SALINAN

WALI KOTA SALATIGA
PROVINSI JAWA TENGAH

PERATURAN WALI KOTA SALATIGA
NOMOR 9 TAHUN 2023

TENTANG
SISTEM MANAJEMEN KEAMANAN INFORMASI
SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

DENGAN RAHMAT TUHAN YANG MAHA ESA

WALI KOTA SALATIGA,

Menimbang : a. bahwa penerapan sistem pemerintahan berbasis elektronik dapat mewujudkan tata kelola pemerintahan yang bersih, efektif, transparan, dan akuntabel serta pelayanan publik yang berkualitas dan terpercaya;
b. bahwa dalam rangka melindungi kerahasiaan, keutuhan dan ketersediaan aset informasi sistem pemerintahan berbasis elektronik di Lingkungan Pemerintah Kota Salatiga dari berbagai ancaman keamanan informasi, perlu dilakukan pengelolaan keamanan informasi;
c. bahwa berdasarkan pertimbangan sebagaimana dimaksud pada huruf a dan b, perlu menetapkan Peraturan Wali Kota tentang Sistem Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik;

Mengingat : 1. Undang-Undang Nomor 17 Tahun 1950 tentang Pembentukan Daerah-daerah Kota Kecil dalam Lingkungan Propinsi Jawa Timur, Jawa Tengah, dan Jawa Barat;
2. Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 244, Tambahan Lembaran Negara Republik Indonesia Nomor 5587), sebagaimana telah diubah beberapa kali terakhir dengan Undang-Undang Nomor 6 Tahun 2023 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 2 Tahun 2022 tentang Cipta Kerja Menjadi Undang-Undang (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 41, Tambahan Lembaran Negara Republik Indonesia Nomor 6856);
3. Peraturan Pemerintah Nomor 69 Tahun 1992 tentang Perubahan Batas Wilayah Kotamadya Daerah Tingkat II Salatiga dan Kabupaten Daerah Tingkat II Salatiga (Lembaran Negara Republik Indonesia Tahun 1992 Nomor 114, Tambahan Lembaran Negara Republik Indonesia Nomor 3500);

4. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
5. Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2021 Nomor 541);
6. Peraturan Wali Kota Salatiga Nomor 118 Tahun 2021 tentang Organisasi dan Tata Kerja Dinas Komunikasi dan Informatika (Berita Daerah Kota Salatiga Tahun 2021 Nomor 118);

MEMUTUSKAN:

Menetapkan : PERATURAN WALI KOTA TENTANG SISTEM MANAJEMEN KEAMANAN INFORMASI SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK.

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Wali Kota ini yang dimaksud dengan:
1. Daerah adalah Kota Salatiga.
2. Pemerintah Daerah adalah Wali Kota sebagai unsur penyelenggara Pemerintahan Daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan daerah otonom.
3. Wali Kota adalah Wali Kota Salatiga.
4. Sekretaris Daerah adalah Sekretaris Daerah Kota Salatiga.
5. Perangkat Daerah adalah unsur pembantu Wali Kota dan DPRD dalam penyelenggaraan urusan pemerintahan yang menjadi kewenangan Daerah.
6. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada pengguna SPBE.
7. Keamanan SPBE adalah pengendalian keamanan yang terpadu dalam SPBE.
8. Manajemen Keamanan SPBE adalah serangkaian proses untuk mencapai penerapan keamanan SPBE yang efektif, efisien dan berkesinambungan serta mendukung layanan SPBE yang berkualitas.
9. Sistem Manajemen Keamanan Informasi yang selanjutnya disingkat SMKI adalah pengaturan kewajiban bagi penyelenggara sistem elekronik dalam penerapan manajemen pengamanan informasi berdasarkan asas risiko.
10. Data adalah catatan atas kumpulan fakta.
11. Informasi adalah sekumpulan data/ fakta yang diolah dengan cara tertentu sehingga mempunyai arti bagi penerima/ pengguna.
12. Aplikasi SPBE adalah satu atau sekumpulkan program komputer dan prosedur yang dirancang untuk melakukan tugas atau fungsi layanan SPBE.
13. Jaringan Intra adalah jaringan tertutup yang menghubungkan antar simpul jaringan dalam suatu organisasi.
14. Sistem Penghubung Layanan adalah perangkat integrasi/penghubung untuk melakukan pertukaran Layanan SPBE.
15. Infrastruktur SPBE adalah semua perangkat keras, perangkat lunak, dan fasilitas yang menjadi penunjang utama untuk menjalankan sistem, aplikasi, komunikasi data pengolahan dan penyimpanan data, perangkat integrasi/ penghubung dan perangkat elektronik.

16. *Application Programming Interface* yang selanjutnya disingkat API adalah sekumpulan perintah, fungsi, serta protokol yang mengintegrasikan dua bagian dari aplikasi atau dengan aplikasi yang berbeda secara bersamaan.
17. Pusat Data adalah fasilitas yang digunakan untuk menempatkan sistem elektronik dan komponen terkait lainnya untuk keperluaan penempatan, penyimpanan dan pengolahan data dan pemulihan data.

Pasal 2

(1) Peraturan Wali Kota ini dimaksudkan untuk memberikan kepastian hukum pelaksanaan SMKI SPBE.
(2) Pengaturan SMKI SPBE bertujuan untuk memastikan terjaganya kerahasiaan (*confidentiality*), keutuhan (*integrity*), ketersediaan (*availability*) dan nir penyangkalan (*non repudiation*) Data dan Informasi SPBE.

BAB II
SMKI SPBE

Bagian Kesatu
Umum

Pasal 3

SMKI SPBE dilaksanakan dengan Manajemen Keamanan SPBE, yang meliputi:
a. ruang lingkup;
b. penanggung jawab;
c. perencanaan;
d. dukungan pengoperasian;
e. evaluasi kinerja; dan
f. perbaikan berkelanjutan.

Bagian Kedua
Ruang Lingkup

Pasal 4

Ruang lingkup Manajemen Kemamanan SPBE sebagaimana dimaksud dalam Pasal 3 huruf a, meliputi:
a. Data dan Informasi SPBE;
b. Aplikasi SPBE;
c. aset Infrastruktur SPBE; dan
d. kebijakan keamanan informasi SPBE yang telah dimiliki.

Bagian Ketiga
Penanggung Jawab

Pasal 5

(1) Penanggung jawab Keamanan SPBE sebagaimana dimaksud dalam Pasal 3 huruf a adalah Sekretaris Daerah selaku koordinator SPBE.
(2) Dalam melaksanakan tugas sebagai penanggung jawab Keamanan SPBE sebagaimana dimaksud pada ayat (1), koordinator SPBE menetapkan pelaksana teknis Keamanan SPBE.
(3) Pelaksana teknis Keamanan SPBE sebagaimana dimaksud pada ayat (2) terdiri atas:
    a. pejabat pimpinan tinggi pratama Perangkat Daerah yang melaksanakan tugas dan fungsi di bidang keamanan teknologi, informasi dan komunikasi; dan
    b. pejabat pimpinan tinggi atau pejabat administrator Perangkat Daerah yang membawahi, membangun, memelihara, dan/atau mengembangkan Aplikasi SPBE.

(4) Pejabat pimpinan tinggi pratama sebagaimana dimaksud pada ayat (3) huruf a bertugas:
   a. memastikan penerapan standar teknis dan prosedur Keamanan SPBE;
   b. merumuskan, mengoordinasikan, dan melaksanakan program kerja dan anggaran Keamanan SPBE; dan
   c. melaporkan pelaksanaan manajemen keamanan informasi SPBE dan penerapan standar teknis dan prosedur Keamanan SPBE kepada koordinator SPBE.
(5) Pejabat pimpinan tinggi atau pejabat administrator sebagaimana dimaksud pada ayat (3) huruf b bertugas:
   a. menerapkan standar teknis dan prosedur keamanan Aplikasi SPBE di unit kerja masing-masing;
   b. memastikan seluruh pembangunan atau pengembangan Aplikasi dan Infrastruktur SPBE yang dilakukan oleh pihak ketiga memenuhi standar teknis dan prosedur Keamanan SPBE yang telah ditetapkan;
   c. memastikan keberlangsungan proses bisnis SPBE; dan
   d. berkoordinasi dengan pejabat pimpinan tinggi pratama yang melaksanakan tugas dan fungsi di bidang keamanan teknologi, informasi dan komunikasi terkait perumusan program kerja dan anggaran Keamanan SPBE.

Bagian Keempat
Perencanaan

Pasal 6

(1) Perencanaan sebagaimana dimaksud dalam Pasal 3 huruf c dilakukan oleh pelaksana teknis Keamanan SPBE.
(2) Perencanaan sebagaimana dimaksud pada ayat (1) dilakukan dengan merumuskan:
   a. program kerja Keamanan SPBE yang disusun berdasarkan kategori risiko Keamanan SPBE; dan
   b. target realisasi program kerja Keamanan SPBE.
(3) Program kerja SMKI sebagaimana dimaksud pada ayat (2) huruf a paling sedikit meliputi:
   a. edukasi kesadaran Keamanan SPBE;
   b. penilaian kerentanan Keamanan SPBE;
   c. peningkatan Keamanan SPBE;
   d. penanganan insiden Keamanan SPBE; dan
   e. audit Keamanan SPBE.
(4) Kategori risiko Keamanan SPBE sebagaimana dimaksud pada ayat (2) huruf a ditentukan sesuai ketentuan peraturan perundang-undangan.
(5) Target realisasi program kerja Keamanan SPBE sebagaimana dimaksud pada ayat (2) huruf b ditetapkan berdasarkan kebutuhan setiap Instansi Pusat dan Pemerintah Daerah.

Pasal 7

Edukasi kesadaran Keamanan SPBE sebagaimana dimaksud dalam Pasal 6 ayat (3) huruf a dilaksanakan paling sedikit melalui kegiatan:
a. sosialisasi; dan
b. pelatihan.

Pasal 8

Penilaian kerentanan Keamanan SPBE sebagaimana dimaksud dalam Pasal 6 ayat (3) huruf b dilaksanakan paling sedikit melalui:
a. menginventarisasi seluruh aset SPBE meliputi data dan informasi, aplikasi dan infrastruktur;
b. mengidentifikasi kerentanan dan ancaman terhadap aset SPBE; dan
c. mengukur tingkat risiko Keamanan SPBE.

Pasal 9

(1) Peningkatan Keamanan SPBE sebagaimana dimaksud dalam Pasal 6 ayat (3) huruf c dilaksanakan berdasarkan hasil penilaian kerentanan Keamanan SPBE sebagaimana dimaksud dalam Pasal 8.

