



PROVINSI JAWA TENGAH
PERATURAN WALIKOTA SEMARANG
NOMOR 28 TAHUN 2021
TENTANG
SISTEM MANAJEMEN KEAMANAN INFORMASI (SMKI)
PEMERINTAHAN BERBASIS ELEKTRONIK DI LINGKUNGAN
PEMERINTAH KOTA SEMARANG
DENGAN RAHMAT TUHAN YANG MAHA ESA
WALIKOTA SEMARANG,

- Menimbang : a. bahwa untuk melindungi kerahasiaan, keutuhan dan ketersediaan aset data dan informasi pemerintahan berbasis elektronik di lingkungan Pemerintah Kota Semarang dari berbagai ancaman keamanan informasi dan penyalahgunaan akses, maka perlu melakukan pengelolaan keamanan informasi;
- b. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, perlu menetapkan Peraturan Walikota tentang Sistem Manajemen Keamanan Informasi Pemerintahan Berbasis Elektronik di Lingkungan Pemerintah Kota Semarang;
- Mengingat : 1. Pasal 18 ayat (6) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;
2. Undang-Undang Nomor 16 Tahun 1950 tentang Pembentukan Daerah-Daerah Kota Besar Dalam Lingkungan Propinsi Jawa Timur, Jawa Tengah, Jawa Barat dan Daerah Istimewa Semarang ;
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);
4. Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 61, Tambahan Lembaran Negara Republik Indonesia Nomor 4846);

5. Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 244, Tambahan Lembaran Negara Republik Indonesia Nomor 5587) sebagaimana telah diubah beberapa kali 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);
6. Peraturan Pemerintah Nomor 16 Tahun 1976 tentang Perluasan Kotamadya Daerah Tingkat II Semarang (Lembaran Negara Republik Indonesia Tahun 1976 Nomor 25, Tambahan Lembaran Negara Republik Indonesia Nomor 3079);
7. Peraturan Pemerintah Nomor 50 Tahun 1992 tentang Pembentukan Kecamatan di Wilayah Kabupaten-kabupaten Daerah Tingkat II Purbalingga, Cilacap, Wonogiri, Jepara, dan Kendal serta Penataan Kecamatan di Wilayah Kotamadya Daerah Tingkat II Semarang dalam Wilayah Propinsi Daerah Tingkat I Jawa Tengah (Lembaran Negara Republik Indonesia Tahun 1992 Nomor 89);
8. Peraturan Presiden No. 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
9. Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi (Berita Negara Republik Indonesia Tahun 2016 Nomor 551);
10. Peraturan BSSN No.4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2021 Nomor 541);
11. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 59 Tahun 2020 tentang Pemantauan dan Evaluasi Sistem Pemerintahan Berbasis Elektronik (Berita Negara Tahun 2020 Nomor 994);
12. Peraturan Gubernur No. 10 Tahun 2018 tentang Penyelenggaraan Persandian untuk Pengamanan Informasi di Lingkungan Pemerintah Provinsi Jawa Tengah (Berita Daerah Provinsi Jawa Tengah Tahun 2018 Nomor 10);
13. Peraturan Walikota Semarang No.27 Tahun 2021 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik di lingkungan Pemerintah Kota

Semarang (Berita Daerah Kota Semarang Tahun 2021 Nomor 21);

MEMUTUSKAN:

Menetapkan : PERATURAN WALIKOTA TENTANG SISTEM MANAJEMEN KEAMANAN INFORMASI PEMERINTAHAN BERBASIS ELEKTRONIK DI LINGKUNGAN PEMERINTAH KOTA SEMARANG.

BAB I

KETENTUAN UMUM

Pasal 1

Dalam Peraturan Walikota ini yang dimaksud dengan:

1. Daerah adalah Kota Semarang.
2. Pemerintah Daerah adalah Walikota sebagai unsur penyelenggara Pemerintahan Daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan daerah otonom.
3. Walikota adalah Walikota Semarang.
4. Sekretaris Daerah adalah Sekretaris Daerah Kota Semarang.
5. Sistem adalah suatu kesatuan yang terdiri elemen yang dihubungkan bersama untuk memudahkan aliran data, informasi, atau materi untuk mencapai suatu tujuan.
6. Perangkat daerah adalah unsur pembantu kepala Daerah dan Dewan Perwakilan Rakyat Daerah dalam penyelenggaraan Urusan Pemerintahan yang menjadi kewenangan Daerah.
7. Data adalah catatan atas kumpulan fakta yang belum diolah dan apa adanya.
8. Informasi adalah keterangan, pernyataan, gagasan dan tanda-tanda yang mengandung data, fakta, pesan, yang memiliki nilai dan makna dimana penjelasannya dapat dilihat, didengar dan dibaca yang disajikan dalam berbagai format sesuai dengan perkembangan teknologi informasi dan komunikasi secara elektronik maupun nonelektronik.
9. Teknologi Informasi dan Komunikasi yang selanjutnya disingkat TIK adalah segala kegiatan yang terkait dengan pemrosesan, manipulasi, pengelolaan, dan pemindahan informasi antar media.
10. Sistem Pemerintahan Berbasis Elektronik (SPBE) adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk meningkatkan efisiensi, efektifitas, transparansi dan akuntabilitas layanan pemerintahan.
11. Keamanan informasi adalah terjaganya kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*) informasi.
12. 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.
13. Risiko adalah peluang terjadinya suatu peristiwa yang akan mempengaruhi keberhasilan terhadap pencapaian tujuan.
14. Manajemen Risiko adalah pendekatan sistematis yang meliputi proses, pengukuran, struktur, dan budaya untuk menentukan tindakan terbaik

terkait risiko.

15. Tim Tanggap Insiden Keamanan Siber (*CSIRT - Computer Security Incident Response Team*) adalah tim yang bertanggung jawab untuk menerima, meninjau dan menanggapi laporan dan aktifitas insiden keamanan teknologi informasi.
16. Aset Informasi adalah unit informasi yang dapat dipahami, dibagi, dilindungi dan dimanfaatkan secara efektif.
17. Aset Pengolahan Informasi adalah suatu perangkat baik elektronik maupun non-elektronik yang dapat digunakan untuk membuat dan menyunting informasi.
18. Penyimpanan Informasi adalah suatu proses menyimpan informasi dengan menggunakan media baik elektronik maupun non-elektronik.
19. *Data Center* adalah suatu fasilitas fisik (*on-premise*) untuk menempatkan sistem komputer dan perangkat-perangkat terkait, seperti sistem komunikasi data dan penyimpanan data.
20. *Cloud* atau dikenal *Cloud Computing* (komputasi awan) adalah sistem komputasi *off-premise* (non-fisik) yang berfungsi sebagai penyimpanan, pengelolaan, pemrosesan data pada server melalui internet sebagai medianya.

BAB II

MAKSUD, TUJUAN DAN RUANG LINGKUP

Pasal 2

- (1) Peraturan Walikota ini dimaksudkan untuk memberikan pedoman bagi Pemerintah Kota Semarang dalam melaksanakan kebijakan, program dan kegiatan sistem manajemen keamanan informasi untuk pengamanan informasi sistem pemerintahan berbasis elektronik sesuai dengan Peraturan Walikota No. 27 tahun 2021 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik di lingkungan Pemerintah Kota Semarang.
- (2) Kebijakan sebagaimana dimaksud pada ayat (1) tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Peraturan Walikota ini.

Pasal 2

- (1) Tujuan ditetapkannya Peraturan Walikota ini adalah 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.

Pasal 3

Ruang lingkup pengamanan informasi yang diatur dalam Peraturan Walikota ini meliputi:

- a. Aset Informasi;
- b. Aset Pengolahan Informasi;
- c. Penyimpanan Informasi

Pasal 4

Aset Informasi sebagaimana dimaksud dalam Pasal 3 huruf a meliputi informasi yang tercetak, tertulis, dan tersimpan dalam bentuk:

a. fisik, seperti:

1. kertas;
2. papan tulis;
3. spanduk; dan
4. buku atau dokumen.

b. elektronik, seperti:

1. database dan file di dalam komputer;
2. informasi yang ditampilkan pada website, layar komputer; dan
3. informasi yang dikirimkan melalui sensor pemindai dan peranti lain melalui jaringan telekomunikasi.

Pasal 5

Aset Pengolahan Informasi sebagaimana dimaksud dalam Pasal 3 huruf b berupa:

- a. peralatan mekanik yang digerakkan dengan tangan secara manual; dan
- b. peralatan elektronik digital yang bekerja secara penuh.

Pasal 6

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

a. elektronik, meliputi antara lain:

a.1. data *storage*

1. *server*
2. *hard disk*,
3. *flash disk*,
4. kartu memori, memori internal telepon seluler dan lain-lain.

a.2 Penyimpanan *cloud*

b. non-elektronik, meliputi antara lain:

1. lemari,
2. rak,
3. laci,
4. filling cabinet, dan lain-lain.

BAB III
TANGGUNG JAWAB
Pasal 7

Semua Perangkat Daerah terkait, memiliki tanggung jawab dalam pengamanan sistem informasi melalui koordinasi dengan perangkat daerah yang menyelenggarakan tugas dan fungsi di bidang teknologi informasi dan komunikasi.

Pasal 8

- (1) Untuk mendukung tugas pengamanan informasi sebagaimana dimaksud dalam Pasal 7, setiap Perangkat Daerah dapat membentuk Tim Tanggap Insiden Keamanan Siber (*CSIRT*) yang beranggotakan seluruh pengelola teknologi informasi dan komunikasi.
- (2) Tim Tanggap Insiden Keamanan Siber (*CSIRT*) sebagaimana dimaksud diketuai oleh kepala perangkat daerah dan beranggotakan pejabat struktural dan fungsional atau petugas yang menyelenggarakan fungsi Teknologi Informasi.
- (3) Tim Tanggap Insiden Keamanan Siber (*CSIRT*) sebagaimana dimaksud bertanggungjawab memastikan Teknologi Informasi yang digunakan mendukung proses tata kelola keamanan informasi pada sistem pemerintahan berbasis elektronik dalam pencapaian tujuan organisasi.
- (4) Tim Tanggap Insiden Keamanan Siber (*CSIRT*) memiliki wewenang:
 - a. menyusun prosedur penyelenggaraan Keamanan Informasi yang diterapkan secara efektif baik bagi Perangkat Daerah maupun pengguna;
 - b. melakukan evaluasi internal kinerja penyelenggaraan Teknologi Informasi.

Pasal 9

- (1) Dalam rangka efektifitas penerapan manajemen keamanan informasi, setiap perangkat daerah perlu untuk melakukan proses manajemen risiko.
- (2) Proses manajemen risiko sebagaimana dimaksud pada ayat (1) meliputi:
 - a. identifikasi;
 - b. analisa;
 - c. pemantauan; dan
 - d. pengendalian risiko penggunaan teknologi.
- (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 ketiga sebagai penyedia jasa teknologi informasi.

- (4) Penerapan manajemen risiko harus dilakukan secara terintegrasi pada setiap penggunaan operasional Teknologi Informasi terkait sistem yang digunakan.

Pasal 10

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

Pasal 11

- (1) Setiap Perangkat Daerah menyusun standar dan prosedur pengendalian kegiatan teknologi informasi yang memenuhi prasyarat keamanan informasi dengan mengimplementasikan tindakan pengelolaan potensi risiko keamanan.
- (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. penerapan persandian dengan enkripsi dan kriptografi pada informasi;
 - f. penerapan tanda tangan elektronik,
 - g. keamanan fisik dan lingkungan;
 - h. keamanan operasional;
 - i. keamanan komunikasi;
 - j. keamanan dalam proses akuisisi, pengembangan dan pemeliharaan sistem informasi;
 - k. hubungan kerja dengan para stakeholder terkait dan penyedia jasa;
 - l. penanganan insiden keamanan informasi;
 - m. kelangsungan usaha; dan
 - n. kepatuhan.

Pasal 12

- (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, efisiensi, dan keamanan dari aktivitas tersebut antara lain dengan:
- a. menerapkan keamanan fisik 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 sarana dan prasarana layanan jaringan komunikasi baik yang dikelola secara internal maupun oleh pihak lain penyedia jasa;
- e. melakukan pemantauan aktifitas pengguna dalam mengakses sistem informasi;
- f. melakukan pemantauan terhadap aplikasi yang digunakan oleh Perangkat Daerah maupun pengguna.

Pasal 13

- (1) Setiap Perangkat Daerah penyelenggara teknologi informasi harus memastikan ketersediaan data dan sistem dalam rangka menjaga kelangsungan teknologi informasi melalui penyelenggaraan fasilitas Data Center dan *Cloud* baik dikelola oleh internal maupun oleh pihak penyedia jasa lainnya.
- (2) Setiap aktivitas pada fasilitas di Data Center dan *Cloud* harus dapat terpantau guna menghindari kesalahan proses pada sistem dan mencegah hilang dan bocornya data serta memperhatikan aspek perlindungan terhadap data yang diproses dan lingkungan fisik.

Pasal 14

- (1) Perangkat Daerah menerapkan prinsip pengendalian internal terhadap aktivitas Teknologi Informasi secara berkala.
- (2) Perangkat Daerah Penyelenggara Teknologi Informasi melakukan perbaikan berdasarkan hasil umpan balik, maupun evaluasi terhadap keamanan informasi yang dilakukan, dalam rangka meningkatkan efektivitas sistem manajemen keamanan informasi.
- (3) Hasil dari tindakan perbaikan dan peningkatan sebagaimana dimaksud pada ayat (2) dilaporkan kepada Tim Koordinasi SPBE dan didokumentasikan sebagai bagian dari proses pembelajaran bagi Perangkat Daerah.

Pasal 15

- (1) Apabila terdapat indikasi kebocoran dan hilangnya data dan informasi pada perangkat daerah terkait yang berdampak sangat luas, maka Pemerintah Kota Semarang 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.

Pasal 16

Peraturan Walikota ini mulai berlaku pada tanggal diundangkan.

