informasi dalam organisasi SMKI dan/atau dari dan ke pihak eksternal;

    b. tidak ada kebocoran informasi sensitif milik perusahaan;

    c. jalur komunikasi SMKI mencakup:

        1) komunikasi tatap muka;

        2) surat dan memo internal;

        3) *e-mail*;

        4) *website* Perangkat Daerah;

        5) pengumuman perusahaan; dan

        6) material cetak;

    d. personil perusahaan yang tidak ditunjuk untuk memberikan materi informasi tidak diperbolehkan untuk memberikan informasi apapun;

    e. informasi terkait dengan SMKI dan/atau keamanan informasi yang berasal dari sumber eksternal harus dikirimkan kepada koordinator SMKI untuk peninjauan dan pendistribusian kepada pihak yang relevan dalam SMKI organisasi. Hal ini mencakup:

        1) penerbitan peraturan hukum dan perundangan yang baru maupun perubahan terhadap peraturan lama;

        2) usulan perubahan terhadap prasyarat keamanan informasi; dan

        3) teknologi, ancaman, dan kelemahan baru terkait keamanan informasi.

11. Proses perencanaan dan pengendalian operasional SMKI harus dikoordinasikan dan dikomunikasikan. Proses perencanaan operasional SMKI harus dilakukan secara tahunan serta didokumentasikan dan dikomunikasikan kepada pihak yang terkait dengan SMKI. Proses pengendalian operasional SMKI adalah proses yang dilakukan untuk memastikan pelaksanaan operasional SMKI Perangkat Daerah telah sesuai dengan perencanaan yang telah dibuat. Proses pengendalian ini dapat mencakup aktifitas rapat peninjauan dan harus dilakukan paling sedikit 1 (satu) kali dalam 3 (tiga) bulan serta melibatkan personil yang terlibat di SMKI Perangkat Daerah.

12. Metode untuk mencegah, mendeteksi dan menindaklanjuti pelanggaran terhadap hukum terkait Hak Kekayaan Intelektual (HAKI) perlu disusun dan diimplementasikan. Hal ini dapat mencakup aktivitas pemantauan, pengukuran, peninjauan, dan/atau audit.
13. Pemantauan, pengukuran, analisis, dan evaluasi dari implementasi dan operasional SMKI organisasi adalah aktivitas periodik yang dilakukan untuk mengevaluasi kinerja keamanan informasi dan efektivitas SMKI organisasi. Proses pemantauan, pengukuran, analisis, dan evaluasi mencakup:
    13.1. metrik pemantauan dan pengukuran harus dipilih secara seksama untuk memastikan bahwa aktivitas pengukuran akan memberikan pemahaman mendalam mengenai kinerja SMKI dan kontrol pengendalian keamanan informasi Perangkat Daerah;
    13.2. proses pengukuran tersebut mencakup proses-proses berikut:
        a. penentuan dari metrik pengukuran;
        b. pengukuran dari metrik yang telah ditentukan; dan
        c. analisis dan evaluasi dari hasil pengukuran.
    13.3. dalam menentukan metrik pengukuran aspek-aspek berikut harus dipertimbangkan:
        a. sasaran SMKI yang diberikan pada kebijakan SMKI Perangkat Daerah;
        b. kontrol keamanan informasi yang diimplementasikan;
        c. metode dalam mengumpulkan data dan mengkalkulasi metrik;
        d. target pencapaian dari metrik;
        e. jadwal untuk melakukan pengukuran; dan
        f. personil yang bertanggung jawab untuk proses pengukuran.
    13.4. metrik pengukuran yang telah ditentukan harus memungkinkan evaluasi dari pencapaian sasaran SMKI;
    13.5. metrik yang telah ditetapkan harus dipantau dengan mengumpulkan data yang relevan dengan metrik;
    13.6. proses pengukuran harus dilakukan minimal 1 (satu) kali dalam 1 (satu) tahun terutama untuk mengukur pencapaian dari sasaran SMKI;
    13.7. hasil dari pengukuran harus dianalisis dan dievaluasi untuk menentukan pencapaian dari target pengukuran tersebut;
    13.8. hasil dari pengukuran harus dilaporkan kepada manajemen puncak SMKI dalam rapat tinjauan manajemen SMKI;
    13.9. hasil dari proses pemantauan dan pengukuran efektivitas SMKI harus dianalisis dan dievaluasi untuk menentukan apakah implementasi dan operasi SMKI organisasi:
        a. sesuai dengan kebijakan, tujuan, standar, dan prosedur SMKI organisasi;
        b. memadai untuk menghadapi kebutuhan dan tantangan bisnis serta teknologi terkini; dan
        c. sesuai dengan rencana SMKI yang sudah dibuat.
14. Peninjauan keamanan informasi secara independen harus secara rutin dilakukan.
    14.1. peninjauan tersebut harus mencakup:

a. kontrol dan area keamanan informasi, seperti keamanan fisik, jaringan, atau akses *logical*;

b. kebijakan, proses, dan prosedur yang relevan dengan SMKI;

c. kepatuhan implementasi SMKI dan keamanan informasi dengan kebijakan, proses, dan prosedur keamanan informasi Perangkat Daerah serta prasyarat hukum, perundang-undangan, serta kewajiban kontraktual terkait dengan SMKI; dan

d. peninjauan teknis terhadap fasilitas pengolahan informasi dan sarana pendukungnya.

14.2. hasil dari peninjauan harus didokumentasikan dan dilaporkan kepada manajemen SMKI yang relevan; dan

14.3. setiap permasalahan dan/atau ketidaksesuaian harus segera ditindaklanjuti dengan cara mengidentifikasi tindakan korektif dan/atau peningkatan yang sesuai.

15. Instansi harus melakukan proses audit internal dengan ketentuan sebagai berikut:

15.1. audit internal SMKI di Perangkat Daerah harus dilaksanakan minimal 1 (satu) kali dalam 1 (satu) tahun dan harus mencakup seluruh ruang lingkup SMKI;

15.2. audit internal SMKI harus dilakukan oleh auditor yang memiliki kompetensi yang memadai serta memiliki objektifitas dan imparsialitas terhadap proses audit;

15.3. auditor yang dipilih untuk proses audit harus ditunjuk secara formal oleh manajemen puncak SMKI;

15.4. sebuah program audit tahunan SMKI harus ditetapkan oleh koordinator audit internal SMKI dan harus dikomunikasikan kepada koordinator SMKI;

15.5. program audit harus mencakup jadual, metode, kriteria, dan ruang lingkup, tanggung jawab, serta prasyarat pelaporan dari audit;

15.6. proses audit harus dilakukan sesuai dengan program audit yang telah ditetapkan secara formal;

15.7. temuan audit harus diklasifikasikan berdasarkan kritikalitas dan cakupan dari temuan tersebut menjadi:

a. mayor, ketidaksesuaian ini mengindikasikan tidak berjalannya sama sekali sebuah proses SMKI atau kontrol keamanan informasi, atau apabila sebuah temuan dapat menyebabkan dampak buruk terhadap proses atau sistem kritikal perusahaan;

b. minor, ketidaksesuaian ini mengindikasikan sebuah kealpaan/problem kecil yang tidak mengindikasikan bahwa sebuah proses SMKI atau kontrol keamanan informasi tidak berjalannya sama sekali, atau apabila sebuah temuan tidak akan menyebabkan dampak buruk terhadap proses atau sistem kritikal perusahaan; dan

c. peluang untuk perbaikan, kategori temuan ini bukanmerupakan sebuah ketidaksesuaian namun mengindikasikan bahwa sebuah area dapat diperbaiki untuk meningkatkan kinerja dari proses atau sistem.

15.8. setiap ketidaksesuaian dan/atau peluang untuk perbaikan yang proses audit harus dicatat secara formal oleh auditor dan diterima oleh *auditee*;

15.9. setiap ketidaksesuaian harus dikoreksi dan ditingkatkan oleh *auditee* dalam jangka waktu yang disepakati dengan cara merencanakan dan melaksanakan koreksi dan tindakan korektif;

15.10 laporan audit harus dilaporkan kepada manajemen puncak Perangkat Daerah dan dikomunikasikan kepada koordinator SMKI;

15.11 koordinator SMKI dan auditor internal SMKI bertanggung jawab untuk memantau dan memverifikasi koreksi, tindakan korektif maupun peningkatan terkait ketidaksesuaian yang ditemukan dalam audit;

15.12 verifikasi dari auditor internal SMKI dibutuhkan sebelum ketidaksesuaian yang ditemukan dapat dinyatakan ditutup secara formal.

16. Manajemen SMKI Perangkat Daerah wajib untuk melaksanakan tinjauan manajemen SMKI minimal satu kali dalam 1 (satu) tahun atau apabila terjadi perubahan signifikan terhadap SMKI di Perangkat Daerah. Tinjauan ini dilakukan untuk menjamin terjaganya kesesuaian, kecukupan, dan efektivitas dari SMKI di Perangkat Daerah, dengan memperhatikan hal-hal sebagai berikut:

16.1. tinjauan manajemen SMKI harus dihadiri oleh:

a. manajemen puncak dari SMKI di Perangkat Daerah;

b. koordinator SMKI Perangkat Daerah; dan

c. koordinator atau petugas fungsional SMKI;

16.2. apabila dibutuhkan, tinjauan manajemen SMKI dapat dihadiri oleh:

a. pemangku kepentingan yang relevan dari SMKI di Perangkat Daerah yang membidangi teknologi informatika; dan

b. *subject matter expert* yang memadai.

16.3. tinjauan manajemen SMKI harus mencakup masukan sebagai berikut:

a. status dari tindakan yang diputuskan pada tinjauan manajemen terdahulu;

b. perubahan baik internal maupun eksternal yang terkait dengan SMKI;

c. masukan terkait kinerja keamanan informasi yang mencakup *trend* pada:

1) ketidaksesuaian dan tindakan korektif;

2) hasil pemantauan dan pengukuran;

3) hasil audit, baik internal maupun eksternal; dan

4) pemenuhan dari sasaran keamanan informasi.

d. masukan dari pihak terkait;

e. hasil dari *assessment* risiko dan status rencana penanganan risiko; dan

f. peluang untuk peningkatan secara berkesinambungan.

16.4. berdasarkan dari masukan tersebut, tinjauan manajemen SMKI harus menghasilkan keluaran sebagai berikut:

a. keputusan terkait peningkatan SMKI secara berkesinambungan; dan

b. peluang dan kebutuhan untuk perubahan SMKI.

16.5. setiap keluaran dari tinjauan manajemen SMKI harus digunakan sebagai dasar bagi peningkatan dan perencanaan tahunan SMKI.

17. Ketidaksesuaian SMKI didefinisikan sebagai kondisi dimana adanya prasyarat SMKI yang tidak terpenuhi. Setiap ketidaksesuaian atau tidak terpenuhinya prasyarat SMKI harus di identifikasi dan di laporkan:

17.1. identifikasi dan laporan dari setiap ketidaksesuaian dapat didapatkan melalui:

a. proses pengelolaan insiden keamanan informasi;

b. peninjauan internal SMKI;

c. proses audit internal SMKI;

d. proses pemantauan dan pengukuran SMKI;

e. peninjauan dan/atau proses audit eksternal terhadap SMKI atau keamanan informasi; dan

f. laporan dan masukan dari *stakeholder* yang terkait.

17.2. setiap ketidaksesuaian yang terjadi harus ditangani secara tepat dengan cara:

a. melakukan koreksi yang sesuai untuk mengendalikan dan memperbaiki ketidaksesuaian yang telah diidentifikasi; dan

b. menangani setiap akibat dari ketidaksesuaian yang mungkin terjadi.

17.3. untuk setiap ketidaksesuaian, evaluasi harus dilakukan untuk mengevaluasi kebutuhan untuk mengambil tindakan korektif untuk menghilangkan penyebab dari ketidaksesuaian supaya ketidaksesuaian tersebut tidak terjadi lagi atau terjadi di tempat lain.

17.4. tindakan korektif yang diambil harus sesuai dengan dampak dari ketidaksesuaian tersebut untuk memastikan bahwa ketidaksesuaian tersebut tidak berulang atau terjadi ditempat lain dalam ruang lingkup SMKI.

17.5. evaluasi untuk menentukan apakah perlu untuk mengambil setiap tindakan korektif harus dilakukan dengan melakukan:

a. peninjauan terhadap ketidaksesuaian yang terjadi;

b. menentukan penyebab dari ketidaksesuaian;

c. menentukan jika ada kejadian dimana ketidaksesuaian yang sama telah terjadi, atau dapat berpotensi untuk terjadi.

17.6. apabila ditentukan bahwa tindakan korektif memang perlu untuk diambil maka harus dilakukan perencanaan dan implementasi dari tindakan korektif.

17.7. setelah koreksi dan tindakan korektif telah diambil, sebuah peninjauan harus dilakukan untuk menjamin efektifitasnya dalam mencegah terjadinya kembali atau terjadinya ketidaksesuaian tersebut ditempat lain.

18. Kesesuaian, kecukupan, dan efektifitas dari SMKI Perangkat Daerah harus secara berkesinambungan ditingkatkan.

19. Inisiatif peningkatan harus secara formal diidentifikasi, direncanakan, diimplementasikan dan ditinjau.

20. Identifikasi dari peningkatan harus dilakukan berdasarkan *log*, laporan, dan hasil dari:
    a. proses pengelolaan insiden keamanan informasi;
    b. peninjauan internal SMKI;
    c. proses audit internal SMKI;
    d. proses pemantauan dan pengukuran SMKI;
    e. peninjauan dan/atau proses audit eksternal terhadap SMKI atau keamanan informasi; dan
    f. laporan dan masukan dari *stakeholder* yang terkait.
21. Perencanaan dan implementasi dari inisiatif peningkatan harus ditinjau untuk memastikan bahwa inisiatif tersebut dapat mencapai tujuannya.
22. Dokumentasi yang relevan dengan proses peningkatan secara berkesinambungan harus dibuat dan dipelihara.

BAB III

MANAJEMEN RISIKO

A. Tujuan

Tujuan dari manajemen risiko adalah untuk mengelola risiko keamanan informasi yang dihadapi oleh organisasi dalam rangka untuk mempersiapkan diri terhadap terjadinya risiko beserta dampaknya.

B. Ruang Lingkup

Ruang lingkup dari manajemen risiko memastikan Perangkat Daerah dapat menerapkan proses pengelolaan risiko yang mencakup kegiatan:

1. penetapan konteks;
2. *assessment* risiko;
3. penanganan risiko;
4. pemantauan dan peninjauan risiko; dan
5. komunikasi dan koordinasi risiko.