(2) Peningkatan Keamanan SPBE dilaksanakan paling sedikit melalui:
   a. menerapkan standar teknis dan prosedur Keamanan SPBE; dan
   b. menguji fungsi keamanan terhadap data dan informasi, aplikasi dan infrastruktur SPBE.

Pasal 10

(1) Penanganan insiden Keamanan SPBE sebagaimana dimaksud dalam Pasal 6 ayat (3) huruf d dilaksanakan paling sedikit melalui:
   a. mengidentifikasi sumber serangan;
   b. menganalisis informasi yang berkaitan dengan insiden selanjutnya;
   c. memprioritaskan penanganan insiden berdasarkan tingkat dampak yang terjadi;
   d. mendokumentasi bukti insiden yang terjadi; dan
   e. memitigasi atau mengurangi dampak risiko Keamanan SPBE.
(2) Penanganan insiden Keamanan SPBE sebagaimana dimaksud pada ayat (1), dilaksanakan oleh tim koordinasi tanggap insiden keamanan siber yang ditetapkan dengan Keputusan Wali Kota.

Pasal 11

Audit Keamanan SPBE sebagaimana dimaksud dalam Pasal 6 ayat (3) huruf e dilakukan sesuai dengan ketentuan peraturan perundang-undangan.

Bagian Kelima
Dukungan Pengoperasian

Pasal 12

(1) Dukungan pengoperasian sebagaimana dimaksud dalam Pasal 3 ayat (1) huruf d dilakukan oleh koordinator SPBE.
(2) Dukungan pengoperasian sebagaimana dimaksud pada ayat (1) dilakukan dengan meningkatkan kapasitas terhadap:
   a. sumber daya manusia Keamanan SPBE; dan
   b. anggaran Keamanan SPBE.
(3) Sumber daya manusia Keamanan SPBE sebagaimana dimaksud pada ayat (2) huruf a paling sedikit harus memiliki kompetensi:
   a. keamanan data dan informasi;
   b. keamanan aplikasi; dan
   c. keamanan infrastruktur.
(4) Untuk memenuhi kompetensi sebagaimana dimaksud pada ayat (3) paling sedikit melakukan kegiatan:
   a. pelatihan dan/ atau sertifikasi kompetensi keamanan data dan informasi, aplikasi dan infrastruktur; dan
   b. bimbingan teknis mengenai standar Keamanan SPBE.
(5) Anggaran Keamanan SPBE sebagaimana dimaksud pada ayat (2) huruf b disusun berdasarkan perencanaan yang telah ditetapkan sesuai dengan ketentuan peraturan perundang-undangan.

Bagian Keenam
Evaluasi Kinerja

Pasal 13

(1) Evaluasi kinerja sebagaimana dimaksud dalam Pasal 3 ayat (1) huruf e dilakukan oleh Koordinator SPBE.
(2) Evaluasi kinerja sebagaimana dimaksud pada ayat (1) dilakukan terhadap pelaksanaan SMKI SPBE.
(3) Evaluasi kinerja sebagaimana dimaksud pada ayat (2) dilaksanakan dengan:
    a. mengidentifikasi area proses yang memiliki risiko tinggi terhadap keberhasilan pelaksanaan SMKI SPBE;
    b. menetapkan indikator kinerja pada setiap area proses;
    c. memformulasi pelaksanaan SMKI SPBE dengan mengukur secara kuantitatif kinerja yang diharapkan;
    d. menganalisis efektivitas pelaksanaan SMKI SPBE; dan
    e. mendukung dan merealisasikan program audit SMKI SPBE.
(4) Evaluasi kinerja sebagaimana dimaksud pada ayat (1) dilaksanakan paling sedikit 1 (satu) kali dalam 1 (satu) tahun.

Bagian Ketujuh
Perbaikan Berkelanjutan

Pasal 14

(1) Perbaikan berkelanjutan sebagaimana dimaksud dalam Pasal 3 ayat (1) huruf f dilakukan oleh pelaksana teknis Keamanan SPBE.
(2) Perbaikan berkelanjutan sebagaimana dimaksud pada ayat (1) merupakan tindak lanjut dari hasil evaluasi kinerja.
(3) Perbaikan berkelanjutan sebagaimana dimaksud pada ayat (1) dilakukan dengan:
    a. mengatasi permasalahan dalam pelaksanaan SMKI SPBE; dan
    b. memperbaiki pelaksanaan SMKI SPBE secara periodik.

BAB III
STANDAR TEKNIS DAN PROSEDUR SMKI SPBE

Bagian Kesatu
Umum

Pasal 15

(1) SMKI SPBE dilaksanakan dengan memenuhi standar teknis dan prosedur Keamanan SPBE.
(2) Standar teknis dan prosedur Keamanan SPBE sebagaimana dimaksud dalam pada ayat (1) diterapkan untuk:
    a. keamanan Data dan Informasi;
    b. keamanan Aplikasi;
    c. keamanan Sistem Penghubung Layanan;
    d. keamanan Jaringan Intra; dan
    e. keamanan Pusat Data.

Bagian Kedua
Keamanan Data dan Informasi

Pasal 16

Standar teknis keamanan Data dan Informasi sebagaimana dimaksud dalam Pasal 15 ayat (2) huruf a terdiri atas terpenuhinya aspek:
a. kerahasiaan;
b. keaslian;
c. keutuhan;
d. kenirsangkalan; dan

e. ketersediaan.

Pasal 17

Aspek kerahasiaan sebagaimana dimaksud dalam Pasal 16 huruf a dilakukan dengan prosedur:
a. menetapkan klasifikasi informasi;
b. menerapkan enkripsi dengan sistem kriptografi; dan
c. menerapkan pembatasan akses terhadap data dan informasi sesuai dengan kewenangan dan kebijakan yang telah ditetapkan.

Pasal 18

Aspek keaslian sebagaimana dimaksud dalam Pasal 16 huruf b dilakukan dengan prosedur:
a. menyediakan mekanisme verifikasi;
b. menyediakan mekanisme validasi; dan
c. menerapkan sistem *hash function*.

Pasal 19

Aspek keutuhan sebagaimana dimaksud dalam Pasal 16 huruf c dilakukan dengan prosedur:
a. menerapkan pendeteksian modifikasi; dan
b. menerapkan tanda tangan elektronik tersertifikasi.

Pasal 20

Aspek kenirsangkalan sebagaimana dimaksud dalam Pasal 16 huruf d dilakukan dengan prosedur:
a. menerapkan tanda tangan elektronik tersertifikasi; dan
b. penjaminan oleh penyelenggara sertifikasi elektronik melalui sertifikat elektronik.

Pasal 21

Aspek ketersediaan sebagaimana dimaksud dalam Pasal 16 huruf e dilakukan dengan prosedur:
a. menerapkan sistem pencadangan secara berkala;
b. membuat perencanaan untuk menjamin data dan informasi dapat selalu diakses; dan
c. menerapkan sistem pemulihan.

Bagian Ketiga
Keamanan Aplikasi

Pasal 22

(1) Standar teknis dan prosedur keamanan Aplikasi sebagaimana dimaksud dalam Pasal 15 ayat (2) huruf b diterapkan pada:
    a. aplikasi berbasis *website*;
    b. aplikasi berbasis *mobile*; dan
    c. aplikasi berbasis *desktop*.
(2) Aplikasi berbasis *website* sebagaimana dimaksud pada ayat (1) huruf a merupakan aplikasi yang diakses melalui peramban saat terhubung dengan koneksi internet atau intranet.
(3) Aplikasi berbasis *mobile* sebagaimana dimaksud pada ayat (1) huruf b merupakan aplikasi yang dalam pengoperasiannya dapat berjalan di perangkat dan memiliki sistem operasi yang mendukung perangkat lunak secara *standalone*.
(4) Aplikasi berbasis *desktop* sebagaimana dimaksud pada ayat (1) huruf b merupakan aplikasi yang dijalankan pada masing-masing komputer tanpa terhubung dengan koneksi internet.

(5) Aplikasi sebagaimana dimaksud pada ayat (1) harus dilakukan pengujian keamanan setiap periode tertentu dengan:
   a. mengidentifikasi persyaratan minimum keamanan yang belum diterapkan;
   b. memastikan pengkodean pemrograman aplikasi yang dibuat tidak memiliki kerawanan;
   c. melakukan pemindaian otomatis dan/ atau pengujian penetrasi sistem;
   d. mengidentifikasi kerentanan dan mengelola ancaman sejak awal siklus pengembangan aplikasi; dan
   e. menganalisis kerentanan.

Pasal 23

Standar teknis keamanan Aplikasi sebagaimana dimaksud dalam Pasal 22 ayat (1) terdiri atas terpenuhinya fungsi:
a. autentikasi;
b. manajemen sesi;
c. persyaratan kontrol akses;
d. validasi *input*;
e. kriptografi pada verifikasi statis;
f. penanganan eror dan pencatatan log;
g. proteksi data;
h. keamanan komunikasi;
i. kualitas kode dan pengaturan *build*;
j. pengendalian kode berbahaya;
k. logika bisnis;
l. *file*;
m. keamanan API dan *web service*;
n. keamanan konfigurasi;
o. penyimpanan data dan persyaratan privasi;
p. komunikasi jaringan;
q. interaksi *platform*; dan
r. ketahanan.

Pasal 24

Fungsi autentikasi sebagaimana dimaksud dalam Pasal 23 huruf a dilakukan dengan prosedur:
a. menggunakan manajemen kata sandi untuk proses autentikasi;
b. menerapkan verifikasi kata sandi pada sisi server;
c. mengatur jumlah karakter, kombinasi jenis karakter, dan masa berlaku dari kata sandi;
d. mengatur jumlah maksimum kesalahan dalam pemasukan kata sandi;
e. mengatur mekanisme pemulihan kata sandi;
f. menjaga kerahasiaan kata sandi yang disimpan melalui mekanisme kriptografi; dan
g. menggunakan jalur komunikasi yang diamankan untuk proses autentikasi.

Pasal 25

Fungsi manajemen sesi sebagaimana dimaksud dalam Pasal 23 huruf b dilakukan dengan prosedur:
a. menggunakan pengendali sesi untuk proses manajemen sesi;
b. menggunakan pengendali sesi yang disediakan oleh kerangka kerja aplikasi;
c. mengatur pembuatan dan keacakan token sesi yang dihasilkan oleh pengendali sesi;
d. mengatur kondisi dan jangka waktu habis sesi;
e. validasi dan pencantuman session id;
f. perlindungan terhadap lokasi dan pengiriman token untuk sesi terautentikasi; dan
g. perlindungan terhadap duplikasi dan mekanisme persetujuan pengguna.