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

Ditetapkan di Semarang
pada tanggal 14 Juni 2021

WALIKOTA SEMARANG

ttd

HENDRAR PRIHADI

Diundangkan di Semarang
pada tanggal 14 Juni 2021


SEKRETARIS DAERAH KOTA SEMARANG

ttd

ISWAR AMINUDDIN

BERITA DAERAH KOTA SEMARANG TAHUN 2021 NOMOR 28

Salinan sesuai dengan aslinya
KEPALA BAGIAN HUKUM
PADA SEKRETARIAT DAERAH KOTA SEMARANG



Drs. Satrio Imam Poetranto, M.Si
Pembina Tingkat I
NIP.196503111986021004

LAMPIRAN PERATURAN WALIKOTA SEMARANG
NOMOR 28 TAHUN 2021
TENTANG
SISTEM MANAJEMEN KEAMANAN INFORMASI
(SMKI) PEMERINTAHAN BERBASIS ELEKTRONIK DI
LINGKUNGAN PEMERINTAH KOTA SEMARANG

KEBIJAKAN UMUM SISTEM MANAJEMEN KEAMANAN INFORMASI
PEMERINTAH KOTA SEMARANG
RINGKASAN

A. PENDAHULUAN

Kebijakan umum keamanan informasi memuat kebijakan keamanan informasi yang akan menjadi acuan dalam kebijakan spesifik, pedoman, prosedur, risk assessment maupun proses keamanan informasi lainnya. Kebijakan spesifik akan digunakan oleh bagian teknis dalam menyelesaikan tanggung jawab keamanan informasi. Pedoman dan prosedur digunakan untuk mengimplementasikan kebijakan yang telah ditetapkan dan sifatnya anjuran. Hal tersebut berbeda dengan kebijakan yang sifatnya keharusan.

Kebijakan umum keamanan informasi memiliki kesamaan tingkat dengan kebijakan di Pemerintah Kota Semarang yang lainnya dan dipatuhi oleh semua pengguna.

B. KEBIJAKAN SISTEM MANAJEMEN KEAMANAN INFORMASI

1. RUANG LINGKUP KEAMANAN INFORMASI

Ruang lingkup keamanan informasi meliputi:

- a. Keamanan informasi seperti keamanan database, kontrak, dokumentasi sistem, manual pengguna, prosedur pendukung, business continuity plan.
- b. Keamanan aset perangkat lunak seperti keamanan perangkat lunak aplikasi, perangkat lunak sistem, perkakas pengembangan, dan utilitas;
- c. Keamanan aset fisik meliputi keamanan perangkat komputer, perangkat jaringan;
- d. Keamanan layanan meliputi keamanan layanan komputasi dan komunikasi, utilitas umum (listrik, pemanas, *air-conditioning*).
- e. Keamanan sumber daya manusia beserta kualifikasi, keterampilan dan pengalaman;
- f. Keamanan aset yang tidak berwujud seperti reputasi, citra organisasi.

Keamanan informasi merupakan tanggung jawab dari semua pihak yang terkait pada Pemerintah Kota Semarang meliputi seluruh pemangku kepentingan (*stakeholder*) internal dan eksternal di lingkungan Kota Semarang.

2. URGENSI KEAMANAN INFORMASI PEMERINTAH KOTA SEMARANG

Keamanan informasi menjadi hal yang penting bagi Pemerintah Kota Semarang karena:

- a. Memberikan jaminan informasi bagi *stakeholder* utama Pemerintah Kota Semarang;
- b. Meningkatkan jaminan atas aset informasi terhadap risiko keamanan melalui proteksi yang memadai dan berkelanjutan. Risiko tersebut memiliki dampak langsung maupun tidak langsung bagi negara.
- c. Meningkatkan kepatuhan terhadap undang-undang dan peraturan terkait keamanan informasi yang ada di Indonesia maupun internasional;
- d. Meningkatkan kepercayaan publik, *stakeholder* terhadap Pemerintah Kota Semarang;
- e. Meningkatkan respon terhadap pelanggaran atau insiden keamanan informasi.

2.1. Tujuan keamanan informasi

Tujuan keamanan informasi Pemerintah Kota Semarang sebagai berikut

- a. Memastikan kerahasiaan terhadap aset informasi Pemerintah Kota Semarang;
- b. Memastikan ketersediaan dan keutuhan informasi bagi *stakeholder*;
- c. Memastikan kapabilitas organisasi untuk melanjutkan layanan ketika terjadi insiden keamanan;
- d. Memastikan kepatuhan terhadap hukum, undang-undang dan peraturan yang berlaku.

2.2 Prinsip keamanan informasi

Prinsip keamanan informasi Pemerintah Kota Semarang sebagai berikut

a. Prinsip Kerahasiaan

Kemampuan akses dan modifikasi informasi diberikan hanya kepada pihak yang berwenang untuk tujuan yang jelas.

b. Prinsip Keutuhan Integritas

Informasi yang digunakan pengguna bisa dipercaya kebenarannya merefleksikan realitas sebenarnya, terutama informasi strategis.

c. Prinsip Ketersediaan

Informasi tersedia untuk mendukung organisasi dalam rentang waktu yang disepakati bersama dan sesuai dengan peraturan yang ada sesuai tujuan organisasi

d. Prinsip Akuntabilitas

Tanggung jawab pemilik, penyedia dan pengguna sistem informasi dan pihak lain yang terkait dengan keamanan informasi harus dideskripsikan dengan jelas

e. Prinsip Integrasi

Kebijakan, pedoman, prosedur, ukuran dan praktek untuk keamanan informasi harus dikoordinasikan dan diintegrasikan antara satu dengan yang lain.

f. Prinsip Kesadaran

Pemilik, penyedia, pengguna sistem informasi dan pihak lain yang terkait memiliki pemahaman dan informasi yang cukup mengenai kebijakan, pedoman, prosedur, ukuran, praktek keamanan informasi.

g. Prinsip Berkelanjutan

Keamanan informasi harus diperbaiki terus menerus sesuai dengan perkembangan kebutuhan organisasi dan risiko.

2.3 Pemantauan, Pengukuran, Analisis dan Evaluasi Keamanan Informasi

Sekretaris Daerah mengevaluasi kinerja keamanan informasi dan efektifitas Keamanan Informasi. Serta harus menentukan :

- a. Apa yang perlu dipantau dan diukur, termasuk proses dan pengendalian keamanan informasi;
- b. Metode untuk pemantauan, pengukuran, analisis dan evaluasi, jika diterapkan, untuk memastikan hasil yang valid;
- c. Kapan pemantauan dan pengukuran harus dilakukan;
- d. Siapa yang memantau dan mengukur;
- e. Kapan hasil dari pemantauan dan pengukuran harus dianalisis dan dievaluasi, dan
- f. Siapa yang harus menganalisis dan mengevaluasi hasil tersebut.

Sekretaris Daerah menyimpan informasi terdokumentasi yang memadai sebagai bukti hasil pemantauan dan pengukuran.

2.4 Audit Internal

Inspektorat atau pejabat yang berwenang/berkompeten di bidang audit internal keamanan informasi untuk memberikan informasi apakah Keamanan Informasi diimplementasikan secara efektif serta sesuai dengan:

- a. Persyaratan yang ditetapkan Walikota Semarang untuk Keamanan Informasi, dan
- b. Persyaratan Standar ISO 27001 atau SNI;

2.5 Peninjauan Manajemen

Walikota Semarang melakukan evaluasi SMKI untuk memastikan kesesuaian, kecukupan dan efektifitas. Peninjauan manajemen harus mencakup pertimbangan:

- a. Status tindakan dari reviu manajemen sebelumnya;
- b. Perubahan isu eksternal dan internal yang relevan dengan Keamanan Informasi;
- c. Umpan balik dari kinerja keamanan informasi, termasuk kecenderungan dalam hal:
 - 1) Ketidaksesuaian dan tindakan korektif;
 - 2) Hasil pemantauan dan pengukuran;
 - 3) Hasil audit;
 - 4) Pemenuhan terhadap sasaran keamanan informasi;
 - 5) Umpan balik dari pihak yang berkepentingan;
 - 6) Hasil penilaian risiko dan status rencana penanganan risiko; dan
 - 7) Peluang untuk perbaikan berkelanjutan.

Keluaran dari peninjauan manajemen mencakup keputusan yang berkaitan dengan peluang perbaikan berkelanjutan dan setiap kebutuhan untuk perubahan SMKI.

2.6 Perbaikan Ketidaksesuaian dan Tindakan Korektif

Jika terjadi ketidaksesuaian, Sekretaris Daerah:

- a. Bereaksi terhadap ketidaksesuaian, dan jika dapat diterapkan untuk mengambil tindakan untuk mengendalikan dan mengoreksinya dan menangani konsekuensinya;
- b. Mengevaluasi kebutuhan tindakan untuk menghilangkan penyebab ketidaksesuaian, agar hal itu tidak terulang atau terjadi di tempat lain, dengan cara:
 - 1) Meninjau ketidaksesuaian;
 - 2) Menentukan penyebab ketidaksesuaian; dan
 - 3) Menentukan apakah ada ketidaksesuaian serupa, atau berpotensi terjadi kembali;

Tindakan korektif harus sesuai dengan efek dari ketidaksesuaian yang ditemui.

Perangkat Daerah harus menyimpan informasi terdokumentasi sebagai bukti dari:

- a. Sifat ketidaksesuaian dan tindakan berikutnya yang diambil, dan
- b. Hasil dari setiap tindakan korektif.

3. Kebijakan Keamanan Informasi

3.1 Dokumen Kebijakan Keamanan Informasi

Dokumen kebijakan keamanan informasi harus mendapatkan persetujuan dari Walikota Semarang. Dokumen tersebut dipublikasikan ke seluruh pegawai dan pihak yang terkait. Dokumen kebijakan keamanan informasi tersebut termasuk prinsip, kebijakan, prosedur dan standar teknis keamanan.

3.2 Review Kebijakan Keamanan Informasi

Kebijakan keamanan informasi harus direview secara berkelanjutan dan sistematis. Review tersebut akan digunakan untuk perbaikan kebijakan keamanan informasi, oleh pejabat dan pengelola keamanan informasi terkait, dan selanjutnya harus mendapatkan dukungan dari pejabat tertinggi Pemerintah Kota Semarang.

4. Tanggung jawab keamanan Informasi

Tanggung jawab keamanan informasi melibatkan organisasi dan masing-masing personil dalam organisasi tersebut. Bagian ini terbagi menjadi kewenangan penanggung jawab keamanan informasi, tanggung jawab pejabat eselon II, tanggung jawab pelaksana keamanan informasi dan CSIRT, dan proses review independen.

5. Manajemen Risiko Keamanan Informasi

5.1 Ruang Lingkup dan Tujuan

Ruang lingkup manajemen risiko meliputi identifikasi risiko, analisa dan evaluasi risiko, identifikasi dan evaluasi alternatif penanganan risiko, persetujuan pimpinan atas manajemen risiko serta pernyataan pelaksanaan manajemen risiko. Tujuan manajemen risiko yaitu:

- a. Mendukung tata kelola keamanan informasi;
- b. Kepatuhan terhadap ISO 27001;
- c. Persiapan business continuity plan;
- d. Persiapan incident response plan;
- e. Penyusunan persyaratan keamanan informasi.

5.2 Kebijakan Manajemen Risiko Keamanan Informasi

Manajemen risiko terdiri dari beberapa tahapan yaitu pembentukan konteks, identifikasi risiko, analisa & evaluasi risiko, identifikasi & evaluasi alternatif penanganan risiko, persetujuan pimpinan dan pernyataan penerapan manajemen keamanan informasi.

Berikut kebijakan pada masing-masing tahapan tersebut.

a. Pembentukan Konteks;

- 1) Menentukan lingkup dan batasan manajemen risiko sesuai dengan operasi, struktur, lokasi, aset, dan teknologi yang ada di Pemerintah Kota Semarang.
- 2) Merupakan kriteria yang akan digunakan untuk mengevaluasi risiko keamanan informasi di Pemerintah Kota Semarang.

b. Identifikasi Risiko;

- 1) Identifikasi aset informasi sesuai dengan lingkup manajemen risiko dan pemilik dari aset tersebut;
- 2) Identifikasi ancaman atas aset informasi tersebut;
- 3) Identifikasi kerentanan sebagai hasil ancaman tersebut;
- 4) Identifikasi dampak dari hilangnya kerahasiaan, integritas dan ketersediaan serta independensi yang mungkin terjadi atas aset informasi tersebut.

c. Analisis dan Evaluasi Risiko;

- 1) Perkiraan dampak yang diterima oleh Pemerintah Kota Semarang jika terjadi suatu kegagalan keamanan informasi, termasuk juga konsekuensi atas hilangnya kerahasiaan, integritas dan ketersediaan informasi;
- 2) Perkiraan kemungkinan munculnya kegagalan keamanan akibat adanya ancaman, kerentanan, dan dampak yang berkaitan dengan aset informasi tersebut dan pengendalian yang dilakukan saat ini;
- 3) Perkirakan tingkatan untuk setiap risiko;
- 4) Tentukan apakah risiko dapat diterima atau memerlukan tindakan lebih lanjut menggunakan kriteria risiko yang wajar yang telah ditetapkan;

a. Identifikasi dan Evaluasi Alternatif Penanganan Risiko;

- 1) Melakukan pengendalian yang memadai atas risiko tersebut;
- 2) Menerima risiko tersebut sesuai dengan kebijakan Pemerintah Kota Semarang;
- 3) Menghindari risiko tersebut;
- 4) Memilih tujuan dan rancangan pengendalian sebagai bentuk penanganan risiko, yang didasarkan kepada standar SNI ISO/IEC 27001:2009, ISO/IEC 27005:2008, PP60/2008 dan standar lain.

b. Persetujuan Pimpinan;

- 1) Persetujuan dari Pimpinan Pemerintah Kota Semarang atas hasil analisa risiko keamanan informasi dan risk treatment plan;
- 2) Otorisasi Pimpinan Pemerintah Kota Semarang untuk menerapkan dan

melaksanakan manajemen risiko keamanan informasi.

c. Pernyataan Penerapan Manajemen Keamanan Informasi setidaknya terdiri dari:

- 1) Tujuan pengendalian dan rancangan pengendalian yang dipilih serta alasan pemilihan pengendalian tersebut;
- 2) Tujuan pengendalian dan rancangan pengendalian yang dilaksanakan saat ini;
- 3) Pengecualian untuk setiap tujuan pengendalian dan rancangan pengendalian dari standar yang akan disertifikasi serta alasan pengecualiannya.

6. Klasifikasi Informasi

6.1 Ruang Lingkup dan Tujuan

Ruang lingkup informasi yang dimaksud yaitu keseluruhan informasi yang dimiliki oleh Pemerintah Kota Semarang.

Tujuan klasifikasi informasi yaitu untuk memastikan informasi yang dimiliki Pemerintah Kota Semarang mendapatkan tingkat pengamanan yang sesuai dengan bentuk informasi dan kelompok informasinya.

6.2 Bentuk Informasi

Informasi dibagi dalam dua bentuk yaitu:

- a. Bentuk Non-Elektronik: Kode klasifikasi diberikan pada Lembar Disposisi atau Lembar Kendali Dokumen atau di dokumen itu sendiri pada posisi sisi kanan atas;
- b. Bentuk Elektronik: Kode klasifikasi diberikan pada bagian awal dari Nama file atau pada bagian tertentu dari properties file tersebut. Untuk email dapat kode klasifikasi diberikan pada subjek email.