C. Kebijakan

1. Kriteria penerimaan risiko dan penilaian keamanan informasi harus ditetapkan untuk memberikan arahan bagi Perangkat Daerah terhadap penanganan risiko yang harus dilakukan.
2. Perangkat Daerah harus menerapkan konteks terkait rencana perencanaan identifikasi Risiko yang meliputi isu-isu, pihak terkait dan prasyarat keamanan informasi internal dan eksternal yang terkait dengan keamanan informasi harus diidentifikasi dan ditetapkan sebagai pertimbangan dalam mengidentifikasi risiko keamanan informasi. Hal ini setidaknya mencakup:
   a. kegiatan utama yang dilakukan oleh organisasi;
   b. kebijakan internal organisasi;
   c. proses bisnis organisasi;
   d. kewajiban hukum, perundang-undangan dan kewajiban kontrak yang dimiliki oleh organisasi; dan
   e. kondisi teknologi informasi dan keamanan informasi, baik internal maupun eksternal yang relevan dengan organisasi.
3. Perangkat Daerah harus melaksanakan penilaian risiko yang berpengaruh terhadap kegagalan sistem dan operasional teknologi informasi terkait dengan aspek keamanan informasi yang mencakup aktivitas:

   3.1. identifikasi risiko:

   a. mengidentifikasi ancaman, merupakan aktifitas untuk mengidentifikasi ancaman terhadap risiko keamanan informasi;
   b. ancaman didefinisikan sebagai potensi penyebab insiden yang tidak diinginkan yang dapat menyebabkan kerusakan/kerugian bagi organisasi dan sistemnya;
   c. sebuah ancaman tidak dapat dikatakan sebuah risiko apabila tanpa kombinasi dengan kelemahan yang dapat dieksploitasi;
   d. mengidentifikasi kelemahan dilakukan setelah pengidentifikasian ancaman dilakukan;

e. kelemahan didefinisikan sebagai potensi kekurangan pada proses dan kontrol keamanan yang dapat dieksploitasi oleh 1 (satu) ancaman atau lebih;

f. mengidentifikasi dampak merupakan aktifitas yang dilakukan untuk mengidentifikasi potensi dampak jika ancaman yang teridentifikasi, mengeksploitasi kelemahan yang ada;

g. risiko harus dialokasikan ke pemilik risiko; dan

h. pemilik risiko bertanggung jawab untuk mengelola risiko yang telah teridentifikasi;

3.2. Analisis risiko:

a. menilai dampak potensial yang akan terjadi apabila risiko yang teridentifikasi terwujud; dan

b. kriteria dampak merupakan parameter untuk menentukan tingkat kerugian terhadap risiko yang terjadi.

Contoh kriteria dampak adalah sebagai berikut:

Tabel 1 Tabel Dampak Risiko SMKI

Tingkat Dampak	**Operasional**	**Peraturan / Hukum**	**Aset Informasi**	**Reputasi**
1 (Ringan)	Penundaan proses bisnis setengah hari	Tidak ada pelanggaran hukum	Tidak ada kebocoran atau kehilangan aset informasi.	Tidak ada dampak terhadap reputasi Perangkat Daerah
2 (Sedang)	Penundaan proses bisnis 1 (satu) hari	Pelanggaran ringan dengan surat peringatan	Berdampak pada kebocoran atau kehilangan aset informasi yang bersifat PUBLIK	Mengganggu kepercayaan sebagian kecilpihak eksternal. Berdampak pada reputasi Perangkat Daerah atau namun reputasi dapat dipulihkan dalam waktu tidak terlalu lama.
3 (Berat)	Penundaan proses bisnis 3 (tiga) hari	Pelanggaran sedang yang dikenakan sanksi administratif	Berdampak pada kebocoran atau kehilangan aset informasi yang bersifat TERBATAS	Mengganggu kepercayaan sebagian besar pihak eksternal. Berdampak pada reputasi Perangkat Daerah dan pemulihan reputasi membutuhkan waktu yang lama.

4 (Sangat Berat)	Penundaan lebih dari 3 (tiga) hari	Pelanggaran berat dengan sanksi hukum	Berdampak pada kebocoran atau kehilangan aset informasi yang bersifat RAHASIA.	Mengganggu kepercayaan sebagian besar pihak eksternal. Berdampak pada reputasi Perangkat Daerah dan sangat sulit dilakukan pemulihan reputasi.

c. menilai kemungkinan realistis terjadinya risiko yang teridentifikasi; dan

d. kriteria kecenderungan merupakan parameter untuk menentukan tingkat kejadian terhadap risiko.

Contoh kriteria kecenderungan adalah sebagai berikut:

Nilai	**Tingkat**	**Kriteria Kecenderungan**
		Frekuensi terjadinya
1	**Rendah**	Kejadian tidak lebih dari 2 kali / tahun
2	**Sedang**	Kejadian lebih dari 2 kali / tahun, namun tidak lebih dari 5 kali / tahun
3	**Tinggi**	Kejadian lebih dari 5 kali / tahun, namun tidak lebih dari 10 kali / tahun
4	**Ekstrim**	Kejadian lebih dari 10 kali / tahun

Tabel 1. Tabel Kecenderungan Risiko SMKI

e. evaluasi risiko:

1) membandingkan hasil analisis risiko dengan kriteria risiko yang sudah ditetapkan;

2) risiko yang masuk dalam kriteria penerimaan risiko akan diterima;

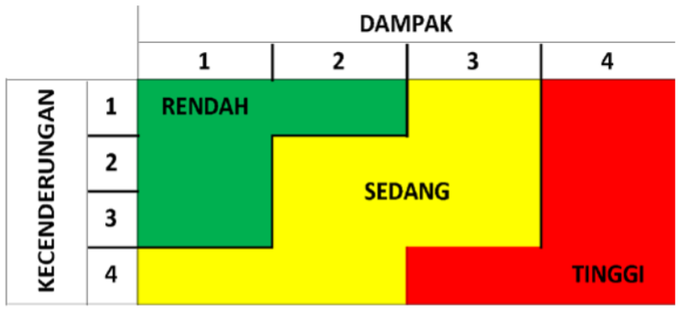
3) risiko yang tidak masuk dalam kriteria penerimaan risiko perlu mendapatkan penanganan; dan

4) setiap penanganan risiko harus diberikan prioritas.

4. Hasil evaluasi risiko harus dianalisis terkait risiko tersebut dapat diterima dalam level tertentu berdasarkan kriteria penerimaan risiko yang telah ditetapkan atau memerlukan penanganan risiko lebih lanjut.

Tabel risiko adalah matriks antara nilai dari dampak dan kecenderungan yang menghasilkan tingkat risiko.

Contoh tabel risiko adalah sebagai berikut:



Tabel SEQ Tabel * ARABIC 2 Tabel Nilai Risiko SMKI

5. Dalam hal risiko tersebut tidak dapat diterima, Perangkat Daerah harus menerapkan penanganan risiko yang diperlukan yang mencakup:
   a. mengendalikan/*control* adalah merupakan Tindakan pengendalian risiko dengan mengurangi dampak maupun kemungkinan terjadinya risiko melalui menerapkan suatu sistem atau aturan;
   b. menghindari/*avoid* adalah tindakan pengendalian risiko dengan tidak melakukan suatu aktivitas atau memilih aktivitas lain dengan *output* yang sama untuk menghindari terjadinya risiko;
   c. mengalihkan/*transfer* adalah tindakan pengendalian risiko dengan mengalihkan seluruh atau sebagian tanggung jawab pelaksanaan suatu proses kepada pihak ketiga.
6. Penanganan risiko harus memadai untuk mengurangi risiko ke tingkat yang dapat diterima berdasarkan kriteria penerimaan risiko.
7. Pemilik risiko harus memastikan setiap rencana penanganan risiko telah memadai dan relevan bagi risiko yang ada.
8. Setiap rencana penanganan risiko harus diberikan prioritas oleh pemilik risiko.
9. Setiap keputusan terkait dengan penanganan risiko dan kontrol keamanan risiko yang relevan harus disetujui oleh Pimpinan Perangkat Daerah terkait.
10. Perangkat Daerah harus melakukan proses pemantauan dan peninjauan risiko untuk memastikan efektifitas kontrol yang dilakukan yang mencakup:
    a. proses pemantauan dan peninjauan risiko adalah proses berkesinambungan untuk memastikan bahwa:
       1) risiko baru telah terindentifikasi, di-*assess* dan ditangani;
       2) setiap perubahan terhadap risiko yang sudah ada telah teridentifikasi, di-*assess* dan ditangani; dan
       3) kontrol keamanan yang sudah ada telah memadai dan efektif dalam menangani risiko.
    b. proses pemantauan dan peninjauan risiko harus dilakukan secara formal dan rutin;
    c. Perangkat Daerah harus menentukan frekuensi pemantauan dan peninjauan risiko.

11. Perangkat Daerah harus melakukan proses komunikasi dan koordinasi risiko untuk memastikan pengelolaan penanganan kontrol terkendali dan efektif dalam mengurangi tingkat risiko yang diharapkan.
12. Metode komunikasi dan koordinasi risiko harus ditetapkan yang meliputi:
    a. proses komunikasi dan koordinasi risiko merupakan proses berkesinambungan untuk mengkomunikasi dan mengoordinasikan setiap informasi, aktifitas dan keputusan terkait dengan risiko keamanan informasi dan proses manajemen risiko;
    b. setiap informasi, aktifitas dan keputusan harus dikomunikasikan dan dikoordinasikan dengan pemilik risiko, personil terkait dan Kepala Perangkat Daerah; dan
    c. setiap komunikasi dan koordinasi eksternal terkait risiko keamanan informasi dan manajemen risiko harus disetujui oleh Kepala Perangkat Daerah.

BAB IV

ORGANISASI SISTEM MANAJEMEN KEAMANAN INFORMASI

A. Tujuan

Organisasi Tim Keamanan Informasi Pemerintah Daerah Kota dibentuk dengan tujuan sebagai berikut:

1. sebagai pedoman dalam pembentukan organisasi fungsional keamanan informasi yang bertanggung jawab dalam pengelolaan keamanan informasi serta hubungan kerja dengan pihak eksternal;
2. menumbuhkan kesadaran pada sumber daya manusia Pemerintah Daerah Kota Bogor tentang arti penting keamanan informasi;
3. memastikan keamanan informasi terkait penggunaan perangkat *mobile* dan pelaksanaan aktivitas *teleworking.*

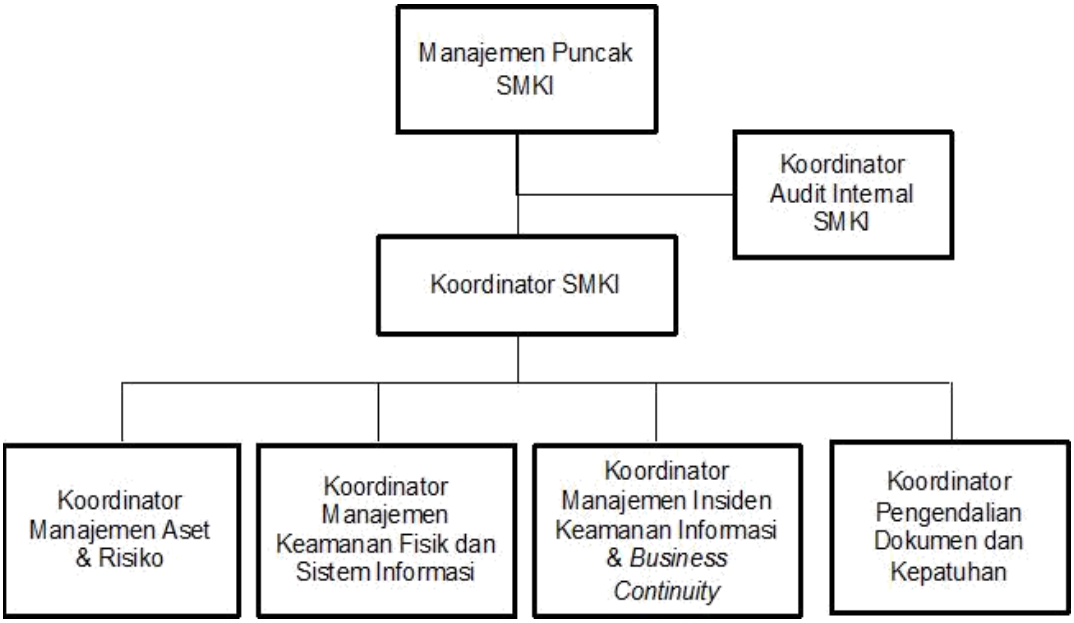
B. Ruang Lingkup

Ruang lingkup terkait dengan organisasi SMKI ini mengatur mengenai:

1. struktur organisasi Tim Keamanan Informasi Pemerintah Daerah Kota;
2. hubungan kerja dengan pihak berwenang, komunitas keamanan informasi, dan pihak ketiga; dan
3. penggunaan perangkat *mobile* dan teknologi *teleworkin*g.

C. Kebijakan

1. Perangkat Daerah wajib membentuk struktur organisasi berbasiskan sistem manajemen keamanan informasi untuk memastikan pelaksanaan keamanan informasi sesuai dengan standar ISO 27001:2013.
2. Organisasi Sistem Manajemen Keamanan Informasi merupakan organisasi fungsional yang memiliki struktur seperti yang diberikan pada Gambar 2 berikut:



Gambar 2. Struktur Organisasi SMKI di Perangkat Daerah

3. Manajemen puncak SMKI memiliki tugas dan tanggung jawab sebagai berikut:
   a. memberikan arahan dan tujuan umum dari SMKI organisasi, dalam bentuk kebijakan Sistem Manajemen Keamanan Informasi (SMKI);
   b. memastikan bahwa tujuan dan rencana dari SMKI organisasi telah ditetapkan;
   c. menetapkan struktur organisasi beserta alokasi tugas dan tanggung jawab dalam SMKI organisasi;
   d. mengkomunikasikan kepada personil dalam organisasi terkait pentingnya pemenuhan aturan terkait keamanan informasi organisasi sesuai ketentuan peraturan perundang-undangan serta perlunya peningkatan SMKI organisasi secara berkesinambungan;
   e. menyediakan sumber daya yang memadai untuk menetapkan, mengimplementasi, mengoperasikan, memantau, meninjau, memelihara, dan meningkatkan SMKI organisasi;
   f. menetapkan kriteria penerimaan risiko dan tingkat risiko yang dapat diterima;
   g. menyetujui tingkat risiko residual keamanan informasi;
   h. memastikan pelaksanaan audit internal SMKI; dan
   i. menghadiri dan memimpin rapat tinjauan manajemen SMKI.
4. Koordinator SMKI memiliki tugas dan tanggung jawab sebagai berikut:
   a. menyusun, mengoordinasikan, serta memantau pelaksanaan program kerja SMKI;

b. mengoordinasikan pelaksanaan proses manajemen risiko SMKI organisasi;

c. mengoordinasikan pelaksanaan aktifitas SMKI serta pengamanan informasi di organisasi;

d. mengoordinasikan proses peninjauan secara berkala terhadap implementasi SMKI di organisasi;

e. mengoordinasikan proses pengukuran efektivitas SMKI dan kontrol keamanan informasi di organisasi;

f. mengoordinasikan aktivitas dan tindakan untuk meningkatkan efektivitas SMKI, yang mencakup antara lain koreksi dan tindakan korektif untuk ketidaksesuaian yang ditemukan serta pelaksanaan rencana penanganan risiko; dan

g. memberikan laporan secara berkala terkait kondisi SMKI dan keamanan informasi organisasi kepada manajemen puncak SMKI.