Pasal 26

Fungsi persyaratan kontrol akses sebagaimana dimaksud dalam Pasal 23 huruf c dilakukan dengan prosedur:

a. menetapkan otorisasi pengguna untuk membatasi kontrol akses;
b. mengatur peringatan terhadap bahaya serangan otomatis apabila terjadi akses yang bersamaan atau akses yang terus-menerus pada fungsi;
c. mengatur antarmuka pada sisi *administrator*; dan
d. mengatur verifikasi kebenaran token ketika mengakses data dan informasi yang dikecualikan.

Pasal 27

Fungsi validasi *input* sebagaimana dimaksud dalam Pasal 23 huruf d dilakukan dengan prosedur:

a. menerapkan fungsi validasi *input* pada sisi server;
b. menerapkan mekanisme penolakan *input* jika terjadi kesalahan validasi;
c. memastikan *runtime environment* aplikasi tidak rentan terhadap serangan validasi *input*;
d. melakukan validasi positif pada seluruh *input*;
e. melakukan filter terhadap data yang tidak dipercaya;
f. menggunakan fitur kode dinamis;
g. melakukan perlindungan terhadap akses yang mengandung konten skrip; dan
h. melakukan perlindungan dari serangan injeksi basis data.

Pasal 28

Fungsi kriptografi pada verifikasi statis sebagaimana dimaksud dalam Pasal 23 huruf e dilakukan dengan prosedur:

a. menggunakan algoritma kriptografi, modul kriptografi, protokol kriptografi, dan kunci kriptografi sesuai dengan ketentuan peraturan perundang-undangan;
b. melakukan autentikasi data yang dienkripsi;
c. menerapkan manajemen kunci kriptografi; dan
d. membuat angka acak yang menggunakan generator angka acak kriptografi.

Pasal 29

Fungsi penanganan eror dan pencatatan *log* sebagaimana dimaksud dalam Pasal 23 huruf f dilakukan dengan prosedur:

a. mengatur konten pesan yang ditampilkan ketika terjadi kesalahan;
b. menggunakan metode penanganan eror untuk mencegah kesalahan terprediksi dan tidak terduga serta menangani seluruh pengecualian yang tidak ditangani;
c. tidak mencantumkan informasi yang dikecualikan dalam pencatatan *log*;
d. mengatur cakupan *log* yang dicatat untuk mendukung upaya penyelidikan ketika terjadi insiden;
e. mengatur perlindungan *log* aplikasi dari akses dan modifikasi yang tidak sah;
f. melakukan enkripsi pada data yang disimpan untuk mencegah injeksi *log*; dan
g. melakukan sinkronisasi sumber waktu sesuai dengan zona waktu dan waktu yang benar.

Pasal 30

Fungsi proteksi data sebagaimana dimaksud dalam Pasal 23 huruf g dilakukan dengan prosedur:

a. melakukan identifikasi dan penyimpanan salinan informasi yang dikecualikan;
b. melakukan perlindungan dari akses yang tidak sah terhadap informasi yang dikecualikan yang disimpan sementara dalam aplikasi;

c. melakukan pertukaran, penghapusan, dan audit informasi yang dikecualikan;
d. melakukan penentuan jumlah parameter;
e. memastikan data disimpan dengan aman;
f. menentukan metode untuk menghapus dan mengekspor data sesuai permintaan pengguna; dan
g. membersihkan memori setelah tidak diperlukan.

Pasal 31

Fungsi keamanan komunikasi sebagaimana dimaksud dalam Pasal 23 huruf h dilakukan dengan prosedur:
a. menggunakan komunikasi terenkripsi;
b. mengatur koneksi masuk dan keluar yang aman dan terenkripsi dari sisi pengguna;
c. mengatur jenis algoritma yang digunakan dan alat pengujiannya; dan
d. mengatur aktivasi dan konfigurasi sertifikat elektronik yang diterbitkan oleh penyelenggara sertifikasi elektronik.

Pasal 32

Fungsi kualitas kode dan pengaturan *build* sebagaimana dimaksud dalam Pasal 23 huruf i dilakukan dengan prosedur:
a. menandatangani aplikasi dengan sertifikat yang valid;
b. memastikan aplikasi dalam mode rilis;
c. menghapus simbol *debugging* dari *native binary*;
d. menghapus kode *debugging* dan kode bantuan pengembang;
e. mengidentifikasi kelemahan seluruh komponen *third party*;
f. menentukan mekanisme penanganan eror;
g. mengelola memori secara aman; dan
h. mengaktifkan fitur keamanan yang tersedia.

Pasal 33

Fungsi pengendalian kode berbahaya sebagaimana dimaksud dalam Pasal 23 huruf j dilakukan dengan prosedur:
a. menggunakan analisis kode dalam kontrol kode berbahaya;
b. memastikan kode sumber aplikasi dan pustaka tidak mengandung kode berbahaya dan fungsionalitas lain yang tidak diinginkan;
c. mengatur izin terkait fitur atau sensor terkait privasi;
d. mengatur perlindungan integritas; dan
e. mengatur mekanisme fitur pembaruan.

Pasal 34

Fungsi logika bisnis sebagaimana dimaksud dalam Pasal 23 huruf k dilakukan dengan prosedur:
a. memproses alur logika bisnis dalam urutan langkah dan waktu yang realistis;
b. memastikan logika bisnis memiliki batasan dan validasi;
c. memonitor aktivitas yang tidak biasa;
d. membantu dalam kontrol anti otomatisasi; dan
e. memberikan peringatan ketika terjadi serangan otomatis atau aktivitas yang tidak biasa.

Pasal 35

Fungsi *file* sebagaimana dimaksud dalam Pasal 23 huruf l dilakukan dengan prosedur:
a. mengatur jumlah *file* untuk setiap pengguna dan *kuota* ukuran *file* yang diunggah;
b. melakukan validasi *file* sesuai dengan tipe konten yang diharapkan;
c. melakukan perlindungan terhadap metadata *input* dan metadata *file*;

d. melakukan pemindaian *file* yang diperoleh dari sumber yang tidak dipercaya; dan
e. melakukan konfigurasi server untuk mengunduh *file* sesuai ekstensi yang ditentukan.

Pasal 36

Fungsi keamanan API dan *web service* sebagaimana dimaksud dalam Pasal 23 huruf m dilakukan dengan prosedur:
a. melakukan konfigurasi layanan web;
b. memverifikasi *uniform resource identifier* API tidak menampilkan informasi yang berpotensi sebagai celah keamanan;
c. membuat keputusan otorisasi;
d. menampilkan metode Restful *hypertext transfer protocol* apabila *input* pengguna dinyatakan valid;
e. menggunakan validasi skema dan verifikasi sebelum menerima *input*;
f. menggunakan metode perlindungan layanan berbasis *web*; dan
g. menerapkan kontrol anti otomatisasi.

Pasal 37

Fungsi keamanan konfigurasi sebagaimana dimaksud dalam Pasal 23 huruf n dilakukan dengan prosedur:
a. mengkonfigurasi server sesuai rekomendasi server aplikasi dan kerangka kerja aplikasi yang digunakan;
b. mendokumentasi, menyalin konfigurasi, dan semua dependensi;
c. menghapus fitur, dokumentasi, sampel, dan konfigurasi yang tidak diperlukan;
d. memvalidasi integritas aset jika aset aplikasi diakses secara eksternal;
e. menggunakan respons aplikasi dan konten yang aman; dan
f. sistem dan atau aplikasi yang akan dijalankan di lingkungan produksi, setidaknya telah melewati pengujian keamanan.

Pasal 38

Fungsi penyimpanan data dan persyaratan privasi sebagaimana dimaksud dalam Pasal 23 huruf o dilakukan dengan prosedur:
a. menyimpan seluruh data dan informasi yang dikecualikan hanya dalam fasilitas penyimpanan kredensial sistem;
b. membatasi pertukaran data dan informasi yang dikecualikan dengan *third party*;
c. menonaktifkan *cache keyboard* pada saat memasukkan data dan informasi yang dikecualikan;
d. melindungi informasi yang dikecualikan saat terjadi *inter process communication*; dan
e. melindungi data dan informasi yang dikecualikan yang dimasukkan melalui antarmuka pengguna.

Pasal 39

Fungsi komunikasi jaringan sebagaimana dimaksud dalam Pasal 23 huruf p dilakukan dengan prosedur:
a. menerapkan *secure socket layer* atau *transport layer security* yang tidak *obsolet* secara konsisten; dan
b. memverifikasi sertifikat *remote endpoint*.

Pasal 40

Fungsi interaksi *platform* sebagaimana dimaksud dalam Pasal 23 huruf q dilakukan dengan prosedur:
a. memastikan aplikasi hanya meminta akses terhadap sumber daya yang diperlukan;

b. melakukan validasi terhadap seluruh *input* dari sumber eksternal dan pengguna;
c. menghindari pengiriman fungsionalitas sensitif melalui skema *custom uniform resource locator* dan fasilitas *inter process communication*;
d. menghindari penggunaan JavaScript dalam WebView;
e. menggunakan protokol *hypertext transfer protocol secure* pada WebView; dan
f. mengimplementasikan penggunaan serialisasi API yang aman.

Pasal 41

Fungsi ketahanan sebagaimana dimaksud dalam Pasal 23 huruf r dilakukan dengan prosedur:
a. mencegah aplikasi berjalan pada perangkat yang telah dilakukan modifikasi yang tidak sah;
b. mendeteksi dan merespons *debugger*;
c. mencegah *executable file* melakukan perubahan pada sumber daya perangkat;
d. mendeteksi dan merespons keberadaan perangkat *reverse engineering*;
e. mencegah aplikasi berjalan dalam *emulator*;
f. mendeteksi perubahan kode dan data di ruang memori;
g. menerapkan fungsi device binding dengan menggunakan properti unik pada perangkat;
h. melindungi seluruh *file* dan *library* pada aplikasi; dan
i. menerapkan metode *obfuscation*.

Bagian Keempat
Keamanan Sistem Penghubung Layanan

Pasal 42

Standar teknis keamanan Sistem Penghubung Layanan sebagaimana dimaksud dalam Pasal 15 ayat (2) huruf c terdiri atas terpenuhinya fungsi:
a. keamanan interoperabilitas data dan informasi;
b. kontrol sistem integrasi;
c. kontrol perangkat *integrator*;
d. keamanan API dan *Web Service*; dan
e. keamanan migrasi data.

Pasal 43

Fungsi keamanan interoperabilitas data dan informasi sebagaimana dimaksud dalam Pasal 42 huruf a dilakukan dengan prosedur:
a. menerapkan sistem tanda tangan elektronik tersertifikasi untuk pengamanan dokumen dan surat elektronik;
b. menerapkan sistem enkripsi data;
c. memastikan data dan informasi selalu dapat diakses sesuai otoritasnya; dan
d. menerapkan sistem hash function pada *file*.