Dua bentuk informasi tersebut diklasifikasikan berdasarkan tiga kriteria keamanan yaitu kerahasiaan, integritas dan ketersediaan.

6.3. Kelompok Informasi

Dalam proses pengklasifikasian informasi dibagi menjadi dua kelompok, yaitu:

1. Informasi yang bersifat publik;
 - a. Informasi yang bersifat terbuka
 - b. Informasi yang wajib diumumkan secara serta merta
 - c. Informasi yang wajib tersedia setiap saat

Segala Informasi yang menjadi kewenangan Perangkat Daerah dan tidak termasuk dalam informasi yang dikecualikan dalam Undang-undang dan Peraturan perundangan lain yang berlaku.

2. Informasi yang dikecualikan;

Informasi dikecualikan sebagaimana diatur dalam Undang-undang dan Peraturan perundangan lain yang berlaku.

7. Pengelolaan Hak Akses

7.1 Ruang Lingkup dan Tujuan

Ruang lingkup pengelolaan hak akses yaitu akses fisik maupun logik terhadap informasi elektronik maupun non-elektronik oleh pihak internal maupun eksternal.

Tujuan pengelolaan hak akses yaitu untuk mengendalikan akses terhadap informasi yang dimiliki Pemerintah Kota Semarang sehingga informasi hanya bisa diakses oleh pihak yang berwenang saja. Pengelolaan hak akses meliputi pemberian hak akses, pemberian hak akses kepada pihak eksternal, pengendalian akses jaringan dan sistem operasi.

7.2 Kebijakan Pengelolaan Hak Akses

Pengelolaan hak akses dibagi tiga yaitu pemberian hak akses, pemberian hak akses kepada pihak eksternal, pengendalian akses jaringan dan sistem operasi. Berikut kebijakan pada masing-masing bagian tersebut.

a. Pengelolaan Hak Akses

Pengelolaan hak akses dibagi tiga yaitu pemberian hak akses, pemberian hak akses kepada pihak eksternal, pengendalian akses jaringan dan sistem operasi. Berikut kebijakan pada masing-masing bagian tersebut.

b. Pemberian Hak Akses

1) Pemberian hak akses atas informasi dilakukan dengan tata cara umum sebagai berikut:

- a) Pihak-pihak yang membutuhkan akses terhadap suatu informasi mengajukan permohonan hak akses kepada pemilik informasi secara tertulis;
- b) Pemilik informasi harus memastikan bahwa pihak-pihak pengguna yang membutuhkan akses terhadap informasi telah menandatangani perjanjian kerahasiaan sesuai dengan ketentuan yang ada;
- c) Untuk informasi yang berbentuk non-elektronis, persetujuan diberikan oleh pemilik informasi untuk disampaikan kepada pengguna sebagai pemberitahuan;
- d) Untuk informasi yang berbentuk non-elektronis, persetujuan diberikan oleh pemilik informasi untuk disampaikan kepada pengguna sebagai

pemberitahuan serta di tindaklanjuti pemberian hak akses kepada pengguna terhadap informasi yang diminta secara elektronik.

- 2) Pengelola informasi menindaklanjuti pemberian hak akses informasi dengan ketentuan sebagai berikut;
 - a) Memberikan atau membuka akses apabila seluruh pedoman sudah dipenuhi, serta berhak untuk membatasi hak akses dari setiap pengguna sesuai dengan kebutuhan yang telah ditentukan dan sesuai dengan perizinan yang diberikan oleh pemilik informasi;
 - b) Menjaga catatan pengelolaan hak akses serta memastikan bahwa pihakpihak yang memiliki hak akses istimewa telah dikendalikan dengan memadai;
 - c) Melakukan verifikasi pemberian password baru, password pengganti, dan password sementara, memastikan bahwa pengguna hak akses telah menerima password yang diberikan, dan password dari vendor selama proses pemasangan sistem dan/atau piranti lunak harus segera diganti;
 - d) Melakukan peninjauan secara periodik terhadap hak akses informasi, termasuk pemeriksaan tingkatan akses yang diberikan dan penghapusan atau pemblokiran terhadap kelebihan penerbitan hak akses, dan harus segera merubah atau memblokir hak akses apabila pengguna pindah jabatan ataupun pindah kerja/keluar dari Pemerintah Kota Semarang.
- 3) Setelah hak akses diberikan, setiap pemilik hak akses informasi elektronik (User ID dan Password) diharuskan:
 - a) Mengganti password segera setelah menerima hak atas akses informasi dengan segera mengubah password sementara ketika pertama log-on;
 - b) Menjaga kerahasiaan password dengan tidak menuliskan password pada kertas, komputer, dan/atau media lain yang tidak dilindungi dan mudah dibaca oleh pihak yang tidak berkepentingan;
 - c) Mengubah password dengan segera apabila terdapat indikasi mencurigakan atau masalah pada sistem;
 - d) Menggunakan password dengan kriteria: mudah dihafal, tidak mudah ditebak orang lain, gunakan kombinasi angka, huruf kecil, tanda baca dan huruf besar;
 - e) Mengganti password secara berkala, untuk password akun tertentu (akun khusus atau akun yang kritis) harus lebih sering diganti, dan

tidak menggunakan kembali password yang pernah digunakan;

f) Menggunakan password dinas yang berbeda dengan password untuk kebutuhan pribadi (contohnya membedakan email (surel) pribadi dengan surel kantor).

c. Pemberian Hak Akses kepada Pihak Eksternal Pemilik informasi sebagai pihak yang memberikan izin atas permintaan akses informasi kepada pihak eksternal harus memperhatikan hal-hal sebagai berikut:

- 1) Permohonan tertulis pihak eksternal atas setiap jenis informasi yang akan diakses dan fasilitasnya;
- 2) Akses fisik, akses logik oleh pengguna dan sambungan jaringan antara Pemerintah Kota Semarang dengan pihak eksternal, baik akses on-site, off-site maupun remote-site;
- 3) Klasifikasi keamanan informasi dengan mempertimbangkan nilai, sensitifitas informasi dan tingkat risiko Pemerintah Kota Semarang;
- 4) Pihak-pihak eksternal lain yang terlibat dalam penanganan aset informasi di Pemerintah Kota Semarang dan pengendalian yang diperlukan untuk melindungi informasi yang tidak boleh diakses oleh pihak eksternal;
- 5) Perbedaan pemahaman dan pengendalian yang dilakukan pihak eksternal dalam hal penyimpanan, pemrosesan, komunikasi, pertukaran, dan perubahan informasi;
- 6) Dampak hak akses tidak tersedia bagi pihak eksternal saat dibutuhkan atau dampak kesalahan informasi yang diterima oleh pihak eksternal.

d. Pengendalian Akses Jaringan dan Sistem Operasi

- 1) Mengendalikan akses ke jaringan data dan layanan yang ada di jaringan data. Pengendalian tersebut dengan menetapkan kriteria yang harus dipenuhi, pihak yang diperbolehkan mengakses jaringan data, serta jaringan/layanan jaringan yang bisa diakses;
- 2) Memperoleh kepastian mengenai sumber sambungan jaringan dengan mengotentifikasi pengguna sambungan jaringan tersebut. Pengendalian otentifikasi tambahan dapat diimplementasikan untuk pengendalian akses melalui jaringan lain;
- 3) Menggunakan peralatan akses jaringan khusus yang hanya dapat digunakan bersama dengan teknik tertentu. Peralatan tersebut harus dapat mengidentifikasi jaringan yang mendapatkan izin untuk diakses dan harus

selalu memastikan keamanan peralatan tersebut;

- 4) Menetapkan domain jaringan berdasarkan pada penilaian risiko dan tingkat kebutuhan keamanan untuk setiap domain;
- 5) Memastikan bahwa penggunaan jaringan selalu dipantau, dibatasi, atau dilarang untuk tujuan tertentu. Tujuan tertentu tersebut antara lain email pribadi, pemindahan data yang tidak ada kaitannya dengan kegiatan Pemerintah Kota Semarang, akses interaktif dan aplikasi interaktif yang dapat memindahkan data ketempat lain;
- 6) Memastikan bahwa penggunaan jaringan bersama, khususnya yang keluar dari Pemerintah Kota Semarang telah memiliki pengendalian tambahan terutama jika terdapat jaringan yang dapat digunakan bersama dengan pihak ketiga (pengguna diluar Pemerintah Kota Semarang);
- 7) Berkaitan dengan pengelolaan komputer pengguna harus dipastikan bahwa:
 - a) Di setiap komputer pengguna telah menampilkan peringatan bahwa komputer hanya dapat diakses oleh pihak yang mempunyai otorisasi;
 - b) Komputer pengguna tidak memperlihatkan karakter untuk password yang sedang dimasukkan pada saat log-on;
 - c) Komputer pengguna tidak menampilkan sistem atau aplikasi sampai proses log-on benar-benar selesai;
 - d) Layar komputer harus bersih pada saat istirahat (time-out). Aplikasi harus ditutup setelah jangka waktu tertentu apabila tidak digunakan.
- 8) Berkaitan dengan pengelolaan akun dan password, harus dipastikan bahwa:
 - a) Seluruh pegawai Pemerintah Kota Semarang/pengguna selalu menggunakan user ID dan password untuk menjaga akuntabilitas informasi. Pengendalian –*unique identifier* (user ID) berlaku pada seluruh jenis pengguna sistem informasi di Pemerintah Kota Semarang;
 - b) User ID selalu digunakan sehingga aktivitas pengguna dan fungsi dapat dilacak, dibatasi dan dikendalikan;
 - c) Kepentingan pribadi atau diluar kegiatan Pemerintah Kota Semarang tidak diperbolehkan menggunakan akun yang sama dengan akun untuk kegiatan Pemerintah Kota Semarang;
 - d) Pada keadaan tertentu penggunaan ID bersama untuk grup atau pekerjaan tertentu diperbolehkan setelah mendapatkan persetujuan Manajer Keamanan Informasi;
 - e) Terdapat rekaman pengguna, penggunaan password, serta catatan

- penggunaan password yang sama dan atau berulang;
- f) Penyimpanan password para pengguna di tempat atau sistem terpisah dari data sistem aplikasi, serta terlindung pada saat pembuatan, penyimpanan dan pengirimannya;
 - g) Setiap pengguna diwajibkan untuk menggunakan pedoman identifikasi, otentifikasi, dan otorisasi dalam menggunakan utilitas sistem operasi. Penggunaan utilitas sistem operasi dibatasi dan harus terdapat rekaman/log dari seluruh penggunaannya;
 - h) Seluruh akun yang sudah tidak digunakan harus dihapus/dibuang/dinonaktifkan;
- 9) Menentukan peralatan komunikasi yang tepat dan dapat digunakan di Pemerintah Kota Semarang, termasuk metode pengamanan akses jarak jauh, serta piranti lunak dan piranti keras pendukungnya;
- 10) Seluruh pegawai Pemerintah Kota Semarang/pengguna disarankan untuk tidak meninggalkan seluruh piranti mobile computer dan alat komunikasi tanpa mendapat penjagaan dan perhatian seperti di mobil, kamar hotel, conference center, tempat rapat.

8. Persandian (Kriptografi)

8.1 Ruang Lingkup dan Tujuan

Tujuan dari kebijakan terkait teknologi kriptografi untuk memastikan penggunaan teknologi kriptografi yang sesuai dan efektif untuk melindungi kerahasiaan, keaslian dan/atau integritas dari informasi, serta penggunaan teknologi kriptografi dalam pengolahan dan penyimpanan informasi di dalam lingkungan Pemerintah Kota Semarang.

8.2 Kebijakan Kriptografi

- a. Kontrol kriptografi dapat digunakan untuk menjamin kerahasiaan dan integritas dari informasi sensitif di lingkungan perangkat daerah.
- b. Kontrol kriptografi dapat mencakup namun tidak terbatas pada: 1) Enkripsi informasi dan jaringan komunikasi; 2) Pemeriksaan integritas informasi, seperti *hashing*; 3) Otentikasi identitas; 4) tanda tangan elektronik (*Digital signatures*);
- c. Implementasi dari kontrol kriptografi harus mempertimbangkan klasifikasi dari informasi yang akan diamankan.
- d. Pemilihan kontrol kriptografi harus mempertimbangkan: 1) Jenis dari

kontrol kriptografi; 2) Kekuatan dari algoritma kriptografi; dan 3) Panjang dari kunci kriptografi.

- e. Implementasi dari kontrol kriptografi harus secara berkala ditinjau untuk memastikan kecukupan dan kesesuaian dari kontrol tersebut dalam mengamankan kerahasiaan dan integritas dari informasi.
- f. Pengelolaan dari kunci kriptografi harus dikendalikan secara ketat dan dibatasi hanya pada personil yang terotorisasi.
- g. Pengelolaan dari kunci kriptografi didasarkan pada prinsip dual custody untuk mengurangi risiko penyalahgunaan.

9. Pengendalian Fisik dan Lingkungan

9.1 Ruang Lingkup dan Tujuan

Ruang lingkup fisik dan lingkungan meliputi wilayah kerja dan peralatan kerja. Pengamanan wilayah kerja termasuk batasan keamanan fisik, pengendalian akses fisik, keamanan kantor, ruangan, dan fasilitas, perlindungan terhadap ancaman dari lingkungan eksternal, area akses publik, pengantaran, dan penerimaan, aktivitas pekerjaan di area rahasia;

Pengamanan peralatan kerja termasuk penempatan peralatan dan perlindungannya, fasilitas pendukung, keamanan instalasi kabel, pemeliharaan peralatan, keamanan peralatan yang berada di luar lingkungan Pemerintah Kota Semarang, keamanan penghapusan dan penggunaan ulang peralatan atau media informasi, pemindahan aset informasi.

Tujuan pengendalian fisik dan lingkungan yaitu:

Menghindari terjadinya akses fisik secara ilegal, penghancuran, atau campur tangan dari pihak lain terhadap aset informasi di lingkungan Pemerintah Kota Semarang;

Menghindari terjadinya kehilangan, kerusakan, pencurian, persekongkolan terhadap aset dan informasi, serta gangguan lainnya akibat aktivitas yang dilakukan oleh Pemerintah Kota Semarang.