5. Koordinator audit internal SMKI memiliki tugas dan tanggung jawab sebagai berikut:

a. menyusun dan memantau program dan jadwal audit internal SMKI;

b. mengoordinasikan pelaksanaan proses audit internal SMKI;

c. merangkum dan melaporkan hasil audit internal SMKI kepada manajemen puncak SMKI;

d. memberikan rekomendasi terkait kontrol keamanan informasi yang diperlukan untuk meningkatkan efektivitas SMKI; dan

e. mengoordinasikan proses verifikasi koreksi dan tindakan korektif yang diambil terhadap ketidaksesuaian yang ditemukan dalam proses audit internal SMKI.

6. Koordinator manajemen aset dan risiko SMKI memiliki tugas dan tanggung jawab sebagai berikut:

a. mengoordinasikan dan memantau pengelolaan aset informasi dan aset pengolahan dan penyimpanan informasi organisasi, hal ini mencakup proses registrasi, inventarisasi, serta pemeliharaan inventarisasi aset tersebut;

b. menyusun dan memelihara dokumen registrasi aset informasi dan aset pengolahan dan penyimpanan informasi organisasi;

c. melakukan peninjauan terkait proses penanganan aset informasi dan aset pengolahan dan penyimpanan informasi organisasi berdasarkan kebijakan dan prosedur terkait pengelolaan aset SMKI organisasi;

d. menyusun dan mengkoordinasikan aktivitas proses pengelolaan manajemen risiko SMKI di organisasi, bekerja sama dengan pemilik risiko, berdasarkan kebijakan dan prosedur terkait pengelolaan risiko SMKI organisasi;

e. mengkoordinasikan proses registrasi terhadap risiko SMKI di organisasi, bekerja sama dengan pemilik risiko;

f. mengkoordinasikan pengkinian secara rutin terhadap registrasi risiko organisasi, bekerja sama dengan pemilik risiko; dan

g. menyusun dan memelihara dokumen *risk profile* dan *risk treatment plan* SMKI organisasi.

7. Koordinator manajemen keamanan fisik dan sistem informasi SMKI memiliki tugas dan tanggung jawab sebagai berikut:

a. mengoordinasikan dan memantau proses dan aktifitas pengamanan fisik dan lingkungan dalam organisasi;

b. melaksanakan proses pengelolaan dan pemeliharaan fasilitas pengamanan fisik organisasi berdasarkan kebijakan dan prosedur terkait keamanan fisik dan lingkungan SMKI organisasi;

c. melaksanakan proses pengelolaan dan pemeliharaan hak akses fisik ke fasilitas organisasi berdasarkan kebijakan dan prosedur terkait keamanan fisik dan lingkungan SMKI organisasi;

d. mengoordinasikan dan memantau proses dan aktifitas pengelolaan akses *logical*;

e. melaksanakan proses pengelolaan dan pemeliharaan akses *logical* dari pengguna ke sistem informasi organisasi berdasarkan *kebijakan* dan prosedur terkait keamanan akses logical ke sistem informasi organisasi, hal ini mencakup proses pendaftaran, pemeliharaan dan pencabutan hak akses *logical* pengguna ke sistem informasi;

f. mengakomodasi penyusunan dan pemeliharaan *access control matrix* bersama-sama dengan Perangkat Daerah pemilik aplikasi dan/atau informasi;

g. mengoordinasikan dan memantau pengelolaan keamanan operasional sistem informasi organisasi berdasarkan kebijakan dan prosedur terkait pengelolaan keamanan operasional sistem informasi organisasi; dan

h. merancang, memantau dan memelihara sistem keamanan dari sistem informasi organisasi yang ini mencakup perangkat keras, lunak maupun aktif jaringan dan keamanan jaringan dalam sistem informasi organisasi.

8. Koordinator manajemen insiden keamanan informasi dan *business continuity* SMKI memiliki tugas dan tanggung jawab sebagai berikut:
    a. mengoordinasikan proses pendokumentasian laporan terkait kejadian, kelemahan dan insiden keamanan informasi berdasarkan kebijakan dan prosedur terkait pengelolaan insiden keamanan informasi organisasi;
    b. mengoordinasikan dan memantau pengelolaan insiden keamanan informasi berdasarkan kebijakan dan prosedur terkait pengelolaan insiden keamanan informasi organisasi;
    c. mendokumentasikan proses pengelolaan insiden keamanan informasi di organisasi;
    d. mengoordinasikan dan memantau pengelolaan *business continuity management* di organisasi berdasarkan kebijakan dan prosedur terkait business continuity management organisasi;
    e. mengoordinasikan penyusunan, pengujian, dan pemeliharaan *business continuity plan* dan *disaster recovery plan* organisasi;
    f. memastikan terjaganya aspek keamanan informasi dalam proses *business continuity management*.
9. Koordinator pengendalian dokumen dan kepatuhan SMKI memiliki tugas dan tanggung jawab sebagai berikut:
    a. mengoordinasikan dan memantau proses pengelolaan dokumentasi terkait SMKI organisasi hal ini mencakup kebijakan dan prosedur terkait SMKI organisasi;
    b. mengidentifikasi dan mendokumentasikan peraturan perundang-undangan dan kewajiban kontrak yang relevan dengan SMKI dan keamanan informasi organisasi;
    c. melakukan pemantauan berkala terhadap kepatuhan SMKI organisasi dengan prasyarat dari kebijakan dan prosedur SMKI organisasi serta peraturan perundang-undangan dan kewajiban kontrak yang relevan dengan SMKI dan keamanan informasi organisasi;
    d. menyusun dan mengoordinasikan pelaksanaan program *security awareness* bagi personil organisasi; dan
    e. menyusun metrik pengukuran efektivitas SMKI dan kontrol keamanan informasi organisasi.
10. Pengelolaan *Data Center* di lingkungan Pemerintah Daerah Kota harus ditetapkan dalam dengan keputusan yang berkekuatan hukum mengikat dalam Peraturan Wali Kota ini.
11. Pengelola *Data Center* tersebut berkewajiban melakukan pengamanan dan pemeliharaan berkelanjutan atas aset pengolahan serta penyimpanan informasi yang dikelola di *Data Center* dan aset informasi yang disimpan di *Data Center*.

12. Aset informasi yang merupakan isi (content) dari sistem informasi yang dimiliki oleh Perangkat Daerah, dikelola oleh Perangkat Daerah masing-masing sesuai kepemilikannya (*ownership*).
13. Penanggung jawab pemilik aset informasi adalah Kepala Perangkat Daerah terkait. pemilik aset informasi bertanggung jawab melakukan pengamanan dan pemeliharaan secara berkelanjutan atas aset informasi.
14. Perangkat Daerah harus menentukan tim keamanan informasi yang mempunyai tanggung jawab dalam berkoordinasi dengan pihak lain:
    a. mengidentifikasi pihak-pihak berwenang terkait keamanan informasi pada tingkat pemerintahan yang lebih tinggi (*PGCSIRT*, *Gov-CSIRT*, Kementerian Komunikasi dan Informatika, penegak hukum, *Indonesia Security Incident Response Team on Internet Infrastructure* (*IDSIRTII*), BSSN, dan sebagainya), serta menjalin kerja sama dalam rangka pelaporan dan koordinasi penanganan bersama atas gangguan keamanan informasi;
    b. tim keamanan informasi wajib berpartisipasi dalam keanggotaan komunitas atau forum yang relevan terkait keamanan informasi sebagai sarana meningkatkan keterampilan dan pengetahuan serta *best practice* terkini atas keamanan informasi; dan
    c. seluruh anggota Tim Keamanan Informasi dan pihak kedua wajib menandatangani Perjanjian Kerahasiaan (*Non-Disclosure Agreements*) yang mengikat para pihak untuk menjaga kerahasiaan aset informasi.

Kebijakan dalam penggunaan Perangkat *Mobile* dan *Teleworking*

1. Penggunaan perangkat *mobile*, baik milik pribadi atau milik Perangkat Daerah untuk mengakses dan/atau menyimpan informasi milik Perangkat Daerah harus sangat dibatasi sesuai dengan kebutuhan pekerjaan dengan mempertimbangkan prinsip-prinsip kehati-hatian saat menggunakan perangkat *mobile* dengan menghindari meninggalkan perangkat tanpa pengawasan.
2. Perangkat *mobile* harus mengaktifkan fitur otentikasi pengguna, seperti penggunaan *user name* dan *password*, sesuai dengan kebijakan terkait pengendalian akses.
3. Informasi sensitif harus dienkripsi atau dilindungi dengan *password* pada saat disimpan di *mobile device*, sesuai dengan klasifikasi informasinya.
4. Informasi sensitif milik Perangkat Daerah yang disimpan pada perangkat *mobile device* harus di-*backup* secara berkala untuk menghindari hilangnya aspek ketersediaan dari informasi.

5. Aktivitas *teleworking* sebagai sarana pegawai untuk bekerja dari lokasi di luar area kerja Perangkat Daerah dengan mengakses jaringan internal secara remote melalui jaringan *internet* diperbolehkan namun sangat dibatasi hanya untuk personil yang diberi izin berdasarkan kebutuhan pekerjaannya.
6. Akses ke jaringan internal Perangkat Daerah dari jaringan *internet* harus menggunakan koneksi aman dengan menggunakan antara lain teknologi *VPN*.
7. Kebijakan terkait teknologi *teleworking* sebagai sarana pegawai bekerja pada lokasi di luar Perangkat Daerah dengan mengakses jaringan internal Perangkat Daerah. Teknologi ini diperbolehkan untuk digunakan dalam kondisi sebagai berikut:
   a. perangkat akses (misalnya komputer, *notebook*) yang digunakan untuk *teleworking* harus terinstalasi *firewall* dan *antivirus*;
   b. mekanisme akses terhadap sistem atau aplikasi disesuaikan dengan klasifikasi aset informasi:

1) informasi publik : dapat diakses langsung.

2) informasi rahasia :

- harus menggunakan protokol *HTTPS* atau *SSH*; dan
- harus menggunakan *VPN*, sebelum kemudian mengakses melalui protokol *HTTPS* atau *SSH*.

BAB V

KEAMANAN SUMBER DAYA MANUSIA

A. Tujuan

Kebijakan keamanan sumber daya manusia ditetapkan untuk memberikan pedoman dalam mengelola keamanan sumber daya manusia dalam ruang lingkup SMKI di Pemerintah Daerah Kota.

B. Ruang Lingkup

Ruang lingkup kebijakan keamanan sumber daya manusia terdiri dari:

1. pegawai dalam lingkungan Pemerintah Daerah Kota;
2. pegawai dari pihak eksternal yang dalam aktivitas pekerjaannya memiliki akses ke aset informasi dan aset pengolahan dan penyimpanan informasi dalam lingkungan Pemerintah Daerah Kota.

C. Kebijakan

1. Calon pegawai di lingkungan Pemerintah Daerah Kota dan pegawai dari pihak eksternal, harus melalui proses *screening* untuk memastikan bahwa mereka sesuai dengan tugas dan tanggung jawab yang akan mereka dapatkan.
2. Proses screening perlu mencakup verifikasi terhadap latar belakang kandidat sesuai dengan peraturan perundang-undangan serta etika yang ada.
3. Pegawai dalam lingkungan Pemerintah Daerah Kota dan pegawai dari pihak eksternal yang dalam aktivitas pekerjaannya memiliki akses ke aset informasi dan aset pengolahan dan penyimpanan informasi dalam lingkungan Pemerintah Daerah Kota harus menandatangani perjanjian kerahasiaan (*non-disclosure agreement*) dengan memperhatikan tingkat sensitivitas dari aset yang diakses.
4. Setiap pegawai internal maupun eksternal harus mematuhi seluruh kebijakan dan prosedur Perangkat Daerah terkait keamanan informasi.
5. Setiap pegawai internal maupun eksternal harus diberikan informasi yang memadai terkait tugas dan tanggung jawab terkait keamanan informasi yang mereka miliki.
6. Program peningkatan kesadaran keamanan informasi (*awareness*) secara berkelanjutan untuk menjaga dan meningkatkan kesadaran keamanan informasi dari pegawai harus dilaksanakan.
7. Setiap pelanggaran terhadap kebijakan dan prosedur terkait keamanan informasi harus ditindaklanjuti dan apabila diperlukan, tindakan pendisiplinan harus diambil sesuai dengan peraturan yang berlaku.

8. Tanggung jawab dan kewajiban terkait keamanan informasi yang tetap berlaku setelah pemberhentian atau perubahan status kepegawaian harus didefinisikan, dikomunikasikan, dan ditegakkan kepada pegawai internal maupun eksternal.
9. Hal ini mencakup tanggung jawab keamanan informasi yang tercakup dalam perjanjian kerja seperti:
    a. Seluruh aset organisasi harus dikembalikan setelah pemberhentian kepegawaian;
    b. Seluruh hak akses organisasi harus dinonaktifkan atau dihapus setelah pemberhentian kepegawaian; dan
    c. Seluruh hak akses organisasi harus disesuaikan setelah perubahan status kepegawaian.

BAB VI

PENGELOLAAN ASET

A. Tujuan

Pengelolaan aset informasi bertujuan untuk memberikan pedoman dalam mengelola aset yang terkait informasi serta fasilitas fisik pengolahan informasi, sehingga aset informasi mendapatkan perlindungan yang sesuai dengan tingkat kepentingannya.

B. Ruang Lingkup

Ruang lingkup kebijakan terkait pengelolaan aset informasi terdiri dari:

1. klasifikasi, pelabelan dan penanganan informasi dalam ruang lingkup Peraturan Wali Kota terkait SMKI; dan
2. penanganan aset pengolahan dan penyimpanan informasi dalam ruang lingkup Peraturan Wali Kota.