Pasal 44

Fungsi kontrol sistem integrasi sebagaimana dimaksud dalam Pasal 42 huruf b dilakukan dengan prosedur:
a. menerapkan protokol *secure socket layer* atau protokol *transport layer security* versi terkini pada sesi pengiriman data dan informasi;
b. menerapkan *internet protocol security* untuk mengamankan transmisi data dalam jaringan berbasis *transmission control protocol/ internet protocol*;
c. menerapkan sistem anti *distributed denial of service*;
d. menerapkan autentikasi untuk memverifikasi identitas eksternal antar layanan yang terhubung;
e. menerapkan manajemen keamanan sesi;

f. menerapkan pembatasan akses pengguna berdasarkan otorisasi yang telah ditetapkan;
g. menerapkan validasi *input*;
h. menerapkan kriptografi pada verifikasi statis;
i. menerapkan sertifikat elektronik pada *web authentication*;
j. menerapkan penanganan eror dan pencatatan *log*;
k. menerapkan proteksi data dan jalur komunikasi;
l. menerapkan pendeteksi *virus* untuk memeriksa beberapa konten *file*;
m. menetapkan perjanjian tingkat layanan (SLA); dan
n. memastikan sistem integrasi tidak memiliki kerentanan yang berpotensi menjadi celah peretas.

Pasal 45

Fungsi kontrol perangkat *integrator* sebagaimana dimaksud dalam Pasal 42 huruf c dilakukan dengan prosedur:
a. menggunakan sistem operasi dan perangkat lunak dengan *security patches* terkini;
b. menggunakan anti-*virus* dan anti-*spyware*;
c. mengaktifkan fitur keamanan pada peramban web;
d. menerapkan *firewall* dan *host-based intrusion detection systems*;
e. mencegah instalasi perangkat lunak yang belum terverifikasi;
f. mencegah akses terhadap situs yang tidak sah; dan
g. mengaktifkan sistem *recovery* dan *restore* pada perangkat *integrator*.

Pasal 46

Fungsi keamanan API dan *Web Service* sebagaimana dimaksud dalam Pasal 42 huruf d dilakukan dengan prosedur:
a. menerapkan protokol *secure socket layer* atau protokol *transport layer security* di antara pengirim dan penerima API;
b. menerapkan protokol *open authorization* versi terkini untuk menjembatani interaksi antara *resource owner*, *resource server* dan/atau *third party*;
c. menampilkan metode RESTful *hypertext transfer protocol* apabila *input* pengguna dinyatakan valid;
d. melindungi layanan web RESTful yang menggunakan *cookie* dari *cross-site request forgery*; dan
e. memvalidasi parameter yang masuk oleh penerima API untuk memastikan data yang diterima valid dan tidak menyebabkan kerusakan.

Pasal 47

Fungsi keamanan migrasi data sebagaimana dimaksud dalam Pasal 42 huruf e dilakukan dengan prosedur:
a. memastikan migrasi data dilakukan secara bertahap dan terprogram oleh sistem;
b. memastikan aplikasi yang menggunakan sistem basis data lama tetap dipertahankan sampai sistem pendukung basis data baru dapat berjalan atau berfungsi dengan normal;
c. mendokumentasikan format sistem basis data lama secara rinci;
d. melakukan pencadangan seluruh data yang tersimpan pada sistem sebelum melakukan migrasi data;
e. menerapkan teknik kriptografi pada proses penyimpanan dan pengambilan data; dan
f. melakukan validasi data ketika proses migrasi data selesai.

Bagian Kelima
Keamanan Jaringan Intra

Pasal 48

(1) Standar teknis keamanan Jaringan Intra sebagaimana dimaksud dalam Pasal 15 ayat (2) huruf d diterapkan pada Jaringan Intra Pemerintah Daerah.
(2) Standar teknis keamanan Jaringan Intra sebagaimana dimaksud pada ayat (1) terdiri atas terpenuhinya:
    a. aspek administrasi keamanan Jaringan Intra;
    b. kontrol akses dan autentikasi;
    c. persyaratan perangkat dan aplikasi keamanan Jaringan Intra;
    d. kontrol keamanan *gateway*;
    e. kontrol keamanan *access point* pada jaringan nirkabel; dan
    f. kontrol konfigurasi *access point* pada jaringan nirkabel.

Pasal 49

Aspek administrasi keamanan Jaringan Intra sebagaimana dimaksud dalam Pasal 48 ayat (2) huruf a dilakukan dengan prosedur:
a. menyusun dan mengevaluasi dokumen arsitektur jaringan intra;
b. mengidentifikasi seluruh aset infrastruktur jaringan;
c. menyusun dan menetapkan standar operasional prosedur terkait pemeliharaan keamanan Jaringan Intra; dan
d. membuat laporan pengawasan keamanan jaringan seperti laporan pemantauan kerentanan perangkat pada CVE, dan laporan deteksi upaya intrusi pada jaringan internal.

Pasal 50

Kontrol akses dan autentikasi sebagaimana dimaksud dalam Pasal 48 ayat (2) huruf b dilakukan dengan prosedur:
a. menempatkan perangkat infrastruktur jaringan yang menyediakan layanan Jaringan Intra pada zona terpisah;
b. menggunakan autentikasi untuk mengakses Jaringan Intra;
c. menerapkan pembatasan akses dalam Jaringan Intra;
d. mematikan atau membatasi *protocol*, *port*, dan layanan yang tidak digunakan;
e. menerapkan penyaringan tautan dan memblokir akses ke situs berbahaya;
f. menerapkan fungsi *honeypot* untuk menganalisis celah keamanan berdasarkan jenis serangan;
g. menerapkan *virtual private network* dan mengaktifkan fungsi enkripsi pada jalur komunikasi yang digunakan;
h. memberikan kewenangan hanya kepada *administrator* yang telah ditunjuk dan/ diberi kewenangan untuk menginstal perangkat lunak dan/atau mengubah konfigurasi sistem dalam Jaringan Intra;
i. menerapkan *secure endpoints* (seperti penggunaan anti-virus, dan *patching security* terkini pada perangkat *endpoint*);
j. memblokir layanan yang tidak dikenal;
k. menerapkan *secure socket layer* atau *transport layer security* versi terkini pada jalur akses Jaringan Intra; dan
l. menerapkan server perantara saat *client* mengakses server *database* dalam rangka pemeliharaan.

Pasal 51

Persyaratan perangkat dan aplikasi keamanan Jaringan Intra sebagaimana dimaksud dalam Pasal 48 ayat (2) huruf c dilakukan dengan prosedur:
a. menggunakan perangkat *security information and event management* untuk *network logging* dan *monitoring*;
b. menerapkan sistem deteksi dini kerentanan keamanan perangkat jaringan;

c. menggunakan perangkat *firewall*;
d. menggunakan perangkat *intrusion detection systems* dan *intrusion prevention systems*;
e. menerapkan *virtual private network* terenkripsi untuk penggunaan akses jarak jauh secara terbatas;
f. menerapkan kontrol *update patching* pada infrastruktur Jaringan Intra dan sistem komputer;
g. menggunakan perangkat *web application firewall*;
h. menggunakan perangkat *load balancer* untuk menjaga ketersediaan akses terhadap jaringan dan aplikasi;

i. memperbarui teknologi keamanan perangkat keras dan perangkat lunak untuk meminimalisasi celah peretas;
j. mengunduh perangkat lunak melalui *enterprise software distribution system*; dan
k. menerapkan sertifikat elektronik.

Pasal 52

Kontrol keamanan *gateway* sebagaimana dimaksud dalam Pasal 48 ayat (2) huruf d dilakukan dengan prosedur:
a. menerapkan *content filtering*;
b. menerapkan *inspection packet filtering* untuk memeriksa paket yang masuk pada Jaringan Intra;
c. menerapkan kontrol keamanan pada fitur akses jarak jauh perangkat *gateway*;
d. memastikan perangkat *gateway* yang menghubungkan antar Jaringan Intra tidak terkoneksi langsung dengan jaringan publik;
e. melaksanakan manajemen *traffic gateway*; dan
f. memastikan *port* tidak dibuka secara *default*.

Pasal 53

Kontrol keamanan *access point* pada jaringan nirkabel sebagaimana dimaksud dalam Pasal 48 ayat (2) huruf e dilakukan dengan prosedur:
a. menerapkan protokol keamanan *access point* nirkabel dan teknologi enkripsi terkini;
b. menerapkan *media access control* pada *address filtering*;
c. menerapkan *dedicated service set identifier* (SSID);
d. menerapkan pembatasan jangkauan radio transmisi dan pengguna jaringan;
e. menerapkan pembatasan terkait penambahan perangkat nirkabel yang dipasang secara tidak sah;
f. menerapkan manajemen *vulnerability* secara berkala dan berkelanjutan; dan
g. melakukan *patching firmware* secara rutin.

Pasal 54

Kontrol konfigurasi *access point* pada jaringan nirkabel sebagaimana dimaksud dalam Pasal 48 ayat (2) huruf f dilakukan dengan prosedur:
a. menggunakan kata sandi yang kuat;
b. menggunakan protokol model *authentication authorization* dan *accounting* pada perangkat infrastruktur jaringan untuk *management user* atau otentikasi *administrator access point*;
c. memastikan fitur akses konfigurasi jarak jauh hanya dapat digunakan dalam kondisi darurat dengan menerapkan kontrol keamanan;
d. mengisolasi atau melakukan segmentasi jaringan area lokal nirkabel; dan
e. menonaktifkan antarmuka nirkabel, layanan, dan aplikasi yang tidak digunakan.

Bagian Keenam
Keamanan Pusat Data

Pasal 55

Standar teknis keamanan Pusat Data sebagaimana dimaksud dalam Pasal 15 ayat (2) huruf e terdiri atas terpenuhinya:
a. persyaratan keamanan fisik dan manajemen Pusat Data; dan
b. persyaratan koneksi perangkat ke Pusat Data.

Pasal 56

Persyaratan keamanan fisik dan manajemen Pusat Data sebagaimana dimaksud dalam Pasal 55 huruf a dilakukan dengan prosedur:
a. pusat data berada pada lokasi yang aman;
b. ruang komputer tidak boleh berada dibawah area perpipaan (*plumbing*);
c. jendela ruang komputer yang menghadap ke sinar matahari harus ditutup untuk mencegah paparan panas;
d. memiliki area bongkar muat yang memadai untuk menanganan penghantaran barang/ peralatan;
e. memiliki sistem pengkondisian udara, proteksi kebakaran, dan kelistrikan;
f. melakukan pengamanan pusat data selama 24 (dua puluh empat) jam;
g. memasang perangkat sistem pemantauan visual;
h. memastikan setiap tamu/ pengunjung memiliki izin;
i. memastikan dinding dan pintu tahan terhadap api;
j. memastikan tersedianya penyediaan catu daya;
k. memastikan ruang pusat data memiliki terminal pembumian (*grounding*); dan
l. memastikan penyediaan pengkabelan dan manajemen kabel.