9.2 Kebijakan Pengendalian Fisik dan Lingkungan

9.2.1 Kebijakan Pengamanan Wilayah Kerja

- a. Pengendalian Akses Fisik Pengendalian akses fisik dilakukan dengan:
 - 1) Mencatat setiap tamu yang datang;
 - 2) Mengawasi setiap tamu yang datang;
 - 3) Memberikan hak akses hanya sebatas keperluan tamu tersebut;

- 4) Menginformasikan syarat-syarat keamanan dan pedoman yang harus diikuti selama berada di lingkungan Pemerintah Kota Semarang;
- 5) Memberikan kartu identitas selama berada di lingkungan Pemerintah Kota Semarang untuk Seluruh pegawai Pemerintah Kota Semarang, kontraktor, dan pengguna eksternal;
- 6) Reviu terhadap izin pemberian hak akses ke wilayah kerja yang di dalamnya terdapat informasi dan fasilitas pengolahnya, atau jika diperlukan, merekomendasikan untuk menghapus hak akses tersebut.

b. Keamanan Kantor, Ruangan, dan Fasilitas Keamanan kantor dilakukan dengan:

- 1) Menempatkan dan menyimpan secara aman fasilitas utama pengolah informasi dan fasilitas lainnya;
- 2) Menempatkan gedung/wilayah kerja yang sensitif dilokasi yang tidak mudah terlihat dan hanya memberikan izin masuk secara terbatas untuk tujuan-tujuan tertentu;
- 3) Antisipasi atas kemungkinan terjadinya akses secara umum terhadap buku petunjuk dan buku telpon internal yang berisi informasi yang sensitif beserta fasilitasnya.

c. Perlindungan terhadap ancaman dari lingkungan eksternal

Perlindungan terhadap ancaman dari lingkungan eksternal dilakukan dengan:

- 1) Meletakkan dan menyimpan benda-benda yang berbahaya pada jarak yang cukup aman dari wilayah kerja yang di dalamnya terdapat aset informasi dan fasilitas pengolahnya;
- 2) Menyediakan dan menempatkan peralatan pemadam kebakaran di setiap lokasi/wilayah kerja yang memerlukan penjagaan khusus;
- 3) Menyimpan media back-up pada jarak yang cukup aman untuk menghindari kerusakan akibat bencana alam atau bencana sosial.

d. Area Akses Publik, Pengantaran, dan Penerimaan

Keamanan area akses publik, pengantaran dan penerimaan dilakukan dengan:

- 1) Membatasi hak akses untuk wilayah pengantaran dan penerimaan barang dari luar Pemerintah Kota Semarang;
- 2) Merancang wilayah pengantaran dan penerimaan barang sehingga persediaan/peralatan dapat ditempatkan atau dipindahkan ke bagian lain tanpa melibatkan kurir eksternal Pemerintah Kota Semarang;
- 3) Melakukan pemeriksaan terhadap barang-barang yang akan dimasukkan ke lingkungan Pemerintah Kota Semarang di tempat pengantaran dan

penerimaan barang sebelum barang-barang tersebut dialokasikan ke unit-unit Pemerintah Kota Semarang;

- 4) Mendaftarkan barang-barang yang masuk ke Pemerintah Kota Semarang.
- e. Aktivitas Pekerjaan di Area Rahasia. Keamanan aktivitas pekerjaan di area rahasia dilakukan dengan:
- 1) Memastikan bahwa setiap orang yang bekerja di wilayah yang terdapat informasi yang sensitif dan fasilitasnya harus mengerti dan tahu bahwa tempat di mana ia beraktivitas adalah wilayah yang harus dijaga keamanannya;
 - 2) Harus melakukan antisipasi untuk pekerjaan yang tidak terpantau;
 - 3) Mengamankan wilayah-wilayah kerja yang belum digunakan dengan dikunci secara fisik dan harus diperiksa secara rutin;
 - 4) Melarang masuknya alat dengan kemampuan merekam ke dalam wilayah-wilayah kerja tertentu, kecuali telah ada izin sebelumnya.

9.2.2 Kebijakan Pengamanan Peralatan Kerja

a. Penempatan Peralatan dan Perlindungannya

Keamanan penempatan peralatan dan perlindungannya dilakukan dengan:

- 1) Menempatkan semua peralatan sesuai dengan tempatnya;
- 2) Melindungi peralatan yang digunakan mengolah informasi yang bersifat sensitif menempatkan fasilitas pengolah informasi yang menangani data yang sensitif sedemikian rupa sehingga pada saat aplikasi digunakan, informasi yang ada di layar tidak dapat dilihat oleh orang yang tidak berkepentingan;
- 3) Menempatkan jenis peralatan yang membutuhkan perlindungan secara khusus di tempat yang khusus juga;
- 4) Melakukan pengendalian untuk meminimalisir risiko ancaman fisik yang potensial, seperti: pencurian, kebakaran, ledakan bom, asap, banjir, efek zat kimia, gangguan komunikasi;
- 5) Menyediakan penangkal petir untuk setiap gedung di lingkungan Pemerintah Kota Semarang dan menyesuaikannya untuk seluruh jalur komunikasi dan tenaga listrik yang digunakan;
- 6) Melakukan pengawasan untuk mendeteksi kondisi lingkungan, seperti suhu dan kelembaban, yang bisa mempengaruhi berfungsinya fasilitas pengolah informasi.
- 7) Membuat peraturan untuk aktivitas makan, minum, dan merokok di wilayah yang dekat dengan fasilitas pengolah informasi.

b. Fasilitas Pendukung Keamanan fasilitas pendukung dilakukan dengan:

- 1) Memastikan jumlah seluruh fasilitas pendukung (seperti air, listrik, pemanas, ventilasi, AC) telah mencukupi untuk kebutuhan di seluruh lingkungan Pemerintah Kota Semarang;
- 2) Memastikan jumlah bahan bakar telah tersedia dan mencukupi untuk generator jika terjadi padam listrik;
- 3) Menyiapkan penerangan darurat untuk mengantisipasi terjadinya padam listrik;
- 4) Memeriksa secara rutin semua peralatan UPS dan generator untuk memastikan kecukupan kapasitas yang diperlukan oleh Pemerintah Kota Semarang;
- 5) Meletakkan tombol listrik darurat di dekat pintu keluar darurat di ruang peralatan untuk mengantisipasi keadaan darurat;
- 6) Memastikan bahwa persediaan air telah cukup dan stabil untuk memfasilitasi pendingin ruangan, kelembaban, dan sistem pemadam kebakaran;
- 7) Memeriksa ulang dan, jika diperlukan, memasang kembali sistem alarm untuk mendeteksi kegagalan fungsi pada fasilitas pendukung;
- 8) Memastikan peralatan telekomunikasi harus disambungkan dengan penyedia jasa fasilitas setidaknya dengan dua sambungan/jalur yang berbeda untuk mengantisipasi jika terjadi kerusakan pada salah satu sambungan/jalur.

c. Keamanan Instalasi Kabel Keamanan instalasi kabel dilakukan dengan:

- 1) Menempatkan sambungan listrik dan telepon yang berhubungan dengan fasilitas pemrosesan informasi di bawah tanah atau tempat lain yang aman sebagai alternatif perlindungan;
- 2) Melindungi jaringan kabel dari pemotongan ilegal dan kerusakan;
- 3) Melakukan pengidentifikasian kabel dan penandaan peralatan secara jelas untuk meminimalisir kesalahan penanganan;
- 4) Melakukan pencatatan untuk daftar pemotongan kabel dengan tujuan mengurangi kemungkinan terjadinya kesalahan;
- 5) Melakukan instalasi untuk saluran lapis baja dan ruangan atau kotak yang terkunci pada titik pemeriksaan dan pemberhentian;
- 6) Menggunakan rute alternatif dan atau media pengiriman yang menyediakan keamanan yang memadai;

- 7) Menggunakan instalasi kabel dengan fiber optik;
- 8) Menggunakan pelindung elektromagnetik untuk melindungi kabel;
- 9) Melakukan teknik penghapusan dan pemeriksaan fisik untuk media ilegal yang di sambung ke kabel;
- 10) Melakukan pengendalian akses fisik untuk panel sambungan dan ruang kabel.

d. Pemeliharaan Peralatan Keamanan pemeliharaan peralatan dilakukan dengan:

- 1) Melakukan perawatan secara rutin untuk semua peralatan milik Pemerintah Kota Semarang sesuai dengan petunjuk pemeliharaan dan dengan memperhatikan spesifikasi peralatan tersebut;
- 2) Membuat catatan mengenai dugaan kesalahan, pencegahan, dan pemeliharaan terhadap peralatan Pemerintah Kota Semarang;
- 3) Melakukan pengendalian terhadap perawatan yang telah dilaksanakan.

e. Keamanan Peralatan yang Berada di Luar Lingkungan Pemerintah Kota Semarang

Keamanan peralatan yang berada di luar lingkungan Pemerintah Kota Semarang dilakukan dengan:

- 1) Melakukan pelarangan untuk membawa keluar dari lingkungan Pemerintah Kota Semarang setiap bentuk peralatan atau media yang berisi informasi atau fasilitas pengolah informasi tanpa pengawasan yang memadai kecuali peralatan mobile dengan prosedur khusus;
- 2) Melakukan peninjauan secara rutin terhadap petunjuk pemeliharaan untuk setiap peralatan sesuai dengan spesifikasinya.

f. Keamanan Penghapusan Dan Penggunaan Ulang Peralatan atau Media Informasi
Keamanan penghapusan dan penggunaan ulang peralatan atau media informasi dilakukan dengan:

- 1) Menghancurkan dan menghapuskan setiap benda atau media informasi yang sensitif, jika ia tidak akan digunakan lagi;
- 2) Menggunakan / memilih metode penghapusan yang khusus agar informasi yang terdapat di dalamnya tidak dapat dilacak kembali;
- 3) Melakukan penilaian risiko untuk media yang rusak tetapi berisi informasi sensitif untuk menentukan apakah media tersebut akan dihancurkan seluruhnya atau diperbaiki kembali.

g. Pemindahan Aset Informasi Keamanan pemindahan aset informasi dilakukan dengan:

- 1) Memastikan bahwa seluruh aset informasi seperti peralatan, dokumen, software, tidak dipindahkan tanpa izin;
- 2) Menentukan siapa saja pihak-pihak yang berhak melakukan pemindahan aset informasi dan memberikan izin atas pemindahan aset informasi tersebut;
- 3) Menetapkan batas waktu peminjaman atau pemindahan peralatan dan melakukan pengecekan atas pengembalian peralatan tersebut serta melakukan pencatatan waktu peminjaman atau pemindahan dan pengembalian peralatan tersebut.

10. Pengendalian Aspek Sumber Daya Manusia

10.1 Ruang Lingkup dan Tujuan

Ruang lingkup pengendalian aspek SDM yaitu proses pemeriksaan dan verifikasi latar belakang (*screening*) calon pegawai, sosialisasi peran dan tanggung jawab dalam keamanan informasi termasuk perjanjian kerahasiaan, pendidikan dan pelatihan peningkatan keamanan informasi, dan perubahan dan/atau penghapusan hak akses informasi dan pengembalian aset informasi jika ada pemberhentian, perubahan, atau berakhirnya perjanjian kerja Tujuan pengendalian aspek SDM yaitu:

- a. Memastikan bahwa seluruh pegawai Pemerintah Kota Semarang memahami peran dan tanggung jawab mereka terhadap keamanan informasi untuk mengurangi risiko terjadinya pencurian, kecurangan, dan penyalahgunaan aset informasi dan fasilitas pengolahnya;
- b. Memastikan bahwa seluruh pegawai Pemerintah Kota Semarang waspada terhadap ancaman keamanan informasi sehingga mereka sadar akan peran dan tanggungjawab mereka untuk mengurangi risiko terjadinya insiden karena faktor kelalaian manusia;
- c. Memastikan bahwa proses pemberhentian atau perubahan pegawai Pemerintah Kota Semarang dilakukan dengan cara yang benar.

10.2 Kebijakan Pengendalian Aspek Sumber Daya Manusia

Pengendalian Aspek SDM dibagi enam adalah proses pemeriksaan dan verifikasi latar belakang (*Screening*), sosialisasi peran dan tanggung jawab dalam keamanan informasi, perjanjian kerahasiaan, pendidikan dan pelatihan peningkatan keamanan informasi, pengembalian aset informasi, dan perubahan dan/atau penghapusan hak akses informasi.

Berikut kebijakan pada masing-masing bagian tersebut;

a. Proses pemeriksaan dan verifikasi latar belakang (*Screening*)

- 1) Melakukan proses verifikasi dan pemeriksaan mengenai latar belakang

untuk semua calon pegawai Pemerintah Kota Semarang untuk memastikan bahwa latar belakang mereka telah memenuhi persyaratan sesuai peraturan hukum perundang-undangan dan etika, serta sesuai dengan persyaratan yang ditetapkan oleh Pemerintah Kota Semarang;

- 2) Proses pemeriksaan dan verifikasi latar belakang (*screening*) harus meliputi informasi-informasi berikut:
 - a) Keterangan mengenai karakter yang dimiliki, baik secara individu maupun organisasi.
 - b) Keterangan mengenai daftar riwayat hidup yang lengkap.
 - c) Konfirmasi mengenai kualifikasi pendidikan dan akademis.
 - d) Keterangan mengenai kompetensi.
 - e) Keterangan mengenai catatan kriminal (jika ada).
 - f) Kegiatan dalam dunia maya termasuk cracking.

b. Sosialisasi Peran dan Tanggungjawab dalam Keamanan Informasi

- 1) Memberikan arahan yang memadai kepada para pegawai Pemerintah Kota Semarang, mengenai peran dan tanggungjawab mereka terhadap keamanan informasi sebelum hak akses diberikan kepada mereka.
- 2) Memotivasi pegawai Pemerintah Kota Semarang agar memiliki rasa kesadaran akan peran dan tanggungjawab mereka terhadap keamanan informasi sehingga dapat memenuhi semua kebijakan keamanan informasi di lingkungan Pemerintah Kota Semarang.

c. Perjanjian Kerahasiaan

- 1) Memastikan bahwa seluruh pegawai dan pemangku kepentingan lain yang memiliki tugas teknologi informasi dan komunikasi di lingkungan Pemerintah Kota Semarang menyetujui peran dan tanggungjawab keamanan informasi yang diberikan kepada mereka dengan menandatangani surat perjanjian yang menyatakan kesanggupan menjaga kerahasiaan dan larangan penyingkapan untuk jenis aset informasi yang bersifat sensitif bagi Pemerintah Kota Semarang.
- 2) Seluruh pegawai dan pemangku kepentingan lain yang memiliki tugas teknologi informasi dan komunikasi di lingkungan Pemerintah Kota Semarang harus menandatangani perjanjian kerahasiaan sebagai bagian dari perjanjian kerja.
- 3) Memastikan bahwa seluruh rekanan penyedia barang dan jasa di Pemerintah Kota Semarang telah menyetujui peran dan tanggungjawab

keamanan informasi yang diberikan kepada mereka dengan menandatangani surat perjanjian yang menyatakan kesanggupan menjaga kerahasiaan dan larangan penyingkapan untuk jenis aset informasi yang bersifat sensitif bagi Pemerintah Kota Semarang .