C. Kebijakan

1. Kepala Dinas Komunikasi dan Informatika Kota Bogor menetapkan pemilik aset informasi di setiap unit Perangkat Daerah, beserta perangkat fisik pengolah informasi yang terkait.
2. Pemilik aset informasi memiliki tanggung jawab untuk:
   a. mengidentifikasi seluruh aset informasi dan fasilitas pengolahan dan penyimpanan informasi;
   b. mendokumentasikannya dalam daftar inventaris aset SMKI, serta senantiasa memperbaharui daftar inventaris aset SMKI tersebut sesuai kondisi terkini; dan
   c. memastikan bahwa setiap aset telah diklasifikasikan dan dilindungi secara memadai.
3. Aset pengolahan dan penyimpanan informasi yang diinventaris adalah aset dalam bentuk:
   a. perangkat keras, meliputi perangkat keras yang digunakan untuk mengolah dan menyimpan informasi dalam bentuk fisik maupun elektronik, yang mencakup namun tidak terbatas pada komputer, *notebook, server*, *harddisk drive, USB disk*;
   b. perangkat lunak, meliputi perangkat lunak yang digunakan untuk mengolah informasi dalam bentuk elektronik, yang mencakup namun tidak terbatas pada sistem operasi, aplikasi, dan *database*;
   c. perangkat jaringan, meliputi perangkat keras dan lunak yang digunakan untuk membentuk dan infrastruktur jaringan telekomunikasi, yang mencakup namun tidak terbatas pada *hub, switch, router, firewall, IDS, IPS,* dan *network monitoring tools*;

d. perangkat pendukung meliputi perangkat digunakan untuk mendukung operasional perangkat pengolahan dan penyimpanan informasi yang mencakup namun tidak terbatas pada genset, *UPS, AC*, rak *server,* lemari penyimpanan informasi, dan *CCTV*;

e. layanan, meliputi layanan yang digunakan untuk mendukung operasional perangkat pengolahan dan penyimpanan informasi yang mencakup namun tidak terbatas pada layanan jaringan komunikasi, layanan *hosting* dan *co-location*, layanan pemeliharaan perangkat dan sistem, dan layanan pemasangan infrastruktur; dan

f. sumber daya manusia meliputi personil baik internal maupun eksternal yang terlibat dalam pengolahan dan penyimpanan informasi.

4. Pemilik aset dapat mendelegasikan tugas pengamanan dan pemeliharaan aset kepada kustodian aset, namun tanggung jawab akhir terhadap aset tetap berada pada pemilik aset.

5. Aset pengolahan dan penyimpanan informasi harus secara berkala dipelihara dengan memadai.

6. Apabila dalam pemeliharaan aset pengolahan dan penyimpanan informasi tersebut harus menggunakan jasa pihak ketiga penyedia, maka:

   a. kontrak pemeliharaan perlu dibuat dengan pihak ketiga penyedia jasa yang kompeten dan relevan; dan

   b. peralatan yang dibawa keluar untuk pemeliharaan harus diperiksa untuk mencegah kebocoran informasi.

7. Dalam proses penghapusan aset harus dilakukan secara aman dengan metode yang dapat mencegah kebocoran informasi seperti menghancurkan secara fisik *harddisk drive*.

8. Semua aset informasi dan pengolahan dan penyimpanan informasi milik Pemerintah Daerah Kota harus dikembalikan setelah personil pengguna tidak memiliki hubungan kepegawaian lagi dengan Pemerintah Daerah Kota, misalnya karena pengunduran diri, pensiun.

9. Ketentuan dalam proses pengembalian aset tersebut mencakup:

   a. pengembalian aset harus terdokumentasi secara formal;

   b. untuk pengembalian aset yang disebabkan oleh terhentinya status kepegawaian, informasi yang tersimpan dalam aset harus di-*backup* dan informasi yang tersimpan dalam aset harus dihapus secara aman, antara lain dengan *secureformat* atau melakukan instalasi ulang sistem operasi secara menyeluruh; dan

   c. media penyimpanan *backup* informasi harus diamankan secara fisik, antara lain dengan menyimpan dalam lemari terkunci dengan akses yang terbatas.

4. Aset pengolahan informasi, seperti komputer dan laptop yang akan digunakan kembali baik oleh pihak internal maupun eksternal harus diperiksa untuk menjamin tidak ada informasi sensitif yang tersimpan dalam aset tersebut.

5. PERANGKAT DAERAH harus mendefinisikan klasifikasi aset informasi dengan mempertimbangkan sebagai berikut:

   a. Aset informasi diklasifikasikan berdasarkan tingkat sensitivitas informasi serta tingkat kritikalitas sistem, yang meliputi:

      1) klasifikasi aset informasi secara berkala; dan

      2) pengguna yang diijinkan mengakses aset informasi.

   b. pemberian label klasifikasi informasi harus dilakukan secara konsisten terhadap seluruh aset informasi;

   c. klasifikasi aset informasi dan seberapa tingkat kerahasiaan aset informasi, didefinisikan sesuai ketentuan peraturan perundang-undangan, diuraikan sesuai tabel berikut:

Klasifikasi Aset Informasi	**Deskripsi**
Rahasia *(Confidential)*	Aset informasi yang sangat peka dan berisiko tinggi yang pembocoran atau penyalahgunaan akses terhadapnya bisa mengganggu kelancaran operasional secara temporer atau mengganggu citra dan reputasi instansi.
Internal *(Internal Use Only)*	Informasi yang telah terdistribusi secara luas di lingkungan internal instansi/lembaga yang penyebarannya secara internal tidak lagi memerlukan izin dari pemilik informasi dan risiko penyebarannya tidak menimbulkan kerugian signifikan.
Publik	Aset informasi yang secara sengaja dipublikasikan secara luas, merupakan informasi yang wajib disediakan dan diumumkan secara berkala, informasi yang wajib diumumkan secara serta-merta, dan informasi yang wajib tersedia setiap saat.

6. Untuk kepentingan penyelenggaraan pengelolaan aset informasi dalam kebijakan Sistem Manajemen Keamanan Informasi perlu diberikan penjelasan contoh-contoh aset informasi rahasia dan internal yaitu:

Klasifikasi **Aset Informasi**	**Contoh**
Rahasia *(Confidential)*	*User ID, password, Personal Identification Number (PIN), Log* sistem, hasil *penetration test*, data konfigurasi sistem, *Internet Protocol Address* (IP *Address*)
Internal *(Internal Use Only)*	Panduan penggunaan sistem dan aplikasi, kebijakan dan prosedur SMKI, dokumen *Business Continuity Plan.*

7. Setiap pemilik informasi harus memperhatikan keamanan informasi yang tersimpan dalam media penyimpanan informasi antara lain:
   a. dalam hal data yang tersimpan di dalam media bersifat rahasia, perlu diberikan proteksi kata sandi untuk melindungi data;
   b. dalam hal tidak lagi dibutuhkan atau digunakan, seluruh data yang tersimpan di dalam media harus sepenuhnya dihapus sehingga tidak lagi dapat dipulihkan;
   c. data yang tersimpan di dalam media yang akan dibuang harus mendapatkan perlakuan khusus guna meminimalkan terjadinya kebocoran informasi kepada pihak yang tidak sah yaitu:
      1) data yang tersimpan di dalam media yang memuat informasi rahasia harus dibuang dengan cara dihancurkan atau dibakar; dan
      2) data yang tersimpan di dalam media yang memuat informasi lainnya harus dilakukan penghapusan total dengan cara-cara tertentu yang tidak lagi dapat dipulihkan.
8. Panduan terkait pelabelan dan penanganan aset informasi berdasarkan klasifikasi aset informasi adalah sebagai berikut:

Klasifikasi Tipe	Publik	Internal	Rahasia
Dokumen dan catatan (record) dalam bentuk non elektronik (hardcopy).	Tidak diperlukan penanganan khusus.	Diberi label "***Internal***".	Diberi label "**Rahasia**"
Map penyimpan dokumen.	Tidak diperlukan penanganan khusus.	Tidak diperlukan penanganan khusus.	Diberi label "***Rahasia***"
Amplop pengiriman surat internal (di dalam kantor).	Tidak diperlukan penanganan khusus.	Tidak diperlukan penanganan khusus.	Amplop diberi label "***Rahasia***"
Amplop untuk surat eksternal (ke luar kantor).	Tidak diperlukan penanganan khusus.	• Pada amplop ditandai "*Internal*"	• Menggunakan 2 amplop, dimana Amplop pertama Dimasukkankedalam amplop kedua; • Pada amplop pertama ditandai "Rahasia", dan pada amplop kedua tidak diberikan tanda apapun.
Dokumen dan catatan (*record*) dalam bentuk elektronik (*softcopy*).	Tidak diperlukan penanganan khusus.	Memberikan label “Internal” pada bagian awal dari nama *file* atau pada bagian tertentu dari *file properties*.	Memberikan label “Rahasia” pada bagian awal dari nama *file* atau pada bagian tertentu dari *file properties*.

Publikasi / Distribusi	Tidak ada pembatasan.	• Tersedia untuk personil internal Perangkat Daerah pemilik informasi. • Distribusi kepada pihak eksternal dibatasi berdasakan kebutuhan pekerjaan maupun operasional di lingkungan Pemerintah Daerah. • Distribusi kepada pihak eksternal perlu seijin pemilik informasi. • Sensitifitas dan kritikalitas informasi perlu diberitahukan kepada pihak eksternal.	• Distribusi kepada pihak eksternal sangat dibatasi untuk kebutuhan pekerjaan. • Apabila memungkinkan, informasi rahasia tidak disalin oleh pihak eksternal (eyes only). • Distribusi kepada pihak eksternal perlu seijin pemilik Informasi. • Sensitifitas dan kritikalitas informasi perlu diberitahukan kepada pihak eksternal. • Pihak ketiga harus disertai perjanjian kerahasiaan (NDA – *non disclosure agreement*).

Pencetakan informasi	Tidak ada pembatasan.	Dibatasi hanya untuk kebutuhan internal.	• Pencetakan hanya pada *printer* organisasi dan diusahakan tidak mencetak menggunakan jasa pencetakan eksternal.
Surat menyurat internal (di dalam kantor)	Pastikan nama dan alamat tujuan sudah benar.	• Pastikan nama dan alamat tujuan sudah benar. • Mengikuti ketentuan penggunaan amplop untuk surat internal.	• Pastikan nama dan alamat tujuan sudah benar. • Mengikuti ketentuan penggunaan amplop untuk surat internal. • Menginformasi- kan kepada penerima akan pengiriman informasi tersebut. • Mengkonfirmasi kepada penerima bahwa informasi yang dikirim sudah diterima.

Surat menyurat eksternal (ke luar kantor)	Pastikan nama dan alamat tujuan sudah benar	• Pastikan nama dan alamat tujuan sudah benar. • Mengikuti ketentuan penggunaan amplop untuk surat eksternal. • Menggunakan jasa kurir pengiriman tercatat dengan tanda pengiriman.	• Pastikan nama dan alamat tujuan sudah benar. • Mengikuti ketentuan penggunaan amplop untuk surat eksternal. • Menggunakan jasa kurir pengiriman tercatat dengan tanda pengiriman. • Menginformasikan kepada penerima akan pengiriman informasi tersebut. • Mengkonfirmasi kepada penerima bahwa informasi yang dikirim sudah diterima.

Pengiriman ke pihak internal melalui email	• Pengiriman *e-mail* harus menggunakan account *e-mail* Perangkat Daerah/ Unit Kerja • Tidak diperlukan penangan-an khusus.	• Pengiriman *e-mail* harus menggunakan account *e-mail* Perangkat Daerah/Unit Kerja • Pastikan alamat *email* tujuan sudah benar. • Pengiriman informasi, termasuk forwarding / meneruskan *e-mail* hanya boleh dilakukan oleh pemilik informasi.	• Pengiriman *e-mail* harus menggunakan account *e-mail* Perangkat Daerah/Unit Kerja • Memberi *password* pada informasi yang dikirim melalui *e-mail* dan *password* diinformasikan kepada penerima secara terpisah. • Tidak mencantumkan informasi rahasia di *body text e-mail* • Pengiriman informasi, termasuk *forwarding* / meneruskan *e-mail* hanya boleh dilakukan oleh pemilik informasi.

Pengiriman ke pihak eksternal melalui e-mail	• Pengiriman *e-mail* harus mengguna-kan *account e-mail* Perangkat Daerah/ Unit Kerja • Tidak diperlukan penangan-an khusus.	• Pengiriman *e-mail* harus menggunakan *account e-mail* Perangkat Daerah/Unit Kerja • Pastikan alamat email tujuan sudah benar.	• Tidak disarankan menggunakan *e-mail* untuk mengirim informasi dengan klasifikasi ini. • Pengiriman *e-mail* harus menggunakan *account e-mail* Perangkat Daerah/Unit Kerja • Pastikan alamat e-mail tujuan sudah benar. • Memberi *password* pada informasi yang dikirim melalui *e-mail* dan *password* diinformasikan kepada penerima secara terpisah
Penyimpanan informasi *hardcopy*	Tidak diperlukan penanganan khusus	Tidak diperlukan penanganan khusus	Disimpan secara aman dalam tempat penyimpanan yang terkunci.

Penyimpanan informasi softcopy	Tidak diperlukan penanganan khusus	Tidak diperlukan penanganan khusus	• Penyimpanan pada komputer atau media penyimpanan harus yang menggunakan password. • File yang disimpan harus diberi password. • Media penyimpanan eksternal (*externalhard disk*, atau *flashdisk*) Harus disimpan pada tempat penyimpanan yang terkunci.
Penyimpanan pada pihak ketiga	Tidak diperlukan penanganan khusus	Harus disertai dengan perjanjian kerahasiaan (non disclosure agreement - NDA).	Harus disertai dengan perjanjian kerahasiaan (non disclosure agreement - NDA).
Penghancuran (*disposal*)	• Tidak diperlukan penangan-an khusus. • Masih dapat digunakan Kembali sebagai kertas untuk pekerjaan (scrap paper).	• Memperhati-kan masa retensi informasi yang disetujui oleh pemilik informasi. • Masih dapat digunakan Kembali untuk kebutuhan mencetak informasi dengan klasifikasi yang sama.	• Memperhatikan masa retensi informasi yang disetujui oleh pemilik informasi • Dihancurkan dengan metode pemusnahan dan informasi tidak dapat diakses Kembali (dihancurkan secara fisik atau secure format).

Pengamanan pada komputer penyimpan informasi	Tidak diperlukan penanganan khusus.	• *Screen saverlock* harus aktif jika meninggal-kan komputer/ terminal. • *Sign-off* komputer/ terminal jika tidak digunakan atau pulang kerja.	• *Screen saverlock* harus aktif jika meninggalkan komputer/ terminal. • *Sign-off* komputer/ terminal jika tidak digunakan atau pulang kerja. • *File* perlu dienkripsi/ *password*.
Kehilangan atau kebocoran informasi	Tidak diperlukan penanganan khusus.	Harus dilaporkan kepada pemilik informasi	Harus dilaporkan kepada pemilik informasi dan Perangkat Daerah Pengelola insiden keamanan informasi di lingkungan Pemerintah Daerah.