Pasal 57

Persyaratan koneksi perangkat ke Pusat Data sebagaimana dimaksud dalam Pasal 55 huruf b dilakukan dengan prosedur:
a. memastikan keamanan perangkat yang terkoneksi ke infrastruktur Pusat Data;
b. memutus akses fisik atau *logic* dari perangkat yang tidak terotorisasi;
c. memastikan akses tingkat *administrator* ke server fisik utama tidak boleh dilakukan secara *remote*;
d. memastikan hanya personil yang berwenang yang boleh menggunakan komputer di area Pusat Data;
e. melakukan backup informasi dan perangkat lunak yang berada di Pusat Data secara berkala;
f. memastikan perangkat komputer Pusat Data terbebas dari *virus* dan *malware*;
g. melakukan pembatasan akses pemanfaatan *removable media* di area Pusat Data;
h. memastikan pengaktifan konfigurasi *port universal serial bus* telah mendapatkan izin dari personil yang berwenang;
i. memastikan setiap perangkat yang akan terkoneksi ke infrastruktur Pusat Data Nasional menggunakan internet *protocol address* dan *hostname* yang telah ditentukan; dan
j. menerapkan server perantara saat *client* mengakses server *database* dalam rangka pemeliharaan.

BAB IV
KETENTUAN PENUTUP

Pasal 58

Pedoman SMKI SPBE tercantum dalam Lampiran merupakan bagian yang tidak terpisahkan dari Peraturan Wali Kota ini.

Pasal 59

Peraturan Wali Kota ini mulai berlaku pada tanggal diundangkan.

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

Ditetapkan di Kota Salatiga
pada tanggal 8 Juni 2023

Pj. WALI KOTA SALATIGA,

ttd

SINOENG N. RACHMADI

Diundangkan di Kota Salatiga
pada tanggal 8 Juni 2023

SEKRETARIS DAERAH
KOTA SALATIGA

ttd

WURI PUJIASTUTI

BERITA DAERAH KOTA SALATIGA TAHUN 2023 NOMOR 9

Salinan Produk Hukum Daerah
Sesuai Aslinya
KEPALA BAGIAN HUKUM
SEKRETARIAT DAERAH KOTA SALATIGA,

ANDRIANI, S.H.
Pembina Tk.I
NIP. 19700430 199703 2 003

LAMPIRAN
PERATURAN WALI KOTA SALATIGA
NOMOR 9 TAHUN 2023
TENTANG
SISTEM MANAJEMEN KEAMANAN INFORMASI
SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

PEDOMAN SISTEM MANAJEMEN KEAMANAN INFORMASSI
SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK

BAB I
Keamanan Informasi

A. Tujuan

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

B. Ruang Lingkup

Ruang lingkup kebijakan ini adalah seluruh data dan informasi, aplikasi dan infrastruktur yang berada di bawah Pemerintah Kota Salatiga.

C. Kebijakan

1. Organisasi Perangkat Daerah (OPD) berkomitmen untuk mengembangkan, mengimplementasikan, memelihara dan meningkatkan SMKI secara berkesinambungan untuk menjamin keamanan informasi organisasi dari risiko keamanan informasi, baik dari pihak internal maupun eksternal.
2. Seluruh data dan informasi yang dikomunikasikan secara langsung atau melalui teknologi komunikasi harus dilindungi dari kemungkinan terjadi kerusakan, kesalahan penggunaan baik secara sengaja atau tidak, dicegah dari akses oleh pengguna yang tidak berwenang dan dari ancaman terhadap kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*).
3. OPD berkomitmen untuk mendukung pemenuhan prasyarat internal maupun eksternal keamanan informasi yang relevan.
4. OPD berkomitmen untuk mematuhi seluruh peraturan perundang-undangan, regulasi dan kewajiban kontrak yang relevan.
5. OPD berkomitmen untuk memastikan ketersediaan dari sumber daya yang dibutuhkan oleh SMKI di untuk menjamin terciptanya SMKI yang efektif dan efisien.
6. Kontrol keamanan informasi beserta sasaran masing-masing kontrol ditetapkan oleh Kepala Dinas Komunikasi dan Informatika Kota Salatiga secara tahunan, didasarkan atas hasil identifikasi dan analisis risiko yang sesuai dengan ruang lingkup kebijakan SMKI, serta prioritisasi dengan mempertimbangakan ketersediaan dan kemampuan sumber daya.
7. Kebijakan keamanan informasi harus dikomunikasikan ke seluruh pegawai dan pihak ketiga terkait melalui media komunikasi yang ada agar dipahami dengan mudah dan dipatuhi.
8. OPD berkomitmen meningkatkan kepedulian (*awareness*), pengetahuan dan keterampilan tentang keamanan informasi bagi pegawai, serta mitra pihak ketiga lain sejauh diperlukan.
9. Seluruh kelemahan keamanan informasi yang berpotensi atau telah mengakibatkan gangguan penggunaan teknologi informasi atau gangguan keamanan informasi harus segera dilaporkan kepada penanggung jawab terkait.

10. Seluruh pimpinan di semua tingkat bertanggung jawab menjamin kebijakan ini ditetapkan di seluruh unit kerja di bawah pengawasannya.
11. Seluruh pegawai bertanggung jawab untuk menjaga dan melindungi keamanan aset informasi serta mematuhi kebijakan dan prosedur keamanan informasi yang telah ditetapkan.
12. Setiap pelanggaran terhadap kebijakan ini dapat dikenai sanksi administratif sesuai ketentuan perundang-undangan.
13. Setiap pengecualian terhadap kebijakan ini dan kebijakan turunannya harus mendapatkan persetujuan dari Kepala Dinas Komunikasi dan Informatika Kota Salatiga.
14. Dokumen ini harus ditinjau paling sedikit 1 (satu) kali dalam 1 (satu) tahun atau apabila terdapat perubahan signifikan dalam proses bisnis organisasi untuk menjamin kesesuaian dan kecukupan dengan kondisi terkini.
15. Setiap perubahan terhadap dokumen ini harus didokumentasikan dan disetujui melalui proses manajemen perubahan.

BAB II
Manajemen risiko SPBE

A. Tujuan

Kebijakan ini disusun dengan tujuan, antara lain:

1. meningkatkan pencapaian tujuan penerapan manajemen risiko SPBE;
2. memberikan dasar yang kuat untuk perencanaan dan pengambilan keputusan melalui penyajian informasi risiko yang memadai;
3. meningkatkan optimalisasi pemanfaatan sumber daya dalam penerapan manajemen risiko SPBE; dan
4. menciptakan budaya sadar risiko bagi pegawai ASN di lingkungan Pemerintah Kota Salatiga.

B. Ruang Lingkup

Ruang lingkup kebijakan manajemen risiko SPBE, meliputi:

1. kerangka kerja keamanan manajemen risiko SPBE SPBE;
2. proses manajemen risiko SPBE SPBE;
3. struktur manajemen risiko SPBE SPBE; dan
4. budaya sadar risiko.

C. Kebijakan

1. Kerangka Kerja Keamanan Manajemen risiko SPBE

a. Kerangka kerja manajemen risiko SPBE mendeskripsikan komponen dasar yang digunakan sebagai landasan penerapan manajemen risiko SPBE SPBE di Pemerintah Kota Salatiga. Komponen dasar dari kerangka kerja terdiri atas prinsip peningkatan nilai dan perlindungan, kepemimpinan dan komitmen, serta proses dan tata kelola manajemen risiko SPBE.

b. Prinsip utama dari penerapan manajemen risiko SPBE adalah menciptakan peningkatan nilai tambah dan perlindungan bagi Organisasi Perangkat Daerah (OPD). Prinsip utama tersebut memiliki karakteristik sebagai berikut:

1) Terintegrasi, yaitu manajemen risiko SPBE merupakan serangkaian proses yang terintegrasi dengan proses pelaksanaan tugas dan fungsi OPD;
2) Terstruktur dan komprehensif, yaitu manajemen risiko SPBE dibangun secara terstruktur, sistematis dan efisiensi dan konsistensi hasil yang dapat diukur dalam peningkatan kualitas;
3) Dapat disesuaikan, yaitu kerangka kerja dan proses manajemen risiko SPBE dapat disesuaikan dengan konteks internal dan eksternal OPD dalam penerapan manajemen risiko SPBE;
4) Inklusif, yaitu manajemen risiko SPBE melibatkan semua pemangku kepentingan sesuai dengan pengetahuan, pandangan dan persepsinya untuk membangun budaya sadar risiko di Pemerintah Kota Salatiga;
5) Dinamis, yaitu manajemen risiko SPBE dapat dipergunakan untuk mengantisipasi dan merespon perubahan konteks di Pemerintah Kota Salatiga dengan tepat dan sesuai waktu;
6) Informasi tersedia dan terbaik, yaitu informasi yang digunakan sebagai masukan dalam proses manajemen risiko SPBE didasarkan pada data historis, pengalaman, observasi, perkiraan, penilaian ahli dan data dukung lain yang tersedia di Pemerintah Kota Salatiga;
7) Faktor manusia dan budaya, yaitu keberhasilan penerapan manajemen risiko SPBE

c. Wali Kota hendaknya menunjukkan kepemimpinan dan komitmen dalam penerapan kerangka kerja manajemen risiko SPBE, melalui proses:
   1) Integrasi
      a) kerangka kerja Manajemen risiko SPBE hendaknya diintegrasikan dengan proses pelaksanaan tugas dan fungsi Pemerintah Daerah;
      b) integrasi dapat dilakukan dengan memahami struktur dan konteks organisasi yang didasarkan pada tujuan, sasaran dan kompleksitas organisasi; dan
      c) tata kelola manajemen risiko SPBE perlu dibangun dengan menyusun struktur manajemen risiko SPBE beserta tugas-tugasnya untuk menjalankan, mengendalikan dan melakukan pengawasan terhadap penerapan proses manajemen risiko SPBE dalam rangka mencapai sasaran dan target kinerja organisasi dalam manajemen risiko SPBE.
   2) Desain
      a) memahami struktur dan konteks organisasi termasuk tujuan, sasaran dan kompleksitas organisasi;
      b) mengekspresikan komitmen pimpinan terhadap penerapan kerangka kerja manajemen risiko SPBE dalam bentuk kebijakan, pernyataan atau bentuk dukungan lainnya;
      c) menetapkan kewenangan, tanggung jawab dan akuntabilitas dari setiap peran di dalam kerangka kerja manajemen risiko SPBE;
      d) menyediakan sumber daya yang diperlukan seperti SDM dan kompetensi, anggaran, proses dan prosedur, informasi dan pengetahuan dan pelatihan; dan
      e) membangun komunikasi dan konsultasi untuk efektivitas implementasi kerangka kerja manajemen risiko SPBE.
   3) Implementasi
      a) kerangka kerja manajemen risiko SPBE diterapkan dengan melibatkan semua pemangku kepentingan di Pemerintah Kota Salatiga; dan
      b) kerangka kerja manajemen risiko SPBE diterapkan melalui penyusunan rencana, penyediaan sumber daya, pembuatan keputusan dan pelaksanaan manajemen risiko SPBE.
   4) Pemantauan dan Evaluasi
      a) mengukur efektivitas implementasi kerangka kerja manajemen risiko SPBE
      b) Wali Kota perlu melakukan pemantauan dan evaluasi secara berkala untuk pengukuran kinerja dan kesesuaian kerangka kerja manajemen risiko SPBE terhadap tujuan dan sasarannya.
   5) Perbaikan
      Hasil pemantauan dan evaluasi kerangka kerja manajemen risiko SPBE digunakan untuk melakukan perubahan dan perbaikan kerangka kerja manajemen risiko SPBE secara berkelanjutan sehingga kesesuaian, kecukupan dan efektivitas dari kerangka kerja dapat ditingkat.