- 4) Memastikan bahwa seluruh pemangku kepentingan yang menjadi rekan kerja Pemerintah Kota Semarang telah menyetujui peran dan tanggungjawab keamanan informasi yang diberikan kepada mereka dengan menandatangani surat perjanjian yang menyatakan kesanggupan menjaga kerahasiaan dan larangan penyingkapan untuk jenis aset informasi yang bersifat sensitif bagi Pemerintah Kota Semarang dan yang dilarang menurut peraturan perundangan yang berlaku.
- 5) Hal-hal yang harus diperhatikan dalam perjanjian kerahasiaan antara lain adalah sebagai berikut:
 - a) Setiap butir perjanjian yang disetujui tidak mengandung kesalahpahaman dan Pemerintah Kota Semarang mendapat jaminannya dan sesuai dengan kebijakan keamanan informasi yang berlaku.
 - b) Pedoman perlindungan informasi serta mekanisme dan pengendalian atas perlindungan fisik yang dibutuhkan termasuk pengendalian untuk memastikan perlindungan dari penyalahgunaan aplikasi.
 - c) Pengendalian untuk memastikan pengembalian atau penghancuran aset informasi yang penting dan rahasia pada saat berakhirnya perjanjian.
 - d) Kerahasiaan, keintegritasan, dan ketersediaan terhadap hak kekayaan intelektual dan hak cipta, dan pembatasan untuk pengandaan dan penyingkapan informasi.
 - e) Struktur pelaporan yang jelas dan format pelaporan yang telah disetujui mengenai keamanan informasi, termasuk pengaturan untuk masalah-masalah perubahan yang jelas dan spesifik.
 - f) Perbedaan alasan, persyaratan, dan keuntungan yang didapat dan dibutuhkan oleh pihak-pihak yang memiliki hak akses atas informasi.
 - g) Persyaratan untuk mengurus daftar personil yang diizinkan menggunakan jasa layanan yang tersedia, termasuk juga hak

khusus mereka dalam hal penggunaan dan pernyataan bahwa seluruh akses yang tidak memiliki persetujuan adalah dilarang.

- h) Pengaturan mengenai pelaporan, pengumuman, dan penyelidikan atas kasus keamanan informasi dan pelanggaran keamanan, termasuk juga pelanggaran atas persyaratan.
- i) Hak untuk mengawasi, mencabut, dan semua aktivitas yang bersinggungan dengan aset informasi Pemerintah Kota Semarang termasuk proses untuk mencabut hak akses atau memotong sambungan antara dua sistem.
- j) Hak untuk mengaudit semua bentuk tanggungjawab yang telah ditetapkan dalam perjanjian, di mana audit dilakukan oleh pihak ketiga, dan mengakumulasikan hak dasar bagi para auditor.
- k) Keterlibatan pihak ketiga dengan subkontraktor, dan implementasi dari pengendalian keamanan terhadap subkontraktor termasuk rencana antisipasi untuk kemungkinan terjadinya/timbulnya keinginan dari pihak ketiga untuk mengakhiri perjanjian sebelum waktunya.
- l) Dokumentasi terakhir/terbaru mengenai daftar aset, lisensi, perjanjian atau hak yang berhubungan dengan pihak ketiga, termasuk negosiasi ulang untuk suatu perjanjian jika persyaratan keamanan di lingkungan Pemerintah Kota Semarang berubah.

d. Pendidikan dan Pelatihan Peningkatan Keamanan Informasi

Merancang dan memberikan pendidikan dan pelatihan di seluruh lingkungan Pemerintah Kota Semarang secara rutin dengan tujuan sebagai berikut:

- 1) Membangun kesadaran akan keamanan informasi;
- 2) Mengenali masalah-masalah keamanan informasi dan kasus-kasus yang mungkin terjadi;
- 3) Mengantisipasi adanya perubahan dalam kebijakan atau pedoman yang berlaku.

e. Sanksi atas Pelanggaran Pengendalian Keamanan Informasi

- 1) Melakukan proses pendisiplinan kepada seluruh pegawai dan pemangku kepentingan yang memiliki tugas teknologi informasi dan komunikasi di lingkungan Pemerintah Kota Semarang, yang terbukti melakukan pelanggaran keamanan informasi dengan memberikan sanksi sesuai dengan tingkat pelanggaran yang dilakukan.

- 2) Merancang dan menentukan bentuk-bentuk sanksi yang akan diberikan dan sebisa mungkin proses pendisiplinan ini dapat dijadikan alat pencegahan untuk mengantisipasi atau meminimalisir terjadinya pelanggaran terhadap kebijakan keamanan informasi.
- 3) Mengambil tindakan tegas jika pegawai Pemerintah Kota Semarang terbukti melakukan pelanggaran terhadap persyaratan, kebijakan, dan pedoman keamanan informasi yang berlaku.

Pengembalian Aset Informasi

- 1) Memastikan bahwa setiap perjanjian kerja untuk para pegawai Pemerintah Kota Semarang yang dibuat telah mencakup ketentuan mengenai tanggungjawab dan tugas yang terkait dengan keamanan informasi yang harus diselesaikan sesaat setelah pemberhentian / perubahan dilakukan.
- 2) Jika seorang pegawai Pemerintah Kota Semarang yang akan memasuki tahap pemberhentian / perubahan penugasan memiliki informasi atau pengetahuan yang cukup banyak dan penting bagi keperluan dan tujuan Pemerintah Kota Semarang, harus dipastikan bahwa informasi dan pengetahuan itu telah didokumentasikan dan disampaikan kepada Pemerintah Kota Semarang secara lengkap dan jelas.
- 3) Pada proses pemberhentian, perubahan, atau berakhirnya masa perjanjian, harus dipastikan bahwa setiap pegawai Pemerintah Kota Semarang telah mengembalikan seluruh aset informasi yang selama ini menjadi kewenangannya kepada Pemerintah Kota Semarang dengan memindahkan setiap aset informasi dari media pribadi ke media milik Pemerintah Kota Semarang atau dengan menghapuskannya dari media pribadi tersebut.

g. Penghapusan dan/atau Perubahan Hak Akses

- 1) Memastikan bahwa semua hak akses yang dimiliki oleh pegawai Pemerintah Kota Semarang telah dihapuskan sesaat setelah pemberhentian, perubahan, atau berakhirnya perjanjian kerja.
- 2) Hak akses yang harus dihapuskan meliputi: akses fisik, akses logis, kunci, kartu identitas, fasilitas pengolah informasi, dll.
- 3) Penghapusan hak akses sesaat sebelum memasuki pemberhentian atau perubahan penugasan dilakukan dengan memperhatikan hal-hal berikut:
 - a) Inisiatif dan alasan dilakukannya pemberhentian atau perubahan.
 - b) Tanggungjawab terakhir atau terkini dari pegawai Pemerintah Kota Semarang.

- c) Nilai dari aset informasi terkini yang dapat diakses oleh pegawai Pemerintah Kota Semarang.
- 4) Melakukan antisipasi bagi pegawai Pemerintah Kota Semarang, pemangku kepentingan lain, kontraktor, dan pihak yang merasa tidak puas dengan pemberhentian tersebut dan mungkin melakukan pencurian aset informasi yang penting dan sensitif.
- 5) Melakukan tindakan pengarahan kepada kelompok yang masih memiliki hak akses terhadap aset informasi untuk tidak lagi berbagi informasi kepada pegawai yang sudah tidak memiliki hak akses karena adanya pemberhentian atau perubahan penugasan untuk hak akses secara kelompok.

11. Pengamanan Pengembangan dan Pemeliharaan Sistem Informasi

11.1 Ruang Lingkup dan Tujuan

Ruang lingkup pengamanan pengembangan dan pemeliharaan sistem operasi yaitu pertimbangan keamanan dalam pengembangan dan pemeliharaan, pengendalian aplikasi, penggunaan enkripsi, pengamanan kode sumber, file sistem dan data pengujian, manajemen perubahan, pengendalian kebocoran informasi dan kelemahan teknis.

Tujuan pengamanan pengembangan dan pemeliharaan sistem informasi yaitu untuk memastikan keamanan menjadi bagian integral dari sistem informasi.

11.2 Kebijakan Pengamanan Pengembangan dan Pemeliharaan Sistem Informasi

Pengamanan pengembangan dan pemeliharaan sistem informasi terdiri dari beberapa kebijakan yaitu pertimbangan keamanan dalam pengembangan dan pemeliharaan, pengendalian aplikasi, penggunaan enkripsi, pengamanan kode sumber, file sistem dan data pengujian, manajemen perubahan, pengendalian kebocoran informasi dan kelemahan teknis.

Berikut kebijakan pada masing-masing bagian tersebut.

a. Pertimbangan Keamanan dalam Pengembangan dan Pemeliharaan

Dalam pengembangan dan pemeliharaan, pertimbangan berikut harus diperhatikan.

- 1) Nilai aset informasi dan kemungkinan gangguan terhadap aktivitas Pemerintah Kota Semarang karena kegagalan sistem informasi;
- 2) Integrasi sistem dengan sistem yang dimiliki Pemerintah Kota Semarang;
- 3) Kriteria keamanan dalam kontrak dengan vendor;

- 4) Penilaian risiko terhadap produk yang tidak memenuhi persyaratan keamanan yang diperlukan dan menentukan kendali alternatif untuk meminimalkan risiko;
- 5) Reviu keamanan pada fitur-fitur tambahan. Apabila dapat meningkatkan risiko keamanan informasi maka fitur tersebut sebaiknya tidak digunakan;
- 6) Evaluasi keamanan oleh pihak ketiga apabila diperlukan.

b. Pengendalian Aplikasi

Aplikasi yang ada di Pemerintah Kota Semarang harus memiliki pengendalian memadai, minimal mampu melakukan validasi data masukan, validasi pemrosesan, dan validasi data keluaran. Validasi tersebut dilakukan dengan menerapkan hal-hal berikut.

- 1) Pemeriksaan data masukan, data referensi (nama, alamat, nomer referensi), dan parameter lainnya, termasuk dokumen sumber data masukan dari perubahan yang tidak diotorisasi.
- 2) Pemeriksaan secara berkala terhadap isi key field dan data field untuk menegaskan validasi dan integritas data.
- 3) Pedoman khusus dalam menghadapi kesalahan validasi (apabila terjadi kesalahan), serta pengujian kewajaran data masukan.
- 4) Penetapan tanggung-jawab untuk setiap pegawai / personel yang terlibat dalam proses pemasukan data.
- 5) Pencatatan/perekaman seluruh kegiatan proses pemasukan data.
- 6) Penggunaan pengujian dan pemvalidasi secara otomatis yang digunakan untuk mengurangi risiko kesalahan dalam memasukkan data dan mencegah buffer overrun / overflow dan *code injection*.
- 7) Perancangan dan implementasi aplikasi diharuskan dapat meminimalisasi risiko kesalahan dalam pemrosesan informasi.
- 8) Program aplikasi yang digunakan beroperasi dengan benar pada waktu yang telah ditentukan dan jika terjadi kesalahan maka pemrosesan berikutnya segera dihentikan.
- 9) Validasi hasil keluaran, yang meliputi pengujian kewajaran data keluaran, tanggung-jawab untuk setiap pegawai dan personil yang terlibat dalam pemrosesan data keluaran dan catatan atas aktivitas proses validasi data keluaran.

c. Penggunaan Enkripsi

Pada pengembangan aplikasi, informasi yang ada di aplikasi Pemerintah Kota

Semarang harus disandi sesuai dengan tingkatan klasifikasi keamanan informasi dan kunci enkripsi telah dikelola dengan baik sesuai dengan peraturan perundang-undangan, dengan melaksanakan hal-hal sebagai berikut:

- 1) Menerapkan enkripsi pada informasi yang sensitif/kritikal baik selama penyimpanan maupun pemindahan untuk memastikan kerahasiaan
- 2) Menggunakan tanda tangan elektronik atau kode otentifikasi pada pesan yang sensitif/kritikal baik selama penyimpanan maupun pemindahan untuk memastikan integritas/otentifikasi
- 3) Menggunakan teknik kriptografi untuk membuktikan terjadi atau tidaknya suatu kejadian atau tindakan untuk memastikan non-repudiasi.

d. Pengamanan Kode Sumber, File Sistem, dan Data Pengujian

Pengamanan kode sumber, file sistem dan data pengujian dengan memastikan bahwa (i) kode sumber aplikasi, file-file sistem dan data pengujian aplikasi telah dikendalikan dengan baik, (ii) instalasi atas aplikasi hanya dilakukan oleh pihak yang berhak, sesuai pedoman, dan (iii) perubahan atas berbagai paket aplikasi harus diminimalisir dan dikendalikan dengan baik, antara lain dengan melaksanakan hal berikut.

- 1) Penggunaan sistem operasi dengan kode yang sah;
- 2) Pemutakhiran piranti lunak, aplikasi dan program dilakukan oleh pegawai yang terlatih dan telah mendapat otorisasi;
- 3) Analisa risiko terkait apabila menggunakan piranti lunak (software) yang tidak mendapat dukungan/bantuan pelayanan dari vendor;
- 4) Pemastian vendor yang mensuplai piranti lunak (software) dapat membantu apabila dibutuhkan dan aktivitas pemeliharaan oleh vendor tersebut harus senantiasa dipantau;
- 5) Pengujian piranti lunak atau aplikasi harus dilakukan dan strategi rollback harus dapat dilakukan sebelum mengubah sistem yang telah diimplementasikan;
- 6) Pedoman yang digunakan dalam sistem aplikasi pada lingkungan operasional juga diterapkan pada lingkungan pengujian sistem aplikasi, dan harus dilakukan pemisahan otorisasi setiap informasi operasi yang diduplikat (copy) ke sistem pengujian aplikasi, sertainformasi mengenai data pengujian harus segera dihapuskan setelah pengujian selesai dilakukan.
- 7) Penjagaan data kode sumber (source code) secara ketat dan kode sumber tersebut tidak boleh berada dalam lingkungan operasional.