9. Informasi yang dianggap kritikal oleh Perangkat Daerah harus di-*backup* secara memadai untuk menjamin ketersediaannya.
10. Hal yang perlu dipertimbangkan dalam proses *backup* informasi meliputi:
    a. pemilik informasi bertanggung jawab untuk menentukan informasi yang membutuhkan *backup*, frekuensi dan metode *backup* serta waktu retensi untuk setiap *backup* informasi yang ada;
    b. pernyataan formal terkait informasi yang dibutuhkan untuk di-*backup* beserta metode dan frekuensi dari *backup* harus ditentukan bersama dengan personil yang bertugas melaksanakan proses *backup* serta harus dinyatakan secara jelas dalam sebuah rencana *backup* resmi;

c. *backup* informasi harus disimpan sesuai dengan masa retensi dari informasi utama;

d. masa retensi harus dinyatakan secara jelas dalam rencana *backup*; dan

e. perlindungan terhadap *backup* informasi harus dilakukan berdasarkan klasifikasi dari informasi utama.

11. Perangkat Daerah menyediakan akses internet dan *e-mail* kepada pegawainya hanya untuk kebutuhan pekerjaan dan operasional Pemerintah.

12. Ketentuan dalam penggunaan *internet* dan *e-mail* adalah sebagai berikut:

    a. pengguna dilarang menggunakan akses internet dan *e-mail* Perangkat Daerah untuk kegiatan melanggar hukum dan aktifitas yang dapat membahayakan keamanan jaringan Pemerintah;

    b. pengguna dilarang untuk menggunakan akses *internet* dan *e-mail* Perangkat Daerah untuk mengakses, mendistribusikan, mengunggah, dan/atau mengunduh:

        1) materi pornografi;

        2) materi bajakan seperti, perangkat lunak, *file* music, dan video/film;

        3) materi yang melecehkan, mendiskriminasikan, yang membakar emosi atau menimbulkan kebencian atau membuat pernyataan palsu atau yang bersifat merusak mengenai orang lain;

        4) situs yang dapat menimbulkan risiko serangan *malware*, penyusupan, atau *hacking* ke jaringan Pemerintah.

13. Pengguna disarankan untuk tidak membagi informasi pribadi melalui situs *internet* atau media sosial.

14. Pengguna dilarang untuk mendistribusikan informasi pemerintah yang bersifat rahasia tanpa izin dari pemilik informasi.

15. Pesan penyangkalan ini harus dituliskan pada akhir setiap *e-mail*. "Pesan ini mungkin berisi informasi rahasia dan hanya ditujukan kepada pihak yang dituju. Apabila anda bukanlah pihak yang dituju, anda dilarang untuk mengungkapkan, menyebarkan atau menyalin isi *e-mail* ini. Apabila anda mendapatkan *e-mail* ini tanpa sengaja mohon segera hubungi pengirim *e-mail* dan hapus *e-mail* ini segera. Pemerintah Daerah tidak bertanggung jawab untuk pengiriman informasi ini secara lengkap dan tepat dan juga tidak bertanggung jawab untuk keterlambatan dalam pengiriman *e-mail* ini."

16. Perangkat Daerah yang mengelola akun *e-mail* Perangkat Daerah berhak untuk mem-*block* akun *e-mail* pemerintah pada saat terdapat bukti memadai terkait penyalahgunaan dan/atau pelanggaran keamanan.

BAB VII

PENGENDALIAN AKSES

A. Tujuan

Tujuan dari pengendalian akses adalah untuk:

1. membatasi akses terhadap informasi serta fasilitas fisik (*Data Center*);
2. memastikan sistem dan aplikasi diakses oleh pengguna yang telah diotorisasi, serta mencegah akses oleh yang tidak berhak; dan
3. memastikan pengguna bertanggung jawab untuk melindungi informasi otentikasi sensitif masing-masing.

B. Ruang Lingkup

Ruang Lingkup dari pengendalian akses adalah akses ke aset informasi dan aset pengolahan dan penyimpanan informasi dalam lingkungan Pemerintah Daerah Kota yang mencakup:

1. persyaratan pengendalian akses;
2. pengendalian akses jaringan;
3. pengelolaan akses pengguna;
4. tanggung jawab pengguna; dan
5. pengendalian akses atas sistem dan aplikasi.

C. Kebijakan

1. Persyaratan pengendalian akses pada suatu sistem meliputi:
    a. akses ke aset informasi serta aset pengolahan dan penyimpanan informasi dalam lingkungan Pemerintah Daerah Kota harus dikendalikan menggunakan metode pengendalian akses yang memadai;
    b. pemberian hak akses dikelola secara formal pada seluruh siklusnya, mulai dari proses pengajuan, persetujuan, serta pencabutan, serta dilaksanakan oleh para pihak terkait sesuai jenjang kewenangannya;
    c. pengguna yang mengakses sistem informasi dalam lingkungan Pemerintah Daerah Kota diharuskan untuk mengotentikasi dirinya dengan menggunakan kombinasi *user ID* dan informasi otentikasi pribadi seperti *password* atau *PIN*;
    d. pengembangan aturan pemberian akses perlu mempertimbangkan:
        1) klasifikasi dari informasi;
        2) kritikalitas dari aset yang digunakan untuk mendukung operasional bisnis;

3) prasyarat perundang-undangan, kontraktual, serta keamanan yang relevan; dan

4) didasarkan atas prinsip *need to know* dan *need to use*, yaitu disesuaikan dengan kebutuhan pekerjaan dan operasional dalam lingkungan Pemerintah Daerah Kota;

e. aturan pemberian akses harus dikembangkan dan didokumentasikan oleh setiap pemilik sistem dalam bentuk daftar atau matriks akses;

f. peninjauan terhadap aturan pemberian akses harus dilakukan oleh pemilik aset/sistem secara berkala tergantung tingkat kritikalitas sistem tersebut;

g. peninjauan terhadap hak akses pengguna harus didokumentasikan secara formal; dan

h. setiap penyimpangan yang ditemukan dalam proses peninjauan harus segera diperbaiki dengan cara menyesuaikan atau mencabut hak akses yang menyimpang.

2. Pengendalian akses jaringan di lingkungan Perangkat Daerah meliputi:

a. penggunaan layanan jaringan (*network services*) hanya diperbolehkan secara terbatas, sesuai kebutuhan ketugasan dan kepentingan Perangkat Daerah, layanan lainnya yang tidak diperlukan harus dinonaktifkan;

b. jaringan komunikasi dalam lingkungan Perangkat Daerah harus dipisahkan kedalam *domain* jaringan yang terpisah sesuai dengan kebutuhan bisnis dan operasional, dalam rangka untuk mengamankan jaringan internal Perangkat Daerah dan aset di jaringan tersebut;

c. akses secara *remote* ke jaringan internal Perangkat Daerah dari jaringan publik harus sangat dibatasi baik dari perangkat yang digunakan maupun waktu untuk kebutuhan *troubleshooting* dan harus dilakukan melalui *secure channel*, antara lain dengan menggunakan teknologi *VPN*; dan

d. pemberian akses pengguna terhadap jaringan, baik *LAN* maupun *WAN*, dilakukan melalui mekanisme formal.

3. pengelolaan akses terhadap pengguna di Perangkat Daerah harus memenuhi ketentuan sebagai berikut:

a. pemilik aset informasi harus memiliki manajemen identitas pengguna yang mencakup proses pendaftaran dan terminasi pengguna yang didalamnya termasuk:

1) identitas pengguna (*user account*) harus unik, melekat ke setiap individu tunggal, sehingga setiap tindakan pengguna dapat dipertanggungjawabkan;

2) tidak diijinkan menggunakan satu identitas pengguna yang digunakan secara bersama-sama oleh lebih dari 1 (satu) individu, kecuali untuk tujuan tertentu yang sebelumnya harus mendapatkan persetujuan dari pihak berwenang; dan

3) memastikan secara berkala bahwa tidak ada identitas pengguna yang terduplikasi atau redundan sehingga seluruh identitas pengguna aktif adalah sesuai dengan pegawai Perangkat Daerah aktif.

b. pendaftaran, modifikasi, dan pencabutan hak akses pengguna mencakup proses pembuatan *user ID*, memberikan hak akses kepada *user ID* serta mencabut hak akses dan *user ID*.

c. pendaftaran, modifikasi dan pencabutan hak akses pengguna harus disetujui oleh atasan dari pengguna yang memohon hak akses tersebut dan pemilik informasi dan/atau sistem. Persetujuan tersebut harus diberikan sesuai dengan aturan pemberian akses.

d. identitas pengguna harus diotorisasi secara formal oleh pejabat berwenang pada pemilik aset informasi. Akses atas sistem dan aplikasi hanya dapat diaktifkan jika proses otorisasi telah selesai.

e. identitas pengguna pada sistem, seperti *user ID*, harus bersifat unik untuk memungkinkan mengidentifikasi dan meminta pertanggungjawaban pengguna.

f. pemberian informasi otentikasi suatu pengguna yang bersifat rahasia harus dilakukan melalui proses formal yang mencakup:

1) informasi otentikasi perdana yang diberikan untuk pertama kalinya adalah bersifat sementara, dimana pengguna wajib menggantinya pada kesempatan pertama mengakses sistem atau aplikasi; dan

2) informasi otentikasi bawaan (*default*) dari penyedia barang/jasa harus segera diganti pada saat instalasi sistem atau aplikasi;

g. pemilik aset harus melakukan tinjauan secara berkala atas seluruh hak akses pengguna secara berkala, dengan tambahan tinjauan insidental yang dilakukan pada saat:

1) terjadinya proses kepegawaian, seperti promosi, mutasi, terminasi; dan

2) terjadinya perubahan struktur organisasi.

h. hak akses khusus (*privileged access rights*) dari sistem informasi dalam lingkungan Perangkat Daerah, seperti administrator, *root*, hak akses untuk memodifikasi *database* atau hak akses untuk membuat, memodifikasi, atau mencabut pengguna dalam sistem aplikasi, harus sangat dibatasi kepada personil yang terotorisasi.

i. Hak akses khusus harus disetujui dan didokumentasikan secara formal.

j. Alokasi dari hak akses khusus harus ditinjau secara berkala dan setiap terdapat perubahan dalam status penggunaan akses tersebut.

k. Setiap penyimpangan yang ditemukan dalam proses peninjauan harus segera diperbaiki dengan menyesuaikan atau menghapus hak akses khusus yang menyimpang.

l. Apabila memungkinkan, hak akses khusus harus dialokasikan secara individual dan tidak di-*share*. Hal ini dilakukan untuk menjamin akuntabilitas dari pengguna khusus.

m. apabila hak akses khusus tidak bisa dialokasikan secara individual, kontrol tambahan seperti *dual custody*, harus diimplementasikan untuk menghindari penyalahgunaan.

n. jejak audit (*log*) untuk hak akses khusus pada sistem informasi dalam lingkungan Pemerintah Daerah Kota harus diaktifkan.

4. Setiap pengguna harus mempunyai tanggung jawab dalam penggunaan *User ID* dan *password* yaitu:

a. pengguna harus menjaga kerahasiaan dan keamanan *password* pribadi atau kelompok serta informasi otentikasi rahasia lainnya*;*

b. pengguna harus segera mengganti informasi otentikasi rahasia jika terindikasi bahwa informasi tersebut telah diketahui oleh orang lain;

c. *password* yang diberikan untuk pertama kalinya adalah bersifat sementara, dimana pengguna wajib menggantinya pada kesempatan pertama pada saat mengakses sistem atau aplikasi;

d. *password* untuk mengakses sistem informasi dalam lingkungan Perangkat Daerah harus memiliki karakteristik sebagai berikut:

1) memiliki panjang minimum 8 karakter;

2) mengandung kombinasi huruf besar, huruf kecil, dan nomor;

3) tidak terdiri dari kata atau nomor yang mudah ditebak seperti *password*, admin, 12345678 atau abc123; dan

4) tidak terdiri dari informasi pribadi seperti ulang tahun pengguna, nama perusahaan, atau nama pengguna;

e. *password* untuk mengakses sistem informasi dalam lingkungan Pemerintah Daerah Kota harus diganti paling sedikit setiap 3 (tiga) bulan sekali;

f. pada saat penggantian, *password* sebelumnya tidak boleh digunakan kembali sampai setelah 3 (tiga) siklus pergantian *password*;

g. prosedur *login* dari sistem harus menjamin keamanan dari *password* dengan cara:

   1) tidak menampilkan *password* yang dimasukkan; dan

   2) tidak menyediakan pesan bantuan pada saat proses *login* yang dapat membantu pengguna yang tidak berwenang;

h. pengguna wajib menggunakan kata sandi yang berbeda untuk keperluan ketugasan dan pribadi.

5. pengendalian akses sistem dan aplikasi yang dikelola oleh Perangkat Daerah meliputi:

   a. pemilik aset informasi harus memastikan bahwa sistem dan aplikasi dibawah pengelolaannya memiliki fasilitas manajemen hak akses pengguna, manajemen kata sandi yang baik, serta mekanisme otentikasi pengguna yang aman;

   b. fasilitas manajemen hak akses pengguna harus mampu membatasi akses informasi sesuai ketugasannya (*role based access control*);

   c. fasilitas manajemen kata sandi harus memastikan dihasilkannya kata sandi yang berkualitas yaitu:

      1) menegakkan akuntabilitas pengguna melalui penggunaan identitas pengguna tunggal untuk setiap individu;

      2) memberikan fasilitas penggantian kata sandi mandiri;

      3) membantu memberikan rekomendasi kata sandi yang berkualitas;

      4) mewajibkan pengguna untuk mengganti kata sandi pada saat pertama kali *login*;

      5) mewajibkan pengguna untuk mengganti kata sandi secara berkala;

      6) menyimpan riwayat kata sandi pengguna dan mencegah agar pengguna tidak menggunakan kata sandi yang sebelumnya telah digunakan;

      7) tidak menampilkan kata sandi saat sedang dientrikan; dan

      8) kata sandi disimpan dalam bentuk terlindungi (dienkripsi), demikian juga pada saat kata sandi ditransmisikan.

   d. mekanisme otentikasi pengguna perlu dirancang agar meminimalkan peluang terjadinya akses yang tidak sah, yaitu:

1) kata sandi tidak ditransmisikan melalui jaringan secara *plaintext*;

2) memiliki mekanisme penguncian sistem sementara sebagai perlindungan terhadap *brute force attacks*;

3) adanya pencatatan terhadap seluruh upaya otentikasi yang sukses dan gagal; dan

4) adanya pembatasan jumlah akses pengguna yang sama secara simultan;

e. Parameter otentikasi pengguna disesuaikan dengan klasifikasi aset informasi sebagai berikut:

Parameter Otentikasi	**Rahasia & Internal**	**Publik**
Jumlah gagal *login* sebelum penguncian	3	10
Durasi *timeout* sebelum terminasi sesi otomatis	5 menit	16 enit

6. penggunaan program *utility khusus* dalam operasional sistem di lingkungan Perangkat Daerah harus mempertimbangkan keamanan sebagai berikut yaitu penggunaan program *utility* khusus seperti *registry cleaner* atau *system monitoring* yang dapat mengambil alih kendali sistem/aplikasi atau mendapatkan hak akses khusus pada sistem/aplikasi harus sangat dibatasi berdasarkan kebutuhan operasional pengguna.