2. Proses Manajemen risiko SPBE

a. Proses manajemen risiko SPBE merupakan rangkaian proses yang sistematis dan menjadi bagian dari proses pelaksanaan tugas dan fungsi Pemerintah Kota Salatiga untuk pengambilan keputusan pada tingkat strategis, operasional dan pelaksanaan proyek. Proses manajemen risiko SPBE dilaksanakan oleh Pemerintah Kota Salatiga terdiri atas:
   1) komunikasi dan konsultasi;
   2) penetapan konteks risiko;
   3) Penilaian risiko, yang terdiri identifikasi risiko, analisis risiko dan evaluasi risiko;
   4) penanganan risiko;
   5) pemantauan dan reviu; dan
   6) pencatatan dan pelaporan.

   Sedangkan, tata kelola manajemen risiko SPBE merupakan mekanisme untuk mengatur kewenangan dan memastikan akuntabilitas pelaksanaan manajemen risiko SPBE di OPD. Dalam hal ini, tata kelola manajemen risiko SPBE dibangun dengan menyusun struktur manajemen risiko SPBE dan membangun budaya sadar risiko. Struktur manajemen risiko SPBE di Pemerintah Kota Salatiga sedikitnya terdiri atas fungsi yang terkait dengan strategi dan kebijakan, pelaksanaan dan pengawasan manajemen risiko SPBE. Selain itu, budaya sadar risiko perlu dibangun dan dikembangkan oleh OPD melalui perencanaan, pelaksanaan dan pemantauan serta evaluasi kegiatan budaya sadar risiko.

b. Komunikasi dan konsultasi merupakan proses yang berkelanjutan dan berulang untuk menyediakan, membagikan ataupun mendapatkan informasi dan menciptakan dialog dengan para pemangku kepentingan mengenai risiko. Komunikasi dilakukan untuk meningkatkan kesadaran dan pemahaman mengenai risiko. Sementara konsultasi dilakukan untuk mendapatkan umpan balik dan informasi dalam rangka mendukung pengambilan keputusan. Bentuk kegiatan komunikasi dan konsultasi antara lain:
   1) rapat berkala, merupakan rapat yang diadakan secara rutin;
   2) rapat insidentil, merupakan rapat yang diadakan sewaktu-waktu; dan
   3) *focus group discussion* (FGD), merupakan kelompok diskusi yang terarah untuk membahas topik tertentu.

c. Penetapan konteks risiko bertujuan untuk mengidentifikasi parameter dasar dan ruang lingkup penerapan risiko yang harus dikelola dalam proses manajemen risiko SPBE. Tahapan penetapan konteks, meliputi:
   1) inventaris informasi umum bertujuan untuk mendapatkan gambaran umum mengenai OPD yang menerapkan manajemen risiko SPBE. Informasi yang dicantumkan meliputi nama Unit Pemilik Risiko (UPR), tugas UPR, fungsi UPR dan periode waktu pelaksanaan manajemen risiko SPBE dalam kurun waktu satu tahun.
   2) identifikasi sasaran bertujuan untuk menentukan sasaran beserta indikator dan targetnya yang mendukung sasaran OPD sebagai UPR. informasi yang tercantum, meliputi:
      a) sasaran UPR, diisi dengan sasaran dari OPD sebagai UPR yang tertuang dalam dokumen rencana strategis, rencana kerja, penetapan kinerja atau dokumen perencanaan lainnya;

b) sasaran, diisi dengan sasaran yang mendukung sasaran dari UPR;
c) indikator kinerja, diisi dengan indikator kinerja yang mendeskripsikan pencapaian sasaran;
d) target kinerja, diisi dengan target kinerja yang mendeskripsikan ukuran indikator kinerja untuk pencapaian sasaran; dan
e) informasi sasaran.

3) penentuan struktur pelaksana manajemen risiko SPBE bertujuan untuk menentukan OPD yang bertanggung jawab atas pelaksanaan manajemen risiko SPBE. Penentuan struktur pelaksana manajemen risiko SPBE, meliputi:
   a) UPR;
   b) pemilik risiko;
   c) koordinator risiko; dan
   d) pengelola risiko.
4) identifikasi pemangku kepentingan bertujuan untuk mendapatkan informasi dan memahami pihak-pihak yang melakukan interaksi dengan UPR dalam rangka pencapaian sasaran. Pihak-pihak yang terlibat meliputi OPD internal, OPD eksternal, instansi pemerintah atau non-instansi pemerintah. Hubungan kerja antara UPR dan setiap pihak pemangku kepentingan yang terkait dengan penerapan perlu dideskripsikan dengan jelas.
5) identifikasi peraturan perundang-undangan bertujuan untuk memahami kewenangan, tanggung jawab, tugas dan fungsi, serta kewajiban hukum yang harus dilaksanakan oleh UPR. informasi yang perlu dijelaskan dalam melakukan identifikasi peraturan perundang-undangan meliputi nama peraturan dan amanat dalam peraturan.
6) penetapan kategori risiko bertujuan untuk menjamin agar proses identifikasi, analisis dan evaluasi risiko dapat dilakukan secara komprehensif. Kategori risiko, meliputi:
   a) rencana induk Nasional, merupakan risiko yang berkaitan dengan penyusunan dan pelaksanaan perencanaan pembangunan Nasional;
   b) arsitektur SPBE, merupakan risiko yang berkaitan dengan penyusunan dan pemanfaatan arsitektur SPBE yang mendeskripsikan integrasi proses bisnis, layanan, data dan informasi, aplikasi, infrastruktur dan keamanan;
   c) peta rencana, merupakan risiko yang berkaitan dengan penyusunan dan pelaksanaan peta rencana;
   d) proses bisnis, merupakan risiko yang berkaitan dengan penyusunan dan penerapan proses bisnis;
   e) rencana dan anggaran, merupakan risiko yang berkaitan dengan proses perencanaan dan penganggaran;
   f) inovasi, merupakan risiko yang berkaitan dengan ide baru atau pemikiran kreatif yang memberikan nilai manfaat dalam penerapan;
   g) kepatuhan terhadap peraturan, merupakan risiko yang berkaitan dengan kepatuhan OPD terhadap peraturan perundang-undangan, kesepakatan internasional maupun ketentuan lain yang berlaku;
   h) pengadaan barang dan jasa, merupakan risiko yang berkaitan dengan proses pengadaan dan penyediaan barang dan jasa;

i) proyek pembangunan/ pengembangan sistem, merupakan risiko yang berkaitan dengan proyek pembangunan ataupun pengembangan sistem;
j) data dan informasi, merupakan risiko yang berkaitan dengan semua data dan informasi yang dimiliki oleh Pemerintah Kota Salatiga;
k) infrastruktur, merupakan risiko yang berkaitan dengan pusat data, jaringan intra pemerintah dan sistem penghubung layanan pemerintah termasuk perangkat keras, perangkat lunak dan fasilitas yang menjadi penunjang utama;
l) aplikasi, merupakan risiko yang berkaitan dengan program komputer yang diterapkan untuk melakukan tugas atau fungsi layanan;
m) keamanan, merupakan risiko yang berkaitan dengan kerahasiaan, keutuhan, keaslian dan kenirsangkalan sumber daya yang mendukung;
n) layanan, merupakan risiko yang berkaitan dengan pemberian layanan kepada pengguna;
o) sumber daya manusia (SDM), merupakan risiko yang berkaitan dengan SDM yang bekerja sebagai penggerak penerapan di Pemerintah Kota Salatiga; dan
p) bencana alam, merupakan risiko yang berkaitan dengan peristiwa yang disebabkan oleh alam.

d. Penetapan area dampak risiko bertujuan untuk mengetahui area mana saja yang terkena efek dari risiko di Pemerintah Kota Salatiga. Penetapan area dampak risiko diawali dengan melakukan identifikasi dampak risiko. Area dampak risiko yang menjadi fokus penerapan manajemen risiko SPBE, meliputi:
1) finansial, dampak risiko berupa aspek yang berkaitan dengan keuangan;
2) reputasi, dampak risiko berupa aspek yang berkaitan dengan tingkat kepercayaan pemangku kepentingan;
3) kinerja, dampak risiko berupa aspek yang berkaitan dengan pencapaian sasaran;
4) layanan organisasi, dampak risiko berupa aspek yang berkaitan dengan pemenuhan kebutuhan atau jasa kepada pemangku kepentingan;
5) operasional dan aset TIK, dampak risiko berupa aspek yang berkaitan dengan kegiatan operasional TIK dan pengelolaan aset TIK;
6) hukum dan regulasi, dampak risiko berupa aspek yang berkaitan dengan peraturan perundang-undangan dan kebijakan;
7) sumber daya manusia, dampak risiko berupa aspek yang berkaitan dengan fisik dan mental dari pegawai; dan

Area dampak risiko terdiri atas area dampak positif dan/ atau negatif. Area dampak risiko dapat disesuaikan dengan konteks internal dan eksternal di Pemerintah Kota Salatiga.

e. Penetapan kriteria risiko bertujuan untuk mengukur dan menetapkan seberapa besar kemungkinan kejadian dan dampak risiko yang dapat terjadi. Kriteria risiko ini ditinjau secara berkala dan perlu melakukan penyesuaian dengan perubahan yang terjadi. Penetapan kriteria risiko, terdiri atas:

1) kriteria kemungkinan, penetapan kriteria kemungkinan risiko dilakukan berdasarkan penetapan level kemungkinan dan penetapan kriteria dari setiap level kemungkinan terhadap risiko. Untuk kriteria kemungkinan diuraikan menjadi 5 (lima) tingkat sebagai berikut:
   a) hampir tidak terjadi;
   b) jarang terjadi;
   c) kadang-kadang terjadi;
   d) sering terjadi; dan
   e) hampir pasti terjadi.