- 8) Pembatasan akses pegawai pendukung/tambahan/sementara pada bagian sistem informasi terhadap kumpulan data kode sumber (source code)
- 9) Pemeliharaan, penduplikasian, pemutakhiran kumpulan kode sumber (source code) dan dokumen terkait, yang hanya bisa dilakukan setelah mendapatkan otorisasi dari petugas yang berwenang
- 10) Pemeliharaan rekaman hasil pemeriksaan/audit yang berhubungan dengan akses kumpulan program sumber.

e. Manajemen Perubahan

Keamanan dalam manajemen perubahan dilakukan dengan beberapa hal berikut:

- 1) Persetujuan resmi harus dilakukan sebelum pelaksanaan perubahan dan penjagaan dokumen persetujuan perubahan dari pihak yang terkait;
- 2) Pemberitahuan harus dilakukan ketika akan ada perubahan sehingga dapat direviu dan diuji sebelumnya dan perubahan tersebut dimasukkan dalam rencana keberlangsungan;
- 3) Pemilihan waktu yang tepat dalam perubahan sehingga tidak mengganggu operasi;
- 4) Perubahan dokumentasi pendukung ketika diperlukan dan apabila dilakukan perubahan dokumentasi pendukung, dokumentasi sebelumnya harus segera ditarik atau dimusnahkan;
- 5) Perjanjian lisensi piranti lunak, perjanjian penjaminan dengan pihak lain dalam hal terjadi kegagalan/kebangkrutan pihak out-source, penjaminan kualitas dan keamanan piranti lunak.

f. Pengendalian Kebocoran Informasi dan Kelemahan Teknis

Pengendalian kebocoran informasi dan kelemahan teknis dilakukan dengan beberapa hal berikut.

- 1) Penetapan kelompok atau perorangan yang bertanggung-jawab untuk memantau kelemahan-kelemahan yang ada pada seluruh sistem informasi Pemerintah Kota Semarang , termasuk mengamati media dan komunikasi yang berada diluar area Pemerintah Kota Semarang untuk menghindari informasi yang terselubung, memantau secara berkala terhadap pegawai Pemerintah Kota Semarang maupun aktivitas sistem, memantau penggunaan sumber daya yang ada pada sistem komputer, melakukan pencegahan penggunaan jaringan akses yang tidak terotorisasi untuk melacak saluran terselubung / tersembunyi;
- 2) Pengelolaan informasi spesifik yang sangat dibutuhkan dalam membantu

mengatasi penyerangan, termasuk daftar vendor piranti lunak, nomor versi piranti lunak, daftar instalasi piranti lunak ke sistem yang ada, dan orang yang bertanggung-jawab terhadap piranti lunak tersebut;

- 3) Penetapan peranan dan tanggung jawab monitoring serangan, penilaian risiko terhadap serangan, penutupan celah, pembaharuan (update) piranti lunak yang ada.

12. Pengamanan Operasional Sistem Informasi

12.1 Ruang Lingkup dan Tujuan

Ruang lingkup pengamanan operasional sistem informasi adalah dokumentasi pedoman operasi, proses pemisahan tugas, pengawasan penggunaan sistem informasi, manajemen back-up, pengelolaan keamanan jaringan, pengelolaan layanan jasa pihak ketiga, perencanaan dan perizinan sistem, perlindungan untuk kode-kode berbahaya (*malicious* dan *mobile code*), penanganan media, proses pertukaran informasi, pengelolaan pesan elektronik dan transaksi elektronik, dan informasi yang tersedia untuk umum.

Tujuan pengamanan operasional sistem informasi adalah memberikan panduan pelaksanaan pengendalian keamanan informasi dalam kegiatan operasional sistem informasi dan komunikasi.

12.2 Kebijakan Pengamanan Operasional Sistem Informasi

Pengamanan operasional sistem informasi dibagi tiga belas yaitu pendokumentasian pedoman operasi, pemisahan tugas, pengawasan penggunaan sistem informasi, manajemen back-up, pengelolaan keamanan jaringan, pengelolaan layanan jasa pihak ketiga, perencanaan dan perizinan sistem, perlindungan untuk *malicious* dan *mobile code*, penanganan media, pertukaran informasi, pesan elektronik dan transaksi elektronik, informasi yang tersedia untuk umum.

Berikut kebijakan pada masing-masing bagian tersebut.

a. Pendokumentasian Pedoman Operasi

- 1) Memastikan bahwa seluruh pedoman untuk berbagai aktivitas yang berhubungan dengan pengolahan informasi dan fasilitas komunikasi telah terdokumentasi dengan baik dan diberlakukan dengan resmi;
- 2) Melakukan koordinasi dengan tim Help Desk jika terjadi kondisi yang tidak diharapkan atau mengalami kesulitan teknis.
- 3) Menyusun perintah kerja untuk hal-hal berikut:
 - a) Pengolahan dan penanganan informasi di pusat pengolahan data;
 - b) Proses back-up di pusat pengolahan data;

- c) Persyaratan penjadwalan pekerjaan, langkah awal kerja, dan jangka waktu penyelesaian pekerjaan di pusat pengolahan data;
 - d) Penanganan kesalahan atau kondisi lain yang tidak diharapkan yang mungkin muncul saat pelaksanaan tugas, termasuk pembatasan untuk penggunaan fasilitas sistem di pusat pengolahan data.
- 4) Melakukan penyimpanan untuk dokumentasi sistem secara aman, memperhatikan daftar akses untuk dokumentasi sistem dan persetujuan pemilik aplikasi, dan melindungi sistem pendokumentasian yang diselenggarakan atau disediakan oleh jaringan publik secara memadai.

b. Pemisahan Tugas

Untuk mengurangi risiko terjadinya penyalahgunaan sistem informasi, baik yang disengaja maupun tidak disengaja, harus dilakukan proses pemisahan tugas.

Pemisahan tugas tersebut antara lain pemisahan antara pelaksana dan pemberi izin. Jika pemisahan tugas terjadi kesulitan, maka bentuk pengendalian yang lain seperti pengawasan, log, dan supervisi dari atasan.

Proses pemisahan tugas meliputi:

- 1) Memastikan setiap pengguna informasi hanya dapat melakukan akses dan modifikasi terhadap informasi setelah memperoleh otorisasi formal dan diawasi oleh pihak yang menjadi pemilik informasi;
- 2) Memastikan telah terdapat pemisahan antara wilayah pengembangan, pengujian, dan operasional sistem informasi di Pemerintah Kota Semarang, dengan melaksanakan hal-hal sebagai berikut:
 - a) Memastikan bahwa lingkungan pengembangan aplikasi dan lingkungan operasional aplikasi berada pada sistem atau komputer yang berbeda dan pada domain atau direktori yang berbeda. Lingkungan pengujian sistem dengan lingkungan operasional sistem sedapat mungkin serupa/tidak berbeda;
 - b) Menetapkan pedoman tata cara pemindahan aplikasi dari lingkungan pengembangan ke lingkungan operasional;
 - c) Membatasi akses terhadap compiler, editor, atau alat pengembangan lainnya melalui lingkungan sistem operasional jika tidak terlalu dibutuhkan;
 - d) Melakukan proses pembedaan profil pengguna pada saat pengujian sistem dan pada saat pelaksanaan sistem informasi di Pemerintah Kota Semarang;
 - e) Menyediakan menu yang memberikan petunjuk penggunaan yang memadai untuk mengurangi risiko kesalahan pada seluruh aplikasi yang ada di Pemerintah Kota Semarang;

f) Memastikan bahwa tidak terjadi penyalinan data yang sensitif pada lingkungan pengujian sistem.

c. Pengawasan Penggunaan Sistem Informasi

- 1) Menentukan tingkat pengawasan yang diperlukan untuk setiap fasilitas pengolahan informasi yang digunakan oleh setiap individu dan memastikan bahwa setiap aktivitas pengawasan yang dilakukan telah sesuai dengan persyaratan hukum yang berlaku;
- 2) Membuat audit log yang meliputi hal-hal berikut:
 - a) Rekaman user ID, identitas terminal dan lokasi jika memungkinkan, serta alamat dan protokol jaringan;
 - b) Rekaman tanggal dan waktu log-on atau log-off, baik yang sukses maupun ditolak;
 - c) Rekaman daftar percobaan akses ke data atau perangkat sistem informasi yang sukses atau ditolak;
 - d) Rekaman perubahan pada konfigurasi sistem;
 - e) Catatan penggunaan secara istimewa/khusus termasuk penggunaan sistem utilitas dan aplikasi;
 - f) Catatan pengaktifan dan pe-non-aktifan sistem perlindungan;
 - g) Informasi tentang gagal atau suksesnya suatu peristiwa/kondisi yang dilakukan oleh administrator dan operator sistem informasi.
- 3) Proses pengelolaan log harus melakukan dan mempertimbangkan hal-hal berikut:
 - a) Menghindari perubahan pada tipe pesan yang dicatat;
 - b) Menghindari pengeditan atau penghapusan pada berbagai log;
 - c) Menghindari kelebihan kapasitas penyimpanan untuk log file yang dapat menyebabkan kegagalan pada pencatatan peristiwa atau kelebihan penulisan pada catatan peristiwa;
 - d) Melakukan pengarsipan untuk beberapa audit log sebagai bagian dari keperluan pengumpulan bukti.
- 4) Memperhatikan dan mengawasi hal-hal berikut:
 - a) Setiap jenis akses yang dibolehkan, termasuk user ID, tanggal dan waktu peristiwa yang penting, jenis-jenis peristiwa, file yang dapat diakses, program yang digunakan;
 - b) Seluruh aktivitas yang bersifat khusus, seperti penggunaan akun khusus,

memulai atau mematikan sistem, dan pemasangan atau pencabutan alat masukan dan keluaran;

- c) Setiap jenis akses yang tidak diperbolehkan, seperti tindakan user yang gagal atau ditolak, tindakan yang gagal atau ditolak dan berkaitan dengan data/sumber daya lain, pelanggaran kebijakan akses, notifikasi untuk gateway dan firewall;
 - d) Penyelesaian kesalahan yang terjadi dengan tindakan perbaikan yang telah disetujui dan memastikan tidak terjadi penyalahgunaan atau pelanggaran pengendalian pada saat tindakan perbaikan dilaksanakan.
- 5) Untuk menjamin ketepatan pencatatan pengawasan penggunaan sistem informasi, harus dipastikan bahwa setiap pengguna komputer atau media komunikasi lain telah melakukan penyesuaian terhadap standar waktu yang berlaku, baik untuk waktu lokal maupun waktu internasional dan melakukan pemeriksaan/perbaikan pada perbedaan waktu.

d. Manajemen back-up

Untuk memelihara integritas dan ketersediaan informasi dapat membuat cadangan (back-up) penyedia informasi dan fasilitas pemrosesan informasi. Manajemen back-up meliputi hal-hal sebagai berikut:

- 1) Manajemen back-up untuk sistem yang kritis bagi tujuan Pemerintah Kota Semarang harus meliputi seluruh sistem informasi, aplikasi, dan data yang penting sehingga bisa mendapatkan hasil pemulihan yang lengkap jika terjadi bencana;
- 2) Memastikan bahwa cakupan dan frekuensi back-up yang dilakukan telah mewakili persyaratan operasional, persyaratan keamanan informasi terkait, dan tingkat risiko tinggi untuk keberlangsungan operasional Pemerintah Kota Semarang.
- 3) Menyediakan fasilitas back-up yang memadai untuk menjamin bahwa seluruh informasi dan aplikasi dapat kembali lagi jika terjadi bencana atau kegagalan fungsi. Rekaman back-up harus lengkap dan akurat untuk setiap salinan back-up.
- 4) Menyimpan hasil back-up di lokasi yang jauh, sesuai dengan jarak yang cukup aman untuk menghindari kerusakan jika terjadi bencana di lingkungan Pemerintah Kota Semarang. Selain itu Pemerintah Kota Semarang harus memberikan perlindungan fisik dan menyediakan lingkungan yang memadai untuk back-up informasi sesuai dengan standar;

- 5) Melakukan pemeriksaan terhadap media back-up untuk menjamin bahwa media back-up bisa dimanfaatkan dalam keadaan darurat. Ketika kerahasiaan menjadi sangat penting, perlu membuat perlindungan backup dengan menggunakan metode enkripsi;
- 6) Melakukan pemeriksaan dan pengujian secara rutin terhadap pedoman penyimpanan untuk menjamin bahwa pedoman tersebut efektif dan bisa dilengkapi sesuai dengan waktu yang dinyatakan dalam pedoman operasional pemulihan.

e. Pengelolaan Keamanan Jaringan

- 1) Menjamin adanya perlindungan atas jaringan komunikasi informasi dan perlindungan atas infrastruktur pendukungnya serta tersedianya fasilitas jaringan komunikasi cadangan;
- 2) Memisahkan antara pelaksana operasional jaringan dengan pelaksana operasional komputer;
- 3) Melakukan pengendalian khusus untuk menjamin keamanan atas kerahasiaan dan integritas data yang melalui wilayah jaringan publik atau jaringan nirkabel, dan untuk melindungi sistem dan aplikasi yang online;
- 4) Melakukan pengendalian khusus untuk memelihara ketersediaan layanan jaringan dan sambungan komputer;
- 5) Memastikan bahwa penyedia jasa layanan jaringan memiliki kemampuan untuk mengatur layanan sesuai yang telah disepakati secara aman dan dilakukan pengawasan secara rutin;
- 6) Memastikan bahwa penyedia jasa layanan jaringan telah melaksanakan aturan keamanan jaringan dengan memperhatikan keistimewaan keamanan dan tingkat pelayanan yang diberikan, dan sesuai dengan persyaratan Pemerintah Kota Semarang;
- 7) Memperhatikan persyaratan keamanan dalam pengelolaan penyedia jasa jaringan sebagai berikut:
 - a) Tersedianya teknologi yang digunakan untuk keamanan layanan jaringan, seperti otentikasi, enkripsi, dan pengendalian sambungan jaringan;
 - b) Tersedianya batasan teknis yang diperlukan untuk sambungan yang aman dengan layanan jasa jaringan yang sesuai dengan peraturan keamanan dan sambungan jaringan;
 - c) Tersedianya pedoman yang digunakan untuk penggunaan layanan jasa jaringan dalam membatasi akses ke jaringan atau aplikasi.