7. Perangkat Daerah yang mengelola aplikasi harus memastikan bahwa *source code* dikelola dan disimpan secara memadai baik yang dikembangkan oleh internal Perangkat Daerah maupun yang dikembangkan oleh penyedia jasa aplikasi.

8. Apabila *source code* dari penyedia jasa aplikasi tidak dapat diserahkan kepada pengelola aplikasi, Perangkat Daerah bersama penyedia jasa aplikasi tersebut harus mempertimbangkan *escrow* agreement untuk memastikan kelangsungan operasional sistem aplikasi jika ada pengembangan selanjutnya.

9. Pengendalian terhadap akses ke *source code* aplikasi sebagai berikut:

a. untuk sistem aplikasi yang dikembangkan secara internal dan/atau dibeli dengan *source code*, pengendalian akses harus diimplementasikan untuk mencegah akses tanpa izin ke *source code* tersebut.

b. pengendalian tersebut mencakup:

1) tidak menyimpan *source code* pada sistem operasional;
2) menyimpan *source code* pada lokasi fisik yang aman dari ancaman akses tanpa izin maupun ancaman kerusakan karena kondisi lingkungan;
3) membatasi akses secara fisik maupun logical ke *source code* program hanya kepada pengembang dan personil yang berwenang; dan
4) mengimplementasikan metode *versioning* dan proses manajemen perubahan untuk menjamin integritas dari *source code* aplikasi.

BAB VIII

KRIPTOGRAFI

A. Tujuan

Tujuan dari kebijakan terkait teknologi kriptografi adalah untuk memastikan penggunaan teknologi kriptograpi yang sesuai dan efektif untuk melindungi kerahasiaan, keaslian, dan/atau integritas dari informasi dalam lingkungan Pemerintah Daerah Kota.

B. Ruang Lingkup

Ruang Lingkup kebijakan terkait teknologi kriptografi adalah penggunaan teknologi kriptografi dalam pengolahan dan penyimpanan informasi di lingkungan Pemerintah Daerah Kota.

C. Kebijakan

1. kontrol kriptografi dapat digunakan untuk menjamin kerahasiaan dan integritas dari informasi sensitif di lingkungan Perangkat Daerah.
2. kontrol kriptografi dapat mencakup namun tidak terbatas pada:
    a. enkripsi informasi dan jaringan komunikasi;
    b. pemeriksaan integritas informasi, seperti *hashing*;
    c. otentikasi identitas; dan
    d. *digital signatures;*
3. implementasi dari kontrol kriptografi harus mempertimbangkan klasifikasi dari informasi yang akan diamankan.
4. pemilihan kontrol kriptografi harus mempertimbangkan:
    a. jenis dari kontrol kriptografi;
    b. kekuatan dari algoritma kriptografi; dan
    c. panjang dari kunci kriptografi.
5. implementasi dari kontrol kriptografi harus secara berkala ditinjau untuk memastikan kecukupan dan kesesuaian dari kontrol tersebut dalam mengamankan kerahasiaan dan integritas dari informasi.
6. pengelolaan dari kunci kriptografi harus dikendalikan secara ketat dan dibatasi hanya pada personil yang terotorisasi.
7. pengelolaan dari kunci kriptografi didasarkan pada prinsip *dual custody* untuk mengurangi risiko penyalahgunaan.

BAB IX

KEAMANAN FISIK DAN LINGKUNGAN

A. Tujuan

Tujuan dari kebijakan keamanan fisik dan lingkungan adalah untuk:

1. Mencegah akses atas aset informasi dan aset pengolahan dan penyimpanan informasi secara fisik oleh pihak yang tidak berwenang pada lingkungan Pemerintah Daerah Kota; dan
2. Mencegah terjadinya kerusakan atau gangguan pada aset informasi dan aset pengolahan dan penyimpanan informasi pada lingkungan Pemerintah Daerah Kota, karena ancaman dari kondisi lingkungan.

B. Ruang Lingkup

Ruang lingkup kebijakan keamanan fisik dan lingkungan adalah pengamanan fisik dan lingkungan bagi area kerja dan penyimpanan perangkat pengolahan dan penyimpanan informasi, seperti *Data Center*, *disaster recovery center* atau ruang arsip.

C. Kebijakan

1. Setiap area yang didalamnya terdapat informasi dan fasilitas pengolahan informasi Perangkat Daerah harus dilindungi dengan menerapkan pengamanan fisik pada perimeter area tersebut.
2. Setiap area harus merupakan akses terbatas, dimana akses masuk hanya diberikan bagi personil yang telah mendapatkan otorisasi. Mekanisme pembatasan ini dapat dilakukan aturan penerimaan tamu yang diterapkan berdasarkan kritikalitas area tersebut.
3. Untuk area *Data Center, disaster recovery center* dan ruang arsip Perangkat Daerah harus dilindungi dengan menerapkan pengamanan fisik pada perimeter area tersebut dengan kriteria:
    a. konstruksi dinding, atap, dan lantai yang kuat;
    b. pintu akses menuju area harus dilengkapi dengan mekanisme kontrol akses seperti: *access door lock*;
    c. pintu dan jendela harus senantiasa dalam kondisi terkunci, khususnya pada saat tanpa penjagaan;
    d. perangkat *CCTV* perlu terpasang pada sisi eksterior dan interior area;
    e. tidak diperbolehkan menyimpan bahan-bahan berbahaya yang mudah terbakar;
    f. area bongkar muat atau penerimaan barang harus diamankan dan dipantau untuk mencegah akses tanpa izin ke *Data Center, disaster recovery center* dan ruang arsip Pemerintah Daerah Kota; dan

g. *delivery* dari barang harus dilaporkan dan diperiksa sebelum barang tersebut dapat dipindahkan dari area bongkar muat atau penerimaan barang ke *Data Center, disaster recovery center* dan ruang arsip Pemerintah Daerah Kota.

4. Pengendalian akses pengunjung ke dalam area di lingkungan Perangkat Daerah harus memperhatikan keamanan fisik yang meliputi:
   a. kunjungan ke dalam area tersebut harus disetujui secara formal oleh pengelolaan area tersebut;
   b. selama kunjungan di dalam area tersebut, pengunjung harus senantiasa didampingi oleh petugas yang telah mendapatkan otorisasi;
   c. kartu identitas pengunjung perlu diverifikasi, disimpan oleh petugas selama kunjungan, dan dikembalikan sesudah selesai kunjungan; dan
   d. setiap pengunjung ke dalam area harus tercatat, mencakup jam masuk dan keluar, serta selalu dimonitor kesesuaiannya dengan rekaman *CCTV*.
5. Perangkat Daerah harus memperhatikan aspek pengamanan terhadap perangkat yang digunakan melalui:
   a. seluruh perangkat harus ditempatkan di lokasi yang aman, sedemikian rupa sehingga terlindungi dari terjadinya pencurian, akses oleh pihak yang tidak berwenang, kebakaran, air, debu, dan sebagainya;
   b. seluruh perangkat di dalam area harus dipelihara, diinspeksi sesuai spesifikasi perawatan berkala oleh pihak yang berwenang untuk menjamin keberlangsungan efektivitas fungsionalnya;
   c. pemeliharaan yang dilakukan oleh pihak kedua, harus dilaksanakan sesuai dengan kesepakatan tingkat layanan (*Service Level Agreement/SLA*) yang menjabarkan tingkat pemeliharaan dan kinerja yang harus dipenuhi pihak kedua;
   d. bagi pemeliharaan yang tidak dapat dilakukan di lokasi kantor Perangkat Daerah, maka informasi rahasia dan kritikal yang tersimpan dalam peralatan tersebut harus dipindahkan terlebih dahulu;
   e. pemeliharaan perangkat yang mengharuskan dibawa dari luar area harus atas persetujuan pejabat berwenang;
   f. peralatan pengolahan dan penyimpanan informasi yang tidak digunakan lagi oleh Pemerintah Daerah Kota, baik karena rusak, diganti, atau karena sebab lainnya harus dipastikan tidak lagi menyimpan informasi sensitif dan kritikal; dan
   g. media penyimpan informasi yang sudah tidak digunakan lagi harus dihancurkan, atau dihapus isinya agar tidak bisa dibaca dan digunakan lagi oleh pihak yang tidak berwenang.

6. Khusus pengamanan area fisik di *Data Center* harus mempertimbangkan hal-hal sebagai berikut*:*

   a. seluruh perangkat harus ditempatkan di lokasi yang aman, sedemikian rupa sehingga terlindungi dari terjadinya kebakaran, kebocoran, debu, dan sebagainya;

   b. seluruh perangkat di dalam *Data Center* harus dipelihara, diinspeksi sesuai spesifikasi perawatan berkala oleh pihak yang kompeten dan berwenang sesuai dengan rekomendasi dari pembuat perangkat tersebut;

   c. *Data Center* harus dilengkapi dengan *UPS*, generator listrik cadangan, perangkat pemadam kebakaran, dan diusahakan terdapat perlindungan kejut listrik (petir, tegangan tidak stabil);

   d. *Data Center* dan *disaster recovery center* dilengkapi dengan sistem sensor deteksi asap, air, suhu dan kelembaban, yang dapat terpantau;

   e. parameter temperatur dan kelembaban berikut perlu dijaga untuk *data center* meliputi:

      1) temperatur antara 18°-26° (delapan belas derajat sampai dengan dua puluh enam derajat) celcius;

      2) kelembaban (rh) antara 40%-60% (empat puluh persen sampai dengan enam puluh persen).

   f. kabel listrik dan jaringan telekomunikasi yang membawa data atau mendukung layanan sistem informasi harus dilindungi dari penyambungan yang tidak sah (penyadapan) atau kerusakan.

BAB X

KEAMANAN OPERASIONAL SISTEM INFORMASI

A. Tujuan

Tujuan dari kebijakan keamanan operasional sistem informasi adalah untuk:

1. memastikan pengoperasian aset pengolahan dan penyimpanan informasi di Pemerintah Daerah Kota secara benar dan aman;
2. memastikan terlindunginya aset informasi beserta aset pengolahan dan penyimpanan informasi di Pemerintah Daerah Kota dari ancaman *malware;*
3. melindungi terjadinya kehilangan atas aset informasi;
4. tersedianya catatan (*log*) atas aktivitas sistem informasi sebagai barang bukti; dan
5. mencegah terjadinya eksploitasi atas kelemahan sistem informasi pada Pemerintah Daerah Kota.

B. Ruang Lingkup

Ruang lingkup dari kebijakan keamanan operasional sistem informasi adalah pengoperasian aset pengolahan dan penyimpanan informasi di lingkungan Pemerintah Daerah Kota.

C. Kebijakan

1. Aktivitas operasional terkait fasilitas pengolahan informasi serta fasilitas komunikasi harus memiliki prosedur yang terdokumentasi dengan baik;
2. Prosedur operasional tersebut harus tersedia bagi pengguna yang memerlukannya;
3. Seluruh perubahan pada fasilitas pengolahan informasi yang dapat berimplikasi pada keamanan informasi, perlu diperlakukan secara terkendali mencakup antara lain:
    a. menyusun perencanaan mengenai perubahan yang mungkin terjadi serta melakukan pengujian terkait terpenuhinya persyaratan keamanan;
    b. melakukan kajian atas implikasi keamanan informasi yang mungkin terjadi;
    c. mengajukan persetujuan secara formal atas perubahan yang akan dilakukan; dan
    d. mencatat seluruh perubahan yang telah dilakukan.
4. Kinerja dan utilisasi atas fasilitas pengolahan informasi harus senantiasa dipantau dengan alat bantu peringatan dini, dioptimalkan pemanfaatannya, serta diproyeksikan kebutuhan kapasitasnya untuk masa yang akan datang.

5. Untuk mengurangi risiko perubahan tanpa izin atau penyalahgunaan hak akses, pemisahan fasilitas pengembangan, pengujian, dan operasional harus dilakukan.
6. Setiap sistem informasi di lingkungan Perangkat Daerah harus terlindungi dari *malware* secara memadai melalui:
   a. instalasi dari perangkat lunak *antivirus* pada sistem informasi;
   b. mem-*block* akses ke *website* yang dapat menimbulkan ancaman kepada sistem informasi;
   c. program peningkatan kesadaran bagi personil organisasi untuk menangani ancaman *malware*; dan
   d. setiap insiden terkait dengan *malware* harus dilaporkan kepada administrator sistem dan dikategorikan sebagai insiden keamanan informasi.
7. Seluruh aset informasi yang berada di dalam fasilitas pengolahan informasi wajib dilakukan *backup*, dengan persyaratan berikut:
   a. *backup* mencakup aplikasi, *database*, dan *system image*;
   b. frekuensi *backup* dilakukan secara harian, bulanan, dan tahunan;
   c. salinan *backup* harus disimpan secara aman sesuai dengan periode retensi. periode retensi *backup* adalah 1 (satu) tahun dimana:
      1) *backup* harian disimpan selama 31 (tiga puluh satu) hari;
      2) *backup* bulanan disimpan selama 12 (dua belas) bulan;
   d. seluruh hasil *backup* harus dilakukan uji *restore* secara berkala;
   e. media *backup* disimpan pada perangkat storage yang terpisah dari perangkat pengolahan informasi utama;
   f. *backup* merupakan tanggung jawab pengelola *Data Center*, sedangkan pengujian *restore* merupakan tanggung jawab pemilik aset informasi;
   g. parameter *backup* disesuaikan dengan klasifikasi sistem sebagai berikut:

Parameter Backup	**Klasifikasi Sistem**	
	Vital	***Sensitive/ Non-Sensitive***
Cakupan *Backup*	Aplikasi, *Database*	Aplikasi, *Database*

Frekuensi *Backup* *(Recovery Point Objective)*	Harian	Bulanan
Pengujian *Restore*	Triwulanan	Semesteran

8. Sistem harus dikonfigurasi untuk melakukan pencatatan (*logging*) atas seluruh aktivitas pengguna, jaringan, sistem, aplikasi, *error* yang terjadi (*exceptions*). Pemilik aset informasi harus menganalisis *log* terkait pola-pola penggunaan yang tidak wajar.
9. Fasilitas pencatatan *log* dan informasi *log* yang dicatat harus dilindungi dari penghapusan dan akses oleh pihak yang tidak berwenang.
10. Semua fasilitas pemrosesan informasi yang terhubung ke jaringan internal Perangkat Daerah harus disinkronisasi dengan sumber waktu yang akurat dan telah disepakati.
11. Proses dan prosedur untuk mengendalikan instalasi perangkat lunak pada sistem operasional harus ditetapkan dan diimplementasikan untuk memastikan terjaganya kerahasiaan, integritas, dan keterseiaan informasi.
12. Instalasi *software* harus dilakukan oleh administrator sistem yang relevan.
13. Pemilik aset informasi wajib melakukan upaya-upaya identifikasi atas kelemahan teknis (*vulnerabilities*) dari seluruh aset informasi dibawah pengelolaannya, serta melakukan tindakan pengendalian yang sesuai untuk meminimalkan risiko atas hilangnya aset informasi. Tindakan pengendalian dapat berupa penonaktifan fitur tertentu, perbaikan/*upgrade* sistem, aplikasi, atau *patching*.
14. Setiap sistem informasi di lingkungan Perangkat Daerah dapat dilakukan proses audit yang mencakup proses verifikasi terhadap sistem informasi dan/atau informasi Perangkat Daerah dengan mempertimbangkan sebagai berikut:
    a. harus direncanakan dan dikelola dengan baik untuk meminimalisasi gangguan terhadap proses bisnis;
    b. setiap proses audit yang membutuhkan akses kepada sistem informasi dan/atau informasi Perangkat Daerah harus disetujui oleh pemilik dari sistem dan/atau informasi tersebut;
    c. hak akses untuk kebutuhan audit harus dibatasi hanya hak akses *read only*; dan
    d. instalasi dari *tools* yang digunakan untuk proses audit hanya dapat dilakukan oleh personil yang berwenang yaitu administrator jaringan dan sistem teknologi informasi di Perangkat Daerah, dan harus segera dihapus setelah proses audit telah selesai dilakukan.