   Sedangkan, penetapan kriteria kemungkinan dilakukan melalui pendekatan persentase probabilitas statistik, jumlah frekuensi terjadinya suatu risiko dalam satuan waktu ataupun berdasarkan *expert judgement*.
2) kriteria dampak, penetapan kriteria dampak risiko dilakukan dengan kombinasi antara area dampak risiko dan tingkat dampak. Untuk kriteria dampak diuraikan menjadi 5 (lima) tingkat sebagai berikut:
   a) tidak signifikan;
   b) kurang signifikan;
   c) cukup signifikan;
   d) signifikan; dan
   e) sangat signifikan.

f. Matriks analisis risiko berisi kombinasi antara tingkat kemungkinan dan tingkat dampak untuk dapat menetapkan besaran risiko yang direpresentasikan dalam bentuk angka.

   Besaran risiko ini selanjutnya dikelompokan ke dalam tingkat risiko dimana setiap tingkat risiko memiliki rentang nilai besaran risiko. Untuk besaran risiko diuraikan menjadi 5 (lima) tingkat sebagai berikut:
   1) sangat rendah, direpresentasikan dengan warna biru;
   2) rendah, direpresentasikan dengan warna hijau;
   3) sedang, direpresentasikan dengan warna kuning;
   4) tinggi, direpresentasikan dengan warna jingga; dan
   5) sangat tinggi, direpresentasikan dengan warna merah.

g. Selera risiko bertujuan untuk memberikan acuan dalam penentuan ambang batas minimum terhadap besaran risiko yang harus ditangani untuk setiap kategori risiko baik risiko positif maupun risiko negatif. Selera risiko yang dapat diterima adalah “Sangat Rendah dan Rendah”, sedangkan selera risiko “Sedang dan Tinggi” masih dapat diterima namun dengan dilampirkan bukti pendukung.

h. Penilaian risiko pada penerapannya dilakukan melalui proses identifikasi, analisis dan evaluasi risiko. Penilaian risiko bertujuan untuk memahami penyebab, kemungkinan dan dampak risiko yang dapat terjadi di Pemerintah Kota Salatiga. Penilaian risiko dilakukan pada setiap sasaran. Tahapan penilaian risiko, meliputi:
   1) identifikasi risiko, merupakan proses menggali informasi mengenai kejadian, penyebab dan dampak risiko. Informasi yang dicantumkan meliputi:
      a) jenis risiko terbagi menjadi risiko positif dan risiko negatif. Dalam melakukan identifikasi risiko, risiko dituliskan ke dalam masing-masing jenis risiko;
      b) kejadian dapat diidentifikasi dari terjadinya suatu peristiwa yang menimbulkan risiko yang diperoleh dari riwayat peristiwa dan/ atau prediksi terjadinya peristiwa di masa yang akan datang. Kejadian selanjutnya disebut sebagai risiko;

c) penyebab dapat diidentifikasi dari akar masalah yang menjadi pemicu munculnya risiko. Penyebab dapat berasal dari lingkungan internal maupun eksternal Pemerintah Kota Salatiga. Identifikasi penyebab akan membantu menemukan tindakan yang tepat untuk menangani risiko;
d) kategori, penentuan kategori risiko didasarkan pada penyebab dari munculnya risiko;
e) dampak dapat diidentifikasi dari pengaruh atau akibat yang timbul dari risiko; dan
f) area dampak, penentuan area dampak risiko didasarkan pada dampak yang telah teridentifikasi.

2) analisis risiko merupakan proses untuk melakukan penilaian atas risiko yang telah diidentifikasi sebelumnya. Analisis risiko dilakukan dengan cara menentukan sistem pengendalian, tingkat kemungkinan dan tingkat dampak terjadinya risiko. Informasi yang dicantumkan pada analisis risiko, meliputi:
a) sistem pengendalian internal mencakup perangkat manajemen yang dapat menurunkan/ meningkatkan tingkat risiko dalam rangka pencapaian sasaran. Sistem pengendalian internal dapat berupa *Standard Operating Procedure* (SOP), pengawasan melekat, reviu berjenjang, regulasi dan pemantauan rutin yang dilaksanakan terkait risiko;
b) tingkat kemungkinan, penentuan tingkat kemungkinan dilakukan dengan mengukur persentase probabilitas atau frekuensi peluang terjadinya risiko dalam satu periode yang dicocokan dengan kriteria kemungkinan risiko. Penentuan tingkat kemungkinan harus didukung dengan penjelasan singkat untuk mengetahui alasan dari pemilihan tingkat kemungkinan;
c) tingkat dampak, penentuan tingkat dampak dilakukan dengan mengukur besar dampak dari terjadinya risiko yang dicocokan dengan kriteria dampak risiko. Tingkat dampak harus didukung dengan penjelasan singkat untuk mengetahui alasan pemilihan tingkat dampak; dan
d) besaran risiko dan tingkat risiko, penentuan besaran risiko dan tingkat risiko didapat dari kombinasi level kemungkinan dan level dampak dengan menggunakan rumusan dalam matriks analisis risiko.

3) evaluasi risiko dilakukan untuk mengambil keputusan mengenai perlu tidaknya dilakukan upaya penanganan risiko lebih lanjut serta penentuan prioritas penanganannya. Pengambilan keputusan mengacu pada selera risiko yang telah ditentukan. Prioritas penanganan risiko diurutkan berdasarkan besaran risiko. Apabila terdapat lebih dari satu risiko yang memiliki besaran yang sama maka cara penentuan prioritas berdasarkan *expert judgement*.

i. Penanganan risiko, merupakan proses untuk memodifikasi penyebab risiko. Penanganan risiko dilakukan dengan mengidentifikasi berbagai opsi yang memungkinkan diterapkan dan memilih satu atau lebih opsi penanganan risiko. Informasi yang dicantumkan meliputi:

1) prioritas risiko, diurutkan berdasarkan risiko. Risiko yang memiliki prioritas lebih tinggi ditunjukkan dengan nilai besaran risiko yang lebih tinggi.

2) rencana penanganan risiko, merupakan agenda kegiatan untuk menangani risiko agar mencapai selera risiko yang telah ditetapkan. Rencana penanganan risiko dilakukan dengan mengidentifikasi hal-hal sebagai berikut:
   a) opsi penanganan risiko, berisikan alternatif yang dipilih untuk menangani risiko. Opsi penanganan risiko dilakukan dengan mengidentifikasikan berbagai opsi yang mungkin untuk diterapkan. Opsi penanganan risiko terbagi menjadi dua, yaitu penanganan risiko positif dan penanganan risiko negatif, penanganan risiko yang dimaksud meliputi:
      (1) eskalasi risiko, dipilih jika risiko berada di luar atau melampaui wewenang. Opsi ini dilakukan dengan memindahkan tanggung jawab penanganan risiko ke unit kerja yang lebih tinggi.
      (2) eksploitasi risiko, dipilih jika risiko dapat dipastikan terjadi. Opsi ini dilakukan dengan cara memanfaatkan risiko tersebut semaksimal mungkin.
      (3) peningkatan risiko, dilakukan dengan cara meningkatkan tingkat kemungkinan dan/ atau tingkat dampak dari risiko.
      (4) pembagian risiko, dipilih jika risiko tidak dapat ditangani secara langsung dan membutuhkan pihak lain untuk menangani risiko. Pembagian risiko dilakukan dengan bekerja sama dengan pihak lain.
      (5) penerimaan risiko, dipilih jika upaya penanganan lebih tinggi dibanding manfaat yang didapat atau kemungkinan terjadinya kecil. Opsi ini dilakukan dengan cara membiarkan risiko terjadi apa adanya.
   b) rencana aksi penanganan risiko, merupakan rancangan kegiatan tindak lanjut untuk menangani risiko.
   c) keluaran, merupakan hasil dari rencana aksi penanganan risiko.
   d) jadwal implementasi, merupakan jadwal pelaksanaan dari setiap rencana aksi penanganan risiko.
   e) penanggung jawab, berisikan nama unit yang bertanggung jawab dan unit pendukung dari setiap rencana aksi penanganan risiko.
3) risiko residual merupakan risiko yang tersisa dari risiko yang telah ditangani. Dalam melakukan penanganan terhadap risiko residual, dilakukan pengulangan proses penilaian risiko sampai dengan risiko residual berada di bawah selera risiko. Penetapan risiko residual ini dapat ditetapkan berdasarkan *expert judgement*.

j. Pemantauan dan reviu
   1) pemantauan bertujuan untuk memonitor faktor-faktor atau penyebab yang mempengaruhi risiko dan kondisi lingkungan di Pemerintah Kota Salatiga. Selain itu, pemantauan dilakukan guna memonitor pelaksanaan rencana aksi penanganan risiko. Hasil pelaksanaan pemantauan dapat menjadi dasar untuk melakukan penyesuaian kembali proses manajemen risiko SPBE. Pemantauan dilakukan berdasarkan setiap triwulan, semester, tahun, atau sewaktu-waktu (insidental) sesuai dengan kesepakatan dari masing-masing OPD; dan
   2) reviu bertujuan untuk mengontrol kesesuaian dan ketepatan seluruh pelaksanaan proses manajemen risiko SPBE sesuai dengan ketentuan yang berlaku. Reviu dilakukan sesuai dengan kesepakatan dari masing-masing OPD.

k. Pencatatan dan pelaporan
   1) pencatatan merupakan kegiatan atau proses pendokumentasian suatu aktivitas dalam bentuk tulisan dan dituangkan dalam dokumen; dan
   2) pelaporan merupakan kegiatan yang dilakukan untuk menyampaikan hal-hal yang berhubungan dengan hasil pekerjaan yang telah dilakukan selama satu periode tertentu. Proses manajemen risiko SPBE dan keluaran yang dihasilkan perlu dicatat dan dilaporkan dengan mekanisme yang tepat

   Pencatatan dan pelaporan bertujuan untuk mengkomunikasikan aktivitas manajemen risiko SPBE serta keluaran yang dihasilkan, menyediakan informasi untuk pengambilan keputusan, meningkatkan kualitas aktivitas manajemen risiko SPBE serta mengawal interaksi dengan pemangku kepentingan termasuk tanggung jawab serta akuntabilitas terhadap manajemen risiko SPBE. Pencatatan dan pelaporan manajemen risiko SPBE terdiri dari:
   1) pencatatan dan pelaporan periodik, merupakan kegiatan yang dilakukan secara berulang pada waktu yang telah ditentukan; dan
   2) Pencatatan dan pelaporan insidental, merupakan kegiatan yang dilakukan pada waktu tertentu sesuai dengan kebutuhan.

l. Dokumen manajemen risiko SPBE, meliputi:
   1) pakta integritas manajemen risiko SPBE, merupakan dokumen pernyataan atau janji untuk berkomitmen menjalankan manajemen risiko SPBE di Lingkungan Pemerintah Kota Salatiga;
   2) dokumen proses risiko, merupakan dokumen pendukung pelaksanaan proses penetapan konteks, penilaian dan penanganan risiko. Dokumen proses risiko terdiri dari formulir konteks risiko, formulir penilaian risiko dan formulir rencana penanganan risiko; dan
   3) dokumen proses pengendalian risiko, merupakan dokumen pendukung pelaksanaan proses komunikasi dan konsultasi serta pelaporan risiko. Dokumen proses pengendalian risiko terdiri dari dokumen kegiatan komunikasi, konsultasi dan dokumen laporan pemantauan.