f. Pengelolaan Layanan Jasa Pihak Ketiga

- 1) Menjamin pelaksanaan layanan dari pihak ketiga yang terkait dengan operasional sistem informasi dan komunikasi telah mempertimbangkan aspek keamanan informasi serta telah diawasi secara memadai dan berbagai perubahan telah memperoleh persetujuan yang memadai;
- 2) Memastikan bahwa perjanjian yang dilakukan dengan pihak ketiga yang memberikan layanan jasa harus meliputi persetujuan untuk melaksanakan keamanan, mendefinisikan bentuk jasa yang diberikan, dan aspek-aspek manajemen jasa yang diberikan;
- 3) Untuk kondisi outsourcing, harus dipastikan rencana transisi informasi dan fasilitas pengolahnya untuk menjamin bahwa keamanan telah dilaksanakan dan dipelihara selama masa transisi;
- 4) Melakukan pengawasan terhadap kinerja layanan jasa yang diberikan oleh pihak ketiga untuk memastikan kesesuaiannya dengan perjanjian yang disepakati;
- 5) Melakukan reviu atas laporan layanan jasa yang dihasilkan oleh pihak ketiga dan mengatur rapat lanjutan untuk menindaklanjuti laporan tersebut sesuai dengan persyaratan dalam perjanjian;
- 6) Menyediakan informasi mengenai insiden keamanan informasi dan melakukan reviu atas informasi tersebut sesuai dengan persyaratan yang ada dalam perjanjian ataupun pedoman;
- 7) Melakukan reviu terhadap jejak audit pihak ketiga dan catatan insiden keamanan, permasalahan operasional, kegagalan, jejak kesalahan, dan gangguan yang berkaitan dengan layanan jasa pihak ketiga, dan menyelesaikan serta mengatur masalah-masalah yang telah teridentifikasi dari hasil tinjauan tersebut.
- 8) Menetapkan pedoman perubahan pada layanan jasa pihak ketiga, yang meliputi:
 - a) Peningkatan terhadap layanan jasa yang selama ini diberikan dan pengembangan terhadap setiap aplikasi dan sistem yang baru serta modifikasi dan pembaharuan terhadap kebijakan dan pedoman yang berlaku di Pemerintah Kota Semarang;
 - b) Perubahan dan peningkatan pada jaringan, penggunaan teknologi baru, dan pengadopsian produk baru atau versi terbaru dari produk yang sudah digunakan;
 - c) Lingkungan dan alat pengembangan yang baru, perubahan pada lokasi

fisik dari fasilitas layanan jasa, dan perubahan pada vendor;

- d) Pengendalian baru untuk mengatasi insiden keamanan informasi dan untuk memperbaiki keamanan informasi.

g. Perencanaan dan Perizinan Sistem

- 1) Memastikan bahwa persyaratan dan kriteria untuk perizinan terhadap sistem baru telah ditetapkan, disetujui, didokumentasikan, dan diujikan;
- 2) Menentukan persyaratan kinerja dan kapasitas untuk setiap komputer yang digunakan di lingkungan Pemerintah Kota Semarang;
- 3) Melakukan penyesuaian dan pengawasan terhadap sistem untuk memastikan ketersediaan dan keefektifitasan sistem tersebut;
- 4) Melakukan pendeteksian terhadap kendali untuk mengetahui masalah-masalah yang sedang terjadi;
- 5) Melakukan pengawasan terhadap sumber daya sistem dengan memperhatikan sumber daya yang memiliki konsumsi yang paling lama dan biaya paling tinggi;
- 6) Membuat mekanisme seperti dokumentasi untuk mengantisipasi ketergantungan terhadap personil kunci yang mungkin membawa ancaman bagi keamanan sistem atau layanan jasa;
- 7) Menyediakan solusi perbaikan untuk setiap kesalahan yang terjadi;
- 8) Memiliki jaminan bahwa instalasi sistem yang baru tidak akan mempengaruhi sistem yang telah ada. Jaminan ini dapat dilihat dari adanya bukti bahwa pengaruh yang ada pada sistem baru telah dipertimbangkan dan telah diamankan oleh penyedia (provider);
- 9) Menyediakan pedoman pengoperasian atau penggunaan sistem yang baru bagi seluruh pegawai Pemerintah Kota Semarang dalam rangka mengefektifkan pedoman teknis dan menghindari terjadinya human error.

h. Perlindungan Untuk *Malicious Code*

- 1) Melakukan perlindungan terhadap *malicious code* yang didasarkan pada pendeteksian awal, perbaikan software, kesadaran keamanan, dan pengendalian manajemen perubahan dan sistem akses yang memadai;
- 2) Melarang penggunaan software tidak direkomendasikan di lingkungan Pemerintah Kota Semarang dan melaksanakan pedoman untuk perlindungan terhadap ancaman ketika menerima file dan software dari jaringan eksternal atau dari perantara jaringan yang lain;
- 3) Melaksanakan reviu secara rutin terhadap software dan isi data dari sistem yang mendukung proses bisnis di Pemerintah Kota Semarang;

- 4) Melakukan penyelidikan terhadap adanya file yang tidak direkomendasikan dan perubahan ilegal terhadap file atau informasi;
- 5) Melakukan instalasi dan pembaharuan secara rutin terhadap pendeteksian malicious code dan perbaikan perangkat lunak untuk pemindaian (scanning) komputer atau media lain sebagai bentuk kendali pencegahan.
- 6) Menetapkan pedoman pengelolaan dan tanggung jawab untuk mencegah malicious code terhadap sistem yang berjalan, pelatihan yang diperlukan, pelaporan dan perbaikan dari serangan malicious code;
- 7) Menyiapkan *Business Continuity Plan* (BCP) yang memadai untuk *recovery* dari serangan *malicious code*, termasuk semua data penting dan aplikasi back-up serta aturan pemulihan;

i. Penanganan Media

- 1) Memastikan bahwa setiap media yang akan dipindah-tangankan dari Pemerintah Kota Semarang tidak boleh dimiliki khususnya terkait dengan sistem pemulihan isi media tersebut. Jika diperlukan, dilakukan otorisasi bagi media yang akan dipindahkan dari Pemerintah Kota Semarang dan rekaman pemindahannya harus disimpan untuk memelihara bukti audit.
- 2) Bagi informasi yang disimpan di media jika umur media tersebut lebih pendek dari umur kebutuhan informasi yang ada di dalamnya maka untuk menghindari kehilangan informasi akibat penurunan nilai media, harus dilakukan proses penyimpanan yang aman;
- 3) Melakukan pendaftaran untuk media yang bisa dipindah-tangankan untuk membatasi kemungkinan kehilangan data. Pemindahan media sedapat mungkin hanya boleh dilakukan jika terdapat alasan yang kuat untuk melakukannya;
- 4) Melakukan penyimpanan atau penghapusan media secara aman untuk media yang berisi informasi sensitif;
- 5) Melaksanakan pedoman untuk mengidentifikasi setiap jenis media yang membutuhkan penghapusan secara aman;
- 6) Melakukan pencatatan untuk penghapusan media yang bersifat sensitif untuk memelihara bukti audit.
- 7) Melakukan pemilihan secara selektif untuk penyedia jasa pengumpulan dan penghapusan kertas, peralatan, dan media. Pemilihan tersebut dengan mempertimbangkan pengendalian dan pengalaman yang cukup dari penyedia jasa tersebut;

- 8) Melakukan penanganan dan penamaan seluruh media yang bisa mengindikasikan level klasifikasi. Selain itu juga dilakukan proses penyimpanan untuk media yang sesuai dengan spesifikasi masing- masing;
- 9) Memastikan bahwa data yang diinput telah lengkap, proses yang dijalankan lengkap, dan pengesahan output telah dilaksanakan. Selain itu juga dipastikan perlindungan untuk data mentah yang memiliki nilai sensitifitas;
- 10) Memilih dan menggunakan penyedia jasa kurir atau jasa transportasi yang terpercaya, menetapkan daftar penyedia jasa kurir yang boleh digunakan, dan mengembangkan pedoman pemeriksaan untuk setiap penyedia jasa kurir atau jasa transport yang telah dipilih;
- 11) Melakukan proses pengepakan yang memadai untuk setiap media yang akan dikirim untuk melindungi isi dari kerusakan (suhu yang terlalu panas atau lembab, atau pengaruh elektromagnetik) selama dalam perjalanan;
- 12) Melindungi informasi yang sensitif dengan pengendalian tertentu untuk menghindari terjadinya modifikasi dan penyungkapan yang ilegal, misalnya penggunaan kontainer yang terkunci, pengiriman langsung, perusakan bukti pengepakan, dan pemisahan pengiriman dengan rute yang berbeda.

j. Pertukaran Informasi

- 1) Melaksanakan pedoman untuk melindungi pertukaran informasi dari penghapusan, penyalinan, modifikasi, kesalahan alamat, dan penghancuran;
- 2) Melindungi pertukaran informasi yang sensitif dalam bentuk attachment;
- 3) Membuat panduan untuk penggunaan informasi dan fasilitas pengolahnya bagi seluruh pengguna, termasuk juga panduan penggunaan alat komunikasi nirkabel yang memiliki risiko tinggi;
- 4) Memastikan tidak ada kolusi antara pegawai Pemerintah Kota Semarang, kontraktor, dan pengguna lainnya mengenai tanggungjawab mereka terhadap keamanan informasi;
- 5) Melaksanakan panduan untuk menyimpan atau menghapus semua bentuk korespondensi bisnis, termasuk pesan, yang berhubungan dengan hukum dan perundang-undangan lokal dan nasional;
- 6) Dilarang meninggalkan informasi yang bersifat sensitif dan kritis di mesin printer atau mesin penjawab telpon untuk menghindari akses oleh pihak yang tidak berwenang;
- 7) Melakukan pengendalian dan pembatasan akses untuk fasilitas komunikasi yang bisa di-*forward*, misalnya email yang di-*forward* ke alamat eksternal;
- 8) Melakukan tindakan pencegahan dalam berkomunikasi, misalnya jangan

- memberitahu informasi sensitif ketika berbicara ditelpon untuk menghindari bocornya informasi kepada orang disekitar atau orang yang menyadap;
- 9) Tidak boleh mendaftarkan akun email yang berisi informasi pribadi ke perangkat lunak lain yang tidak berkepentingan dengan Pemerintah Kota Semarang;
 - 10) Dalam rangka mengantisipasi terjadinya kesalahan, mesin faksimil dan foto copy yang digunakan harus memiliki media yang jika terjadi kesalahan maka pengiriman akan tetap dicetak;
 - 11) Mengumumkan pihak yang telah melakukan pengiriman dan penerimaan informasi dari dalam atau ke luar Pemerintah Kota Semarang.
 - 12) Menetapkan standar untuk teknik pengepakan dalam proses pengiriman informasi, menetapkan standar untuk identifikasi jasa kurir, serta memastikan tersedianya salinan perjanjian dan memastikan dapat dilakukannya pencarian jejak & pengakuan dari pertukaran informasi yang terjadi.

Pesan Elektronik dan Transaksi Elektronik

- 1) Melindungi informasi dalam bentuk pesan elektronik yang ada di Pemerintah Kota Semarang dari akses ilegal, modifikasi, atau layanan ilegal;
- 2) Memastikan tujuan dan transportasi yang benar untuk setiap pesan yang dikirim ataupun diterima Pemerintah Kota Semarang;
- 3) Memastikan reliabilitas dan ketersediaan secara umum untuk setiap pesan;
- 4) Memastikan keamanan pesan elektronik dengan menggunakan tanda tangan elektronik oleh setiap pihak yang terlibat dalam transaksi;
- 5) Memastikan komunikasi antara kedua belah pihak telah disandi dan protokol yang digunakan untuk berkomunikasi telah dilindungi;
- 6) Memastikan bahwa Pemerintah Kota Semarang telah mendapatkan jaminan keamanan yang terintegrasi ketika menggunakan jasa dari pihak-pihak berwenang.

Informasi Yang Tersedia Untuk Umum

- 1) Membentuk mekanisme perlindungan untuk perangkat lunak dan informasi yang dapat diakses oleh umum. Hal itu ditujukan untuk menjaga integritas perangkat lunak dan informasi tersebut;
- 2) Memeriksa akses sistem informasi bagi publik, untuk menghindari kelemahan dan kegagalan sebelum informasi disediakan. Pemilik informasi memberi persetujuan secara formal sebelum informasi disediakan untuk publik;

3) Melarang setiap pihak eksternal untuk melakukan akses ke dalam jaringan dan sistem informasi Pemerintah Kota Semarang jika ia tidak memiliki otorisasi.

m. Monitoring

- 1) Menjalankan monitoring sistem dan kejadian keamanan informasi. Hasil pemantauan tersebut harus terekam secara otomatis. Log operator termasuk administrator harus selalu dibuat dan log dari fault harus dijalankan;
- 2) Membuat dan menyimpan log atau audit-log yang paling sedikit memuat:
 - a) User ID;
 - b) Tanggal, bulan, tahun, waktu dari event utama, misalnya *log-on* dan *log-off*;
 - c) Identitas terminal, misalnya MAC atau IP dan letak;
 - d) Rekaman usaha akses sistem yang berhasil atau gagal;
 - e) Rekaman usaha akses data atau sumber daya yang berhasil dan gagal;
 - f) Perubahan konfigurasi sistem;
 - g) Pemakaian akses khusus seperti administrator atau super-user atau power-user;
 - h) Pemakaian aplikasi sistem dan utilitas sistem;
 - i) File yang diakses dan hak akses yang dipakai;
 - j) Alamat dan protokol jaringan;
 - k) Alarm yang dibangkitkan sistem pengendalian akses;
 - l) Aktivasi dan deaktivasi sistem proteksi, misalnya anti-virus atau firewall dan IDS/IPS;
- 3) Memonitor pemakaian/akses sistem yang meliputi:
 - a) Akses terotorisasi, termasuk rinciannya yang meliputi:
 - Nama user ID;
 - Waktu dan tanggal kejadian penting;
 - Jenis kejadian;
 - File-file yang diakses;
 - Aplikasi dan/atau utilitas yang dipergunakan.
 - b) Semua operasi admin (all privileged operations), seperti:
 - i. Pemakaian akun dengan privilege di atas user biasa, seperti supervisor, root, administrator;
 - ii. System start-up and stop;
 - iii. Pemasangan atau pelepasan I/O device (attachment / detachment).
 - c) Usaha akses yang gagal atau tidak terotorisasi seperti:

- i. Aksi user yang gagal atau ditolak;
- ii. Aksi gagal atau ditolak yang melibatkan data atau sumberdaya lain seperti I/O;
- iii. Pelanggaran dan peringatan kebijakan akses jaringan dan firewall;
- iv. Alarm dari IDS (intrusion detection systems).

d) Peringatan sistem atau sistem gagal (system alerts or failures)

seperti:

- i. Console alerts or messages;*
- ii. System log exceptions;*
- iii. Network management alarms;*
- iv. Alarms raised by the access control system;*
- v. Perubahan, atau usaha perubahan setting dan/atau kendali keamanan sistem.