BAB XI

KEAMANAN KOMUNIKASI

A. Tujuan

Tujuan dari kebijakan keamanan komunikasi adalah untuk:

1. Memastikan perlindungan atas informasi pada jaringan komputer beserta fasilitas pendukung pengolahan informasi;
2. Menjaga keamanan informasi yang dipertukarkan, baik di dalam Perangkat Daerah maupun antar Perangkat Daerah eksternal.

B. Ruang Lingkup

Ruang lingkup dari kebijakan keamanan komunikasi adalah untuk:

1. Pengendalian jaringan;
2. Keamanan layanan jaringan;
3. Pemisahan jaringan; dan
4. Pertukaran informasi.

C. Kebijakan

1. Jaringan internal PERANGKAT DAERAH harus diamankan untuk menjamin:
   a. pencegahan akses tanpa izin ke jaringan, layanan jaringan dan fasilitas pemrosesan informasi dalam jaringan;
   b. keamanan dari informasi milik organisasi yang dikirimkan melalui jaringan; dan
   c. integritas dan ketersediaan dari layanan jaringan organisasi.
2. Tugas dan tanggung jawab untuk pengelolaan jaringan dan keamanan harus dialokasikan dan apabila memungkinkan dipisahkan dari penanggung jawab opersional sistem aplikasi dan *Data Center*.
3. Konfigurasi dari jaringan, perangkat aktif, dan perangkat keamanan jaringan harus ditinjau secara berkala untuk:
   a. memastikan kesesuaian dengan kondisi terkini; dan
   b. mengidentifikasi kerawanan pada jaringan, layanan jaringan, dan fasilitas pemrosesan informasi dalam jaringan.
4. Jaringan internal Perangkat Daerah harus dipisahkan dari jaringan eksternal dengan menggunakan *security gateway* atau *firewall* dan harus dikonfigurasikan untuk:
   a. memfilter *traffic* tanpa izin maupun *traffic* yang mencurigakan; dan
   b. apabila memungkinkan memfilter dan mencegah infeksi *malware* ke jaringan internal*;*

5. Koneksi ke *security gateway* atau *firewall* harus diotentikasikan, diotorisasi dan diamankan dengan metode pengamanan yang sesuai, misalnya dengan *virtual private network* (VPN), *secure shell* (SSH) atau metode kriptografi.
6. Kebijakan dan *log firewall* harus ditinjau paling sedikit 1 (satu) kali dalam 3 (tiga) bulan.
7. Koneksi eksternal harus diputuskan secara otomatis setelah tidak aktif selama 5 (lima) menit.
8. Akses dari jaringan eksternal yang dilakukan oleh vendor pihak ketiga hanya dapat diberikan untuk kebutuhan *troubleshooting* dan harus secara formal disetujui dan didokumentasikan dan harus dibatasi waktunya sesuai dengan kebutuhan dari akses.
9. Jaringan internal perusahaan harus disegmentasi baik secara fisik maupun *logical* untuk meningkatkan keamanan dan untuk mengendalikan akses dan *traffic* jaringan berdasarkan kritikalitas dari sistem dalam jaringan Perangkat Daerah.
10. Segmentasi jaringan harus ditinjau paling sedikit 1 (satu) kali dalam 3 (tiga) bulan untuk menjamin kesesuaian dengan prasyarat keamanan terkini.
11. *Routing* jaringan harus dilakukan berdasarkan pengendalian terhadap alamat sumber dan tujuan.
12. Tanggung jawab untuk merubah *routing* jaringan hanya diberikan kepada administrator jaringan yang diberi izin.
13. Aturan untuk *routing* harus ditinjau paling tidak 1 (satu) kali dalam 3 (tiga) bulan untuk mendeteksi dan mengoreksi adanya kesalahan atau *routing* tanpa otorisasi.
14. Perangkat jaringan harus ditempatkan pada lokasi yang aman untuk menghindari akses tanpa izin dan ancaman fisik maupun lingkungan.
15. Akses, baik fisik maupun *logical* ke perangkat jaringan harus dibatasi untuk tujuan administrasi dan pemeliharaan jaringan.
16. *Port* dan layanan jaringan, baik fisik maupun *logical*, yang tidak digunakan tidak boleh diaktifkan.
17. Akses ke *port* yang digunakan untuk kebutuhan *diagnostic* dan konfigurasi perangkat jaringan dan keamanan jaringan, seperti *console port*, harus sangat dibatasi dan diberikan kepada:
    a. administrator jaringan dan keamanan jaringan Perangkat Daerah;
    b. pihak ketiga yang telah disetujui dan bekerja untuk kepentingan Perangkat Daerah; dan
    c. aplikasi monitoring jaringan dan keamanan jaringan yang telah disetujui.

18. Semua perangkat jaringan harus dapat diidentifikasi secara fisik maupun logical dengan penamaan yang disepakati dan konsisten.
19. Perangkat jaringan yang dimiliki oleh pihak eksternal harus secara memadai dipisahkan dari perangkat jaringan milik Perangkat Daerah.
20. Mekanisme keamanan, tingkat layanan, dan prasyarat lain untuk semua layanan jaringan harus diidentifikasi dan dimasukkan kedalam perjanjian layanan jaringan.
21. Akses ke layanan jaringan Perangkat Daerah hanya diberikan kepada personil yang terotorisasi berdasarkan prinsip *need to have*.
22. Penggunaan pihak kedua penyedia layanan jaringan harus dimonitor untuk menjamin kesesuaian dengan prasyarat keamanan Perangkat Daerah.
23. Layanan jaringan organisasi harus diamankan menggunakan metode yang dapat mencakup metode otentikasi atau metode kriptografi yang kuat untuk menjamin keamanan dari pengiriman informasi menggunakan jaringan dan layanan jaringan.
24. Terkait aspek pertukaran informasi melalui fasilitas jaringan komunikasi, Perangkat Daerah harus memperhatikan perjanjian kerahasiaan merupakan perikatan formal antara pemilik aset informasi dengan penerima informasi, yang ketentuan di dalamnya memuat:
    a. pemberian izin penggunaan informasi dari pemilik aset informasi kepada penerima informasi untuk keperluan dan periode waktu yang spesifik, dimana pihak penerima informasi wajib menjaga kerahasiaan informasi serta mengupayakan pencegahan terjadinya kebocoran atau penyebaran informasi secara tidak sah;
    b. hak dari pemilik aset informasi untuk melakukan audit dan pemantauan aktivitas penerima informasi berkaitan dengan penggunaan informasi sensitif; dan
    c. konsekuensi yang harus ditanggung penerima informasi apabila terjadi pelanggaran atas perjanjian kerahasiaan.

BAB XII

AKUISISI, PENGEMBANGAN DAN PEMELIHARAAN SISTEM

A. Tujuan

Tujuan dari kebijakan akuisisi, pengembangan, dan pemeliharaan sistem adalah untuk:

1. Memastikan keamanan informasi sebagai bagian tak terpisahkan dari siklus hidup (*lifecycle)* sistem informasi. Termasuk persyaratan untuk sistem informasi yang menyediakan layanan melalui jaringan publik
2. Memastikan keamanan informasi didesain dan diimplementasikan dalam siklus hidup (*lifecycle*) pengembangan dari sistem informasi.
3. Memastikan perlindungan terhadap penggunaan data untuk pengujian.

B. Ruang Lingkup

Ruang lingkup dari kebijakan keamanan komunikasi adalah untuk:

1. Persyaratan keamanan sistem informasi;
2. Keamanan dalam proses pengembangan dan *support;*
3. Data pengujian.

C. Kebijakan

1. Perangkat Daerah harus menetapkan dan mendokumentasikan secara jelas persyaratan keamanan informasi yang relevan sebelum pengembangan, perluasan, atau pengadaan sistem informasi baru.
2. Persyaratan keamanan harus diidentifikasi secara jelas di dalam dokumen persyaratan dan spesifikasi perangkat lunak (*software).*
3. Spesifikasi ini harus disetujui oleh pemilik informasi, pemilik proses bisnis dan pengembang sistem, sebelum fase pengkodean (*coding*) dalam pengembangan sistem.
4. Informasi yang digunakan oleh aplikasi Perangkat Daerah yang ditransimisikan melalui jaringan publik (*internet*) harus diamankan dari aktivitas penipuan, kemungkinan adanya perselisihan kontrak, dan pengungkapan dan/atau perubahan informasi tanpa izin.
5. Pengamanan informasi terhadap informasi yang ditransmisikan melalui sistem informasi yang digunakan dapat mencakup namun tidak terbatas pada:
    a. proses otentikasi dan otorisasi terhadap pengguna aplikasi;
    b. perlindungan untuk memastikan kerahasiaan dan integritas informasi yang dipertukarkan melalui jaringan publik;
    c. perlindungan terhadap *session* transaksi untuk menghindari duplikasi dan/atau modifikasi; dan

d. mengamankan jalur komunikasi antara pihak-pihak yang terlibat

6. Keamanan dalam proses pengembangan dan dukungan yang perlu dipertimbangkan oleh Perangkat Daerah meliputi aturan untuk pengembangan sistem harus ditetapkan dan diimplementasikan untuk proses pengembangan sistem di Perangkat Daerah yang mencakup:
   1) pengamanan dari lingkungan pengembangan, seperti pemisahan lingkungan pengembangan baik secara fisik dan/atau logical, pengendalian akses, pengelolaan perubahan;
   2) panduan *secure coding*;
   3) pengedalian versi aplikasi;
   4) penyimpanan dari *source code*; dan
   5) metode pengujian untuk mengidentifikasi dan memperbaiki *vulnerability*.
7. Perubahan terhadap sistem selama siklus pengembangan sistem harus dikendalikan melalui proses manajemen perubahan yang berlaku di Perangkat Daerah;
8. Apabila platform operasional, misalnya sistem operasi, *database* dan/atau *middleware*, dari sistem informasi Perangkat Daerah mengalami perubahan, aplikasi kritikal Perangkat Daerah harus ditinjau dan diuji untuk memastikan tidak ada dampak buruk terhadap operasional dan keamanan organisasi;
9. Perangkat Daerah harus menetapkan lingkungan pengembangan yang aman untuk pengembangan dan integrasi sistem Perangkat Daerah. Hal ini dapat mencakup namun tidak terbatas pada:
   a. pemisahan lingkungan pengembangan baik secara fisik dan/atau *logical*;
   b. pengendalian akses; dan
   c. perpindahan data dari dan ke lingkungan pengembangan;
10. Perangkat Daerah harus mengawasi aktivitas pengembangan sistem yang dialihdayakan (*outsourced*). Hal ini dapat mencakup:
   a. perjanjian terkait lisensi dan kepemilikan sistem;
   b. pengujian penerimaan sistem untuk menguji kualitas dan akurasi dari sistem;
   c. prasyarat dokumentasi untuk sistem;
   d. perjanjian dengan pihak ketiga sebagai penjamin;
   e. hak untuk melakukan audit proses pengembangan dan kontrol yang diimplementasikan oleh vendor.
11. Pengujian dari fitur keamanan sistem harus dilakukan pada saat pengembangan sistem informasi Perangkat Daerah;

12. Pengujian ini dilakukan berdasarkan prasyarat keamanan sistem yang telah ditetapkan;
13. Kriteria dan jadwal untuk pengujian penerimaan sistem harus ditetapkan untuk sistem informasi baru, *upgrade*, dan versi baru dari sistem informasi Perangkat Daerah;
14. Pengujian penerimaan sistem harus dilakukan sesuai dengan kriteria dan jadwal yang ditetapkan.
15. Pengamanan terhadap data hasil pengujian perlu diperhatikan sebagai berikut:
    a. data untuk pengujian sistem harus dipilih secara hati-hati untuk menghindari pengungkapan atau perubahan informasi sensitif oleh pihak yang tidak berhak, serta melindungi dari kemungkinan kerusakan dan kehilangan informasi;
    b. masking data harus dilakukan apabila data operasional yang sensitif digunakan untuk keperluan pengujian; dan
    c. data operasional yang digunakan untuk keperluan pengujian harus dihapus segera setelah proses pengujian telah selesai dilaksanakan.

BAB XIII

HUBUNGAN KERJA DENGAN PEMASOK (*SUPPLIER*)

A. Tujuan

Tujuan dari kebijakan mengenai hubungan kerja dengan pemasok (*supplier*) adalah untuk memastikan perlindungan atas aset Perangkat Daerah dalam jangkauan akses pemasok dan memelihara tingkat layanan yang dsetujui dari keamanan informasi sesuai dengan perjanjian dengan pemasok.

B. Ruang Lingkup

Ruang lingkup dari kebijakan mengenai hubungan kerja dengan pemasok (*supplier*) adalah para pemasok dalam lingkungan Pemerintah Daerah Kota.