- 4) Menentukan frekuensi reuiu monitoring berdasarkan hasil analisa risiko;
- 5) Memastikan fasilitas logging dan informasi log tidak dapat dirubah dan diakses oleh pihak yang tidak berhak;
- 6) Memastikan bahwa seluruh kegiatan administrator sistem dan operator sistem secara otomatis direkam log-nya;
- 7) Menjalankan sistem pencatatan fault yang meliputi pencatatan otomatis *fault*, analisa *fault* dan tindak lanjut *fault*;

13. Manajemen Insiden Keamanan Informasi

13.1 Ruang Lingkup dan Tujuan

Ruang lingkup manajemen insiden keamanan informasi adalah pengelolaan pelaporan insiden & penetapan penanggung jawab pelaporan insiden, penetapan pedoman pelaporan insiden, pengelolaan tindakan feedback dari proses pelaporan insiden dan pengelolaan tindakan pemulihan/recovery perbaikan sistem.

Tujuan manajemen insiden keamanan informasi adalah memberikan panduan pelaksanaan pengelolaan insiden keamanan informasi Kebijakan Pengamanan Operasional Sistem Informasi

13.2 Kebijakan Manajemen Insiden Keamanan Informasi

Insiden yang berkaitan dengan keamanan informasi adalah:

- a. Gangguan / kehilangan akses layanan, peralatan atau fasilitas sistem informasi;
- b. Sistem tidak berjalan, gagal, malfunction, atau overload;

- c. Perangkat keras dan perangkat lunak tidak berjalan, gagal, malfunction;
- d. Kegagalan sistem informasi termasuk layanan sistem informasi;
- e. Malicious code dan denial service;
- f. Kesalahan akibat dari ketidak-lengkapan/ketidak-akuratan data;
- g. Kesalahan manusia;
- h. Ketidak-patuhan dengan kebijakan atau pedoman;
- i. Pelanggaran terhadap pengaturan keamanan fisik sistem informasi;
- j. Perubahan sistem yang tidak terpantau;
- k. Pelanggaran atas penggunaan akses;
- l. Pelanggaran kerahasiaan dan integritas seluruh hal yang terkait dengan informasi;
- m. Penyalahgunaan sistem informasi Pemerintah Kota Semarang.

Kebijakan manajemen insiden keamanan informasi meliputi:

Melaporkan insiden-insiden yang berhubungan dengan keamanan informasi melalui pedoman yang telah ditetapkan sebelumnya baik yang berkaitan dengan teknologi informasi maupun yang berkaitan dengan fasilitas dan infrastruktur sesegera mungkin;

Menetapkan pegawai yang bertanggung-jawab terhadap pelaporan insiden yang berhubungan dengan keamanan informasi. Pegawai tersebut harus dapat dihubungi setiap saat, diketahui oleh seluruh pegawai dan organisasi Pemerintah Kota Semarang, dan mampu mengambil tindakan yang tepat, cepat, dan akurat;

Menetapkan pedoman pelaporan yang meliputi: (1) Analisis dan indentifikasi penyebab insiden; (2) Penahanan/isolasi (containment); (3) Perencanaan dan penerapan tindakan; (4) Pemulihan; (5) Pelaporan tindakan yang telah diambil.

Hal-hal sebagai berikut harus diperhatikan dalam proses penetapan pedoman laporan insiden keamanan informasi:

- (1) Setiap tindakan / umpan balik yang dilakukan harus direkam untuk mengetahui bahwa tindakan dilakukan dengan tepat dan cermat;
- (2) Rekaman tersebut harus disimpan dengan baik untuk pertimbangan lebih lanjut apabila terjadi kejadian yang sama maupun lainnya dimasa yang akan datang;
- (3) Tindakan pemulihan / perbaikan sistem harus dipantau secara resmi dan seluruh tindakan yang diambil harus didokumentasikan secara

- rinci;
- (4) Seluruh laporan atas tindakan pemulihan/perbaikan sistem harus dilaporkan dan direviu;
 - (5) Tidak dibenarkan mengambil tindakan penanggulangan sendiri tanpa sepengetahuan pihak yang berkompeten di Pemerintah Kota Semarang; Segera beritahukan pihak yang berwenang menanggulangi kejadian terkait keamanan informasi Pemerintah Kota Semarang;
 - (6) Seluruh pihak yang terkait dipastikan telah mengetahui tanggung jawabnya untuk melaporkan setiap kejadian yang dapat berdampak kepada sistem informasi Pemerintah Kota Semarang;
 - (7) Setiap pihak yang berhubungan dengan sistem informasi Pemerintah Kota Semarang harus menerapkan sikap kehati-hatian terhadap segala aspek yang harus dirahasiakan. Pelatihan untuk meningkatkan sikap tersebut dapat digunakan oleh Pemerintah Kota Semarang.

14. Manajemen Kontinuitas Operasi

14.1 Ruang Lingkup dan Tujuan

Ruang lingkup operasi dalam manajemen kontinuitas yaitu operasi proses bisnis yang dianggap kritis oleh Pemerintah Kota Semarang.

Tujuan manajemen kontinuitas operasi yaitu menangani terhentinya aktivitas bisnis dan menjaga proses bisnis kritis dari kegagalan sistem informasi atau bencana untuk memastikan keberjalanan kembali proses bisnis tepat pada waktunya.

14.2 Kebijakan Manajemen Kontinuitas Operasi

Dalam manajemen kontinuitas operasi harus dilakukan beberapa hal berikut. Penilaian risiko dalam kontinuitas operasi; Penilaian risiko antara lain harus melakukan beberapa hal berikut:

- 1) Menentukan kemungkinan ancaman dan dampak secara keseluruhan apabila terjadi gangguan baik dari aspek waktu, skala kerusakan, dan periode pemulihan;
 - 2) Mempertimbangkan untuk mengambil tindakan alternatif yang tepat apabila dianggap perlu, sebagai bagian dari manajemen risiko operasional.
- Penyusunan rencana kontinuitas operasi perbaikan operasi Pemerintah Kota Semarang ketika terjadi bencana, dalam perencanaan harus memperhatikan hal berikut;
- 1) Identifikasi seluruh kehilangan layanan dan informasi yang dapat diterima;
 - 2) Persiapan pedoman untuk memulihkan atau memperbaiki operasi

Pemerintah Kota Semarang dan ketersediaan informasi pada saat dibutuhkan.

Penyusunan organisasi pelaksana kontinuitas operasi;

Pengujian dan pemutakhiran (*updating*) rencana kontinuitas, pengujian yang harus dilakukan yaitu: 1) Simulasi; 2) Pengujian pemulihan teknis; 3)

Pengujian pemulihan di tempat pengganti;

15. Kepatuhan Keamanan Informasi

15.1 Ruang Lingkup dan Tujuan

Ruang lingkup kepatuhan keamanan informasi meliputi kepatuhan terhadap undang-undang, peraturan, kontrak dengan pihak luar, dan kebijakan keamanan informasi.

Tujuan kepatuhan keamanan informasi yaitu untuk menghindari pelanggaran terhadap undang-undang, peraturan, kontrak, dan kebijakan keamanan informasi yang telah ditetapkan Pemerintah Kota Semarang.

15.2 Kebijakan Kepatuhan Keamanan Informasi

Kebijakan kepatuhan keamanan informasi terdiri dari ketaatan kepada persyaratan hukum, perlindungan atas rekaman Pemerintah Kota Semarang, pencegahan atas penyalahgunaan fasilitas pemrosesan informasi, ketaatan kepada kebijakan, pedoman dan prosedur keamanan informasi.

Berikut kebijakan pada masing-masing bagian tersebut.

a. Ketaatan Hukum

Ketaatan hukum dilakukan dengan melakukan beberapa hal berikut.

- 1) Menggunakan produk dan piranti lunak yang legal;
- 2) Memperoleh piranti lunak dari sumber yang diketahui dan mempunyai reputasi yang baik sehingga tidak terjadi pelanggaran hak cipta;
- 3) Memelihara kesadaran atas perlindungan hak kekayaan intelektual dan memberikan peringatan kepada pegawai Pemerintah Kota Semarang yang melanggar hak kekayaan intelektual;
- 4) Memelihara bukti dan keterangan mengenai izin kepemilikan, master disk, buku petunjuk;
- 5) Memastikan hanya piranti lunak dan produk yang dipasang di sistem Pemerintah Kota Semarang telah mempunyai izin;
- 6) Membuat tata cara pemindahan piranti lunak kepada pihak lain;
- 7) Mempersiapkan dan menggunakan peralatan audit yang tepat;
- 8) Mematuhi syarat dan kondisi dari piranti lunak dan informasi yang diperoleh

dari jaringan publik;

- 9) Tidak menduplikasi, mengubah ke format yang lain atau menyadap rekaman komersial (film atau audio) tanpa mendapatkan izin dari pemilik hak cipta;
- 10) Tidak melakukan duplikasi sebagian atau keseluruhan dari buku, artikel, laporan, atau dokumen lainnya, tanpa mendapatkan izin dari pemilik hak cipta;

b. Perlindungan atas Rekaman Pemerintah Kota Semarang

Perlindungan atas rekaman Pemerintah Kota Semarang dilakukan dengan beberapa hal berikut;

- 1) Menyusun panduan penyimpanan, penempatan, penanganan, dan pemindahan rekaman;
- 2) Memastikan bahwa penyimpanan rekaman dikategorikan secara rinci termasuk jangka waktu dan media penyimpanan;
- 3) Menetapkan pedoman penggunaan media penyimpanan elektronik yang menjamin akses data (baik media maupun format) dalam periode tertentu untuk menghindari kehilangan yang diakibatkan perubahan teknologi;
- 4) Menetapkan pedoman penyimpanan dan penanganan media rekaman yang sesuai dengan rekomendasi pabrik. Apabila akan menyimpan rekaman dalam jangka waktu yang lama perlu mempertimbangkan penggunaan media-media khusus;
- 5) Memperhatikan degradasi kemampuan media penyimpanan rekaman;
- 6) Menghancurkan rekaman yang sudah tidak dibutuhkan lagi oleh Pemerintah Kota Semarang setelah periode penyimpanan berakhir;
- 7) Menerapkan pengendalian yang tepat untuk melindungi rekaman dari kehilangan, kerusakan, dan pemalsuan;
- 8) Memastikan bahwa setiap kunci kriptografi dan program yang berhubungan dengan kriptografi disimpan pada jangka waktu tertentu, sesuai dengan dokumen yang disandi sehingga dokumen tersebut dapat dibuka kembali;
- 9) Mengkomunikasikan kebijakan perlindungan dan kerahasiaan data pribadi kepada seluruh pegawai dan pihak yang terkait;
- 10) Menerapkan pengendalian yang tepat untuk memastikan seluruh kebijakan, perundang-undangan, dan peraturan yang terkait dengan perlindungan data pribadi.

c. Pencegahan atas Penyalahgunaan Fasilitas Pemrosesan Informasi

Pencegahan atas penyalahgunaan fasilitas pemrosesan informasi dilakukan

dengan beberapa hal berikut.

- 1) Memastikan seluruh pegawai Pemerintah Kota Semarang memahami bahwa setiap penggunaan fasilitas pemrosesan informasi harus melalui persetujuan pihak yang menjadi pemilik aset informasi tersebut;
- 2) Memastikan tidak ada penggunaan fasilitas diluar kepentingan kegiatan Pemerintah Kota Semarang atau untuk tujuan yang tidak mempunyai otorisasi;
- 3) Memberikan tindakan tegas bagi pegawai yang menggunakan fasilitas atau otorisasi selain untuk kepentingan kegiatan Pemerintah Kota Semarang;
- 4) Memastikan seluruh pegawai memahami dan menyadari secara tepat mengenai batasan penggunaan akses yang diizinkan, salah satunya dengan pernyataan tertulis dari pegawai;
- 5) menampilkan pesan peringatan apabila pengguna melakukan akses yang tidak diizinkan;
- 6) Apabila Pemerintah Kota Semarang membutuhkan pemantauan informasi lintas negara, maka Pemerintah Kota Semarang harus memperhatikan aspek hukum negara tersebut. Pemerintah Kota Semarang dapat membuat perjanjian yang diperlukan untuk kepentingan tersebut.

d. Ketaatan Kepada Kebijakan, Standar, Pedoman dan Prosedur Keamanan Informasi

Pengendalian ketaatan kepada kebijakan, pedoman dan prosedur keamanan informasi dilakukan dengan beberapa hal berikut.

- 1) Mereviu secara berkala kepatuhan terhadap pedoman pemrosesan informasi kepada seluruh pihak yang bertanggung jawab. Apabila ada ketidak patuhan maka dilakukan hal berikut.
 - a) Menentukan menemukan penyebab ketidak-patuhan;
 - b) Menentukan dan menerapkan tindakan perbaikan yang tepat;
 - c) Mengevaluasi tindakan yang perlu diambil untuk memastikan tidak terjadi kembali ketidakpatuhan tersebut.
- 2) Menjaga rekaman hasil reviu ketidakpatuhan dan tindakan yang diambil;
- 3) Memastikan bahwa pemeriksaan kepatuhan keamanan informasi dilakukan oleh pegawai yang berpengalaman, kompeten, dan berwenang serta disupervisi oleh pihak yang berkompeten dan berwenang;
- 4) Memastikan akses data pada pemeriksaan hanya akses membaca (*read only*) dan hanya diperbolehkan untuk mendapatkan salinan yang terpisah dari

- sistem file dan salinan tersebut segera dihapus setelah selesai pemeriksaan;
- 5) Memastikan bahwa apabila terdapat kewajiban untuk menyimpan file yang diperiksa untuk kebutuhan dokumentasi pemeriksaan, maka harus dilakukan dengan perlindungan yang tepat;
 - 6) Memastikan seluruh akses yang dilakukan oleh pemeriksa dipantau dan direkam untuk kebutuhan referensi apabila diuji kembali (*reference trail*) dengan menggunakan referensi stempel waktu (*reference trail timestamp*) untuk data dan sistem yang kritis;
 - 7) Memastikan peralatan audit (seperti piranti lunak atau arsip data) harus dipisahkan dari peralatan pengembangan dan operasional dan tidak disimpan pada *tape library* dan area pengguna, kecuali memiliki tingkat perlindungan tambahan;
 - 8) Reviu konfigurasi jaringan, sistem operasi, aplikasi, desktop, dan komponen sistem lain terhadap standar;
 - 9) Jika pihak ketiga turut terlibat dalam pemeriksaan dan terdapat risiko penyalahgunaan peralatan audit atau informasi, maka pengendalian terhadap risiko dan dampaknya harus segera dilakukan (seperti; segera mengubah *password* yang diberikan kepada pihak ketiga tersebut).

WALIKOTA SEMARANG,

ttd

HENDRAR PRIHADI

Salinan sesuai dengan aslinya
KEPALA BAGIAN HUKUM
PADA SEKRETARIAT DAERAH KOTA SEMARANG



Drs. Satrio Imam Poetranto, M.Si
Pembina Tingkat I
NIP.196503111986021004