C. Kebijakan

1. Perangkat Daerah harus mempertimbangkan aspek keamanan informasi dalam hubungan dengan pemasok mulai dari pemilihan, penunjukan, monitoring, evaluasi, sampai dengan terminasi.
2. Pemilihan dari penyedia jasa Perangkat Daerah harus mengikuti kriteria berikut:
    a. kompetensi, pengalaman dan catatan dari organisasi;
    b. kepastian dari kemampuan penyedia jasa untuk menyediakan layanan; dan
    c. kepastian dari kemampuan penyedia jasa untuk menjaga ketersediaan dari penyediaan layanan pada saat kondisi normal atau kondisi bencana (apabila terjadi bencana alam atau kegagalan dalam penyediaan layanan);
3. Berdasarkan pengelompokan pemasok yang telah bekerjasama, Perangkat Daerah wajib mendefinisikan pembatasan aset dan aset informasi apa saja yang diperbolehkan untuk diakses oleh setiap kelompok pemasok, serta senantiasa memantau akses yang telah dilakukan.
4. Perangkat Daerah menetapkan persyaratan keamanan informasi bagi setiap pemasok yang mengakses aset informasi, serta senantiasa memantau kepatuhan pemasok terhadap persyaratan tersebut. Pemasok yang menangani aset informasi dengan klasifikasi rahasia perlu menandatangani Perjanjian Kerahasiaan.
5. Kewajiban *supplier* dan tingkat layanan harus ditetapkan secara formal dalam kontrak kerja;
6. Perangkat Daerah harus memastikan pengelolaan *delivery* layanan dari pemasok dengan memperhatikan:

a. layanan yang diserahkan kepada Perangkat Daerah oleh pihak *supplier* harus secara berkala dipantau, dan ditinjau;

b. proses pemantauan dilakukan untuk memverifikasi kesesuaian dari tingkat layanan yang diberian dan prasyarat keamanan informasi dengan perjanjian kerja;

c. proses peninjauan dilakukan untuk mengidentifikasi problem terkait penyediaan layanan dan aspek keamanan informasi dalam penyediaan layanan oleh *supplier*;

d. peninjauan dari penyediaan layanan oleh *supplier* harus dilaksanakan paling sedikit 1 (satu) kali dalam 3 (tiga) bulan;

7. Perangkat Daerah dapat melakukan audit terhadap penyediaan layanan yang diberikan pemasok

8. Ketentuan dalam pelaksanaan audit kepada pemasok sebagai berikut:

   a. tanggung jawab untuk mengaudit tingkat layanan dimiliki oleh pihak, baik internal maupun eksternal, yang memiliki independensi dari pengguna layanan yang diberikan oleh supplier dan ditunjuk secara formal;

   b. audit terhadap penyediaan layanan oleh *supplier* harus dilakukan paling sedikit 1 (satu) kali dalam 1 (satu) tahun; dan

   c. setiap ketidaksesuaian yang ditemukan dalam proses peninjauan dan audit harus dikelola dan ditindaklanjuti;

9. Perubahan terhadap layanan yang diberikan oleh *supplier* harus dikelola, dengan memperhatikan kritikalitas dari proses bisnis pengguna layanan dan layanan yang diberikan oleh *supplier*;

10. Perubahan terhadap layanan yang diberikan oleh *supplier* harus dipastikan tidak akan mengganggu aspek kerahasiaan dari informasi Perangkat Daerah serta integritas dan ketersediaan dari informasi dan layanan Perangkat Daerah.

11. Perubahan terhadap layanan yang diberikan oleh *supplier* harus disetujui oleh manajemen Perangkat Daerah yang relevan dan diformalisasikan dalam kontrak kerja.

BAB XIV

PENANGANAN INSIDEN KEAMANAN INFORMASI

A. Tujuan

Tujuan dari kebijakan penanganan insiden keamanan informasi adalah untuk memastikan adanya pendekatan yang konsisten dan efektif atas penanganan insiden keamanan informasi.

B. Ruang Lingkup

Ruang lingkup Perangkat Daerah dari kebijakan penanganan insiden keamanan informasi adalah:

1. Tanggung jawab dan prosedur;
2. Pelaporan atas kejadian insiden keamanan informasi; dan
3. Pelaporan atas kelemahan keamanan informasi.

C. Kebijakan

1. Kejadian keamanan informasi adalah sebuah kejadian pada sistem, layanan ataupun jaringan yang dapat mengindikasikan adanya pelanggaran keamanan informasi atau kegagalan keamanan atau kejadian yang mungkin memiliki keterkaitan dengan keamanan informasi.
2. Kelemahan keamanan informasi adalah sebuah kelemahan yang teridentifikasi pada sistem, layanan atau jaringan yang dapat dieksploitasi oleh pihak yang tidak bertanggung jawab dan dapat menyebabkan pelanggaran terhadap kebijakan keamanan informasi.
3. Insiden keamanan informasi adalah kejadian keamanan informasi yang tidak diinginkan dan tidak diperkirakan dimana kejadian tersebut menimbulkan gangguan terhadap operasional bisnis dan mengancam keamanan informasi.
4. Guna memastikan proses penanganan insiden yang responsif dan efektif, perlu dikembangkan berbagai prosedur yang mencakup:
    a. perencanaan dan persiapan penanganan insiden;
    b. pemantauan, analisis, dan pelaporan atas insiden;
    c. pencatatan atas aktivitas penanganan insiden;
    d. penanganan bukti forensik;
    e. penilaian dan pengambilan keputusan atas insiden dan kelemahan keamanan informasi; dan
    f. pemulihan insiden.

5. Seluruh pegawai dan pihak ketiga wajib melaporkan berbagai kejadian insiden keamanan informasi maupun yang masih bersifat dugaan atas kelemahan keamanan informasi sesegera mungkin, sesuai prosedur pelaporan insiden yang berlaku.
6. Setiap kejadian insiden keamanan informasi harus dianalisis, diklasifikasikan, dan ditentukan skala prioritas penanganannya. Penanganan insiden beserta pemulihannya dilakukan berdasarkan klasifikasi dan prioritas yang telah ditetapkan.
7. Perangkat Daerah harus mengklasifikasikan insiden keamanan informasi untuk memprioritaskan penanganan insiden. Klasifikasi insiden tersebut adalah sebagai berikut:
    a. insiden keamanan informasi diklasifikasikan berdasarkan dampaknya menjadi berikut:
        1) mayor, apabila insiden tersebut menyebabkan terhentinya proses operasional pekerjaan Perangkat Daerah; dan
        2) minor, apabila insiden tersebut menyebabkan gangguan yang tidak menghentikan proses operasional pekerjaan Perangkat Daerah.
    b. insiden keamanan informasi diklasifikasikan berdasarkan tingkat kepentingannya menjadi berikut:
        1) *emergency*, apabila insiden tersebut dapat atau telah menghentikan proses operasional Perangkat Daerah dan/atau insiden tersebut mempengaruhi secara langsung pimpinan dalam lingkungan Perangkat Daerah; dan
        2) normal, apabila insiden tersebut insiden tersebut tidak menghentikan proses operasional Perangkat Daerah dan/atau insiden tersebut mempengaruhi secara langsung pimpinan dalam lingkungan Perangkat Daerah.
8. Setiap insiden keamanan informasi harus ditangani dengan baik untuk mencegah meluasnya insiden, untuk memulihkan layanan atau informasi yang mungkin hilang dan untuk meminimalisasi dampak dari insiden.
9. Setiap tindakan yang diidentifikasi untuk menangani kejadian, kelemahan dan insiden keamanan informasi harus dikonsultasikan kepada koordinator teknologi informasi dan/atau personil yang kompeten dan relevan dengan kejadian, kelemahan, dan insiden keamanan informasi.
10. Setiap tindakan penanganan kejadian, kelemahan, dan insiden keamanan informasi harus didokumentasikan dengan baik.

BAB XV

KELANGSUNGAN USAHA (*BUSINESS CONTINUITY*)

A. Tujuan

Tujuan dari kebijakan mengenai kelangsungan usaha (*business continuity*) adalah untuk memastikan ketersediaan layanan TIK beserta fasilitas pengolahan informasi dalam kondisi darurat dan memulihkan layanan seperti sediakala dalam kondisi kembali normal.

B. Ruang Lingkup

Ruang lingkup dari kebijakan mengenai kelangsungan usaha (*business continuity*) adalah:

1. keberlanjutan keamanan informasi; dan
2. redundansi fasilitas pengolahan informasi.

C. Kebijakan

1. Perangkat Daerah harus menetapkan, mendokumentasikan, mengimplementasikan dan memelihara proses, prosedur, dan kontrol yang diperlukan untuk menjamin keberlanjutan keamanan informasi sesuai prasyarat yang telah ditetapkan pada saat dan setelah terjadinya gangguan besar atau bencana.
2. Perangkat Daerah harus memverifikasi kontrol keberlanjutan keamanan informasi yang telah ditetapkan dan diimplementasikan secara berkala untuk menjamin kesesuaian dan efektivitasnya pada saat dan setelah terjadinya gangguan besar atau bencana.
3. Perangkat Daerah harus menetapkan prasyarat untuk keberlanjutan keamanan informasi dan diintegrasikan dengan prasyarat keberlanjutan bisnis organisasi untuk menjamin keberlanjutan dari keamanan informasi di Perangkat Daerah, pada saat dan setelah terjadinya gangguan besar atau bencana.
4. Prasyarat keamanan informasi dapat diintegrasikan pada siklus proses *Business Continuity Management (BCM)* yang mencakup:
   a. memahami kebutuhan organisasi;
   b. menentukan strategi *BCM*;
   c. mengembangkan dan mengimplementasikan rencana penanggulangan/keberlanjutan bisnis; dan
   d. pengujian, pemeliharaan, dan peninjauan rencana penanggulangan / keberlanjutan bisnis.
5. Aspek redundansi harus ditetapkan untuk fasilitas pengolahan informasi dan sarana pendukungnya untuk memastikan ketersediaan dari proses bisnis dan operasional Perangkat Daerah serta pemberian layanan Perangkat Daerah kepada pelanggan.

6. Apabila prasyarat redundan tidak dapat dipenuhi, maka proses alternatif perlu ditetapkan untuk menjamin ketersediaan dari proses bisnis dan operasional Perangkat Daerah serta *delivery* dari layanan Perangkat Daerah kepada pelanggan.
7. Fasilitas pengolahan informasi beserta sarana pendukungnya yang telah memenuhi aspek redundansi harus diuji secara berkala untuk menjamin kesesuaian dari fungsinya.
8. Guna menjamin ketersediaan layanan serta keamanan informasi dalam kondisi darurat (misalnya: bencana alam) pada lokasi utama, perlu adanya redundansi terhadap fasilitas pengolahan informasi yang disebut sebagai fasilitas *backup site*.
9. *Backup site* yang dimaksud dapat berupa lokasi kerja pengganti atau *Disaster Recovery Center (DRC)* bagi alternatif area *Data Center*.
10. Ketentuan dalam pengelolaan terkait Backup Site meliputi:
    a. lokasi *backup site* secara geografis memiliki probabilitas kejadian bencana alam yang minimal;
    b. *backup site* ditujukan sebagai media penyimpanan *backup* alternatif, serta sebagai fasilitas pengolahan informasi alternatif;
    c. terpenuhinya pemulihan layanan operasional sepenuhnya pada fasilitas *backup site* sesuai kerangka parameter *Recovery Time Objective (RTO)*;
    d. pengelola *backup site* beserta Pemilik Aset Informasi melakukan uji keberlangsungan secara berkala dibawah koordinasi penanggung jawab kelangsungan bisnis, minimal 1 (satu) kali dalam setahun, untuk menguji kesiapan seluruh pihak dalam hal:
        1) memindahkan operasional ke fasilitas *backup site*; dan
        2) memulihkan operasional aplikasi beserta data sesuai parameter *Recovery Time Objective (RTO)* yang telah ditetapkan.

BAB XVI

KEPATUHAN

A. Tujuan

Tujuan dari kebijakan kepatuhan adalah untuk menghindari pelanggaran kewajiban hukum, undang-undang, peraturan, atau kontrak yang terkait keamanan informasi dan persyaratan keamanan dan untuk memastikan keamanan informasi diimplementasikan dan dioperasikan sesuai dengan prosedur dan kebijakan organisasi.

B. Ruang Lingkup

Ruang lingkup dari kebijakan mengenai kepatuhan:

1. kepatuhan dengan prasyarat hukum dan kontraktual; dan
2. peninjauan keamanan informasi.

C. Kebijakan

1. Pemerintah Daerah Kota berkomitmen untuk menjaga kepatuhan terhadap setiap prasyarat keamanan informasi yang relevan. Prasyarat keamanan informasi yang dimaksud mencakup prasyarat hukum, regulasi, dan kontraktual.
2. Seluruh prasyarat hukum, regulasi dan kontraktual yang terkait dengan keamanan informasi dan berlaku bagi Perangkat Daerah harus diidentifikasikan, didokumentasikan, dan dipelihara.
3. Perangkat Daerah harus mematuhi hak atas kekayaan intelektual yang terkait dengan material yang digunakan oleh Perangkat Daerah seperti:
    a. penggunaan perangkat lunak dan material yang bersifat *proprietary* harus mematuhi undang-undang terkait Hak atas Kekayaan Intelektual (HAKI) yang berlaku;
    b. bukti dari lisensi atau izin resmi harus didapatkan dan disimpan untuk seluruh materi berlisensi/*copyright* yang di-*install*;
    c. lisensi yang bersifat berlangganan/harus diperbaharui dalam jangka waktu tertentu, harus dikelola untuk memastikan penggunaannya secara legal dan berkesinambungan; dan
    d. penggunaan lisensi dari materi berlisensi/*copyright* harus dikendalikan dengan baik.
4. Dokumen-dokumen penting Perangkat Daerah harus dilindungi dari kehilangan, pemalsuan, kerusakan, atau penyalahgunaan sesuai dengan peraturan perundangan, regulasi, dan persyaratan kontrak dan bisnis.
5. Perangkat Daerah harus memastikan privasi dan perlindungan terhadap informasi terkait dengan pribadi (*personally identifiable information*) sesuai dengan prasyarat hukum, perundang-undangan, regulasi, dan kontraktual.
6. Pimpinan Perangkat Daerah harus secara rutin memantau dan meninjau kepatuhan dari personil, proses kerja dan pemrosesan informasi dalam area tanggung jawabnya terhadap kebijakan dan standar keamanan informasi Perangkat Daerah serta prasyarat keamanan informasi yang berlaku.

7. Pada saat terjadi ketidaksesuaian, pimpinan Perangkat Daerah bertanggung jawab untuk menangani ketidaksesuaian yang terjadi sesuai dengan kebijakan terkait penanganan ketidaksesuaian dan peningkatan SMKI.
8. Sistem informasi Perangkat Daerah harus ditinjau untuk menganalisis kepatuhan teknis dengan kebijakan dan standar keamanan yang berlaku serta dengan prasyarat keamanan informasi yang relevan dan berlaku, paling tidak 1 (satu) kali dalam 1 (satu) tahun.
9. Apabila diperlukan, peninjauan tersebut dapat melibatkan personil yang memiliki kualifikasi di bidang keamanan informasi untuk mendapatkan pemahaman yang mendalam mengenai risiko keamanan informasi yang mungkin muncul dari pengecualian tersebut.

WALI KOTA BOGOR,

Ttd.

BIMA ARYA