3. Struktur Manajemen

a. Struktur manajemen risiko SPBE, terdiri atas:
   1) komite manajemen risiko SPBE (KMR) dibentuk dan ditetapkan oleh Wali Kota Salatiga, dan memiliki anggota yang terdiri atas pejabat Pemerintah Kota Salatiga yang memiliki kewenangan pengambilan keputusan dan penetapan kebijakan strategis terkait manajemen risiko SPBE. KMR memiliki tugas menyelenggarakan perumusan dan penetapan kebijakan, pengendalian, pemantauan dan evaluasi penerapan kebijakan manajemen risiko SPBE. Dalam melaksanakan tugas dan fungsinya sebagai berikut:
      a) penyusunan dan penetapan kebijakan manajemen risiko SPBE;
      b) penyusunan dan penetapan kerangka kerja dan pedoman pelaksanaan manajemen risiko SPBE;
      c) penyusunan dan penetapan pakta integritas manajemen risiko SPBE;
      d) penyusunan dan penetapan konteks risiko;

e) pengendalian proses risiko melalui komunikasi dan konsultasi, pencatatan dan pelaporan serta pemantauan dan evaluasi terhadap penerapan manajemen risiko SPBE; dan
f) pelaksanaan komitmen pimpinan dan penerapan budaya sadar risiko.

2) unit pemilik risiko (UPR), merupakan OPD di Pemerintah Kota Salatiga. UPR memiliki tugas melaksanakan penerapan manajemen risiko SPBE pada OPD. UPR terdiri atas unsur:
a) pemilik risiko merupakan pejabat yang bertanggung jawab atas pelaksanaan penerapan manajemen risiko SPBE di OPD;
b) koordinator risiko merupakan pejabat/ pegawai yang ditunjuk oleh pemilik risiko untuk bertanggung jawab atas pelaksanaan koordinasi penerapan manajemen risiko SPBE kepada semua pemangku kepentingan baik internal maupun eksternal UPR; dan
c) pengelola risiko merupakan pejabat/ pegawai yang ditunjuk oleh pemilik risiko untuk bertanggung jawab atas pelaksanaan operasional manajemen risiko SPBE pada OPD.

Dalam melaksanakan tugasnya, UPR menjalankan fungsi sebagai berikut:
a) penyusunan dan penetapan penilaian risiko dan rencana pelaksanaan manajemen risiko SPBE termasuk rencana kontijensi penanganan risiko;
b) pelaksanaan koordinasi penerapan manajemen risiko SPBE kepada semua pemangku kepentingan;
c) pelaksanaan operasional manajemen risiko SPBE yang efektif melalui komunikasi dan konsultasi, pencatatan dan pelaporan serta pemantauan dan evaluasi;
d) pelaksanaan pembinaan budaya sadar sosialisasi, bimbingan dan pelatihan; dan
e) manajemen risiko SPBE.

3) unit kepatuhan risiko (UKR), merupakan OPD yang melaksanakan fungsi pengawasan internal di Pemerintah Kota Salatiga. UKR memiliki tugas melaksanakan pengawasan terhadap penerapan kebijakan manajemen risiko SPBE di semua UPR. Dalam melaksanakan tugasnya, UKR menjalankan fungsi sebagai berikut:
a) penyusunan kebijakan pengawasan terhadap penerapan manajemen risiko SPBE;
b) pelaksanaan pengawasan intern terhadap penerapan manajemen risiko SPBE di semua UPR melalui audit, reviu, pemantauan, evaluasi dan kegiatan pengawasan lainnya;
c) pelaksanaan konsultasi dan asistensi kepada UPR dalam penerapan manajemen risiko SPBE;
d) penyusunan dan penyampaian rekomendasi terhadap efektivitas penerapan manajemen risiko SPBE kepada KMR dan UPR; dan
e) pelaksanaan konsultasi dan asistensi kepada UPR dalam pembinaan budaya sadar risiko.

b. Struktur manajemen risiko SPBE dapat mengadopsi struktur manajemen risiko SPBE yang telah ada.

4. Budaya Sadar Risiko

a. Budaya sadar risiko merupakan perilaku ASN yang mengenal, memahami dan mengakui kemungkinan terjadinya risiko, baik secara positif maupun negatif, yang ditindaklanjuti dengan upaya yang berfokus pada penerapan manajemen risiko SPBE di Pemerintah kota Salatiga. ASN harus peka terhadap faktor-faktor dan peristiwa yang mungkin berpengaruh terhadap tujuan dan sasaran penerapan manajemen risiko SPBE di Pemerintah Kota Salatiga.

b. Dengan menyadari adanya risiko, ASN dapat merencanakan dan mempersiapkan tindakan atau penanganan risiko secepatnya. Keterlibatan ASN di dalam budaya sadar risiko akan memberikan nilai tambah dan meningkatkan efektivitas penerapan manajemen risiko SPBE yang pada akhirnya berdampak pada peningkatan kualitas di Pemerintah Kota Salatiga.

c. Faktor keberhasilan yang dapat mendukung keberhasilan dalam menciptakan budaya sadar risiko, antara lain:

1) kepemimpinan, KPMR harus dapat menunjukan sikap kepemimpinan, yaitu konsisten dalam perkataan dan tindakan, mampu mendorong atau menggerakan ASN dalam penerapan budaya sadar risiko, mampu menempatkan manajemen risiko SPBE sebagai agenda penting di dalam setiap pengambilan keputusan dan memiliki komitmen yang kuat dalam menerapkan manajemen risiko SPBE melalui penyediaan sumber daya yang cukup, baik dari anggaran, SDM, kebijakan, pedoman, maupun strategi penerapannya di Pemerintah Kota Salatiga;

2) keterlibatan semua pihak, budaya sadar risiko melibatkan semua ASN yang terkait secara langsung maupun tidak langsung, baik ASN yang berada pada KMR, UPR maupun UKR, karena mereka yang paling memahami terjadinya risiko dan cara penanganannya dalam tingkat strategis maupun operasional;

3) komunikasi pentingnya manajemen risiko SPBE harus dapat disampaikan kepada setiap ASN yang terlibat dalam penerapan melalui penyediaan saluran komunikasi yang variatif dan efektif. Tidak hanya KMR menyampaikan informasi terkait kebijakan manajemen risiko SPBE kepada ASN, tetapi juga ASN dapat menyampaikan informasi risiko kepada pimpinan di setiap jenjang termasuk kepada KMR. saluran komunikasi ini dapat diwujudkan melalui rapat-rapat pengambilan keputusan, berbagai pertemuan dalam proses manajemen risiko SPBE dan penyampaian informasi melalui saluran komunikasi elektronik seperti surat elektronik, sistem naskah dinas elektronik, sistem aplikasi manajemen risiko SPBE, *video conference* dan lain sebagainya;

4) daya responsif sangat penting untuk mencegah ancaman yang dapat menghambat tercapainya tujuan penerapan ataupun meraih peluang untuk mempercepat tercapainya tujuan penerapan dan peningkatan kualitasnya. ASN yang responsif akan lebih siap beradaptasi terhadap perubahan dan penyelesaian masalah yang rumit dalam penerapannya;

5) sistem penghargaan, KMR hendaknya memahami secara langsung permasalahan yang dialami oleh ASN pada pelaksanaan tugas UPR dan UKR, serta menjadikan pencapaian kinerja risiko sebagai salah satu indikator dalam pemberian penghargaan dan sanksi;

6) integrasi proses, proses manajemen risiko SPBE hendaknya diintegrasikan dengan proses manajemen di Pemerintah Kota Salatiga sehingga tidak dipandang sebagai tambahan beban pekerjaan. Integrasi proses dapat dilakukan dengan menyelaraskan proses manajemen risiko SPBE sebagai satu kesatuan dari setiap proses kegiatan, proses manajemen risiko SPBE dan proses manajemen kinerja Pemerintah Kota Salatiga; dan
7) program kegiatan berkelanjutan, agar budaya sadar risiko dapat diterima oleh ASN, KMR hendaknya menyusun program kegiatan budaya sadar risiko secara sistematis dan terencana, seperti kegiatan edukasi, berbagi pengetahuan dan kunjungan kerja/ supervisi ke UPR.

d. Pengembangan budaya sadar risiko dapat dilakukan melalui langkah-langkah berikut ini:
1) menyusun perencanaan kegiatan budaya sadar risiko;
2) melaksanakan kegiatan budaya sadar risiko; dan
3) Melakukan pemantauan dan evaluasi pelaksanaan kegiatan budaya sadar risiko.

e. Perencanaan kegiatan budaya sadar risiko difokuskan pada:
1) pemetaan pemangku kepentingan terhadap pelaksanaan manajemen risiko SPBE. Tujuan dari pemetaan pemangku kepentingan adalah untuk melakukan penilaian terhadap pemangku kepentingan terkait peran dan kapasitas mereka dalam mempengaruhi keberhasilan penerapan budaya sadar risiko, serta untuk menyusun prioritas kegiatan budaya sadar risiko berdasarkan tingkat kekuatan, posisi penting ataupun pengaruh dari pemangku kepentingan. Dalam hal ini, pemangku kepentingan dapat diidentifikasi dengan merujuk pada struktur manajemen risiko SPBE yang mencakup KMR, UPR dan UKR;
2) pengukuran tingkat dukungan kepentingan terhadap budaya sadar risiko. Hal ini menjadi penting untuk mengelola kegiatan budaya sadar risiko secara efektif. Dukungan pemangku kepentingan dapat digolongkan ke dalam 3 (tiga) kategori, yaitu: sangat mendukung secara konsisten, mendukung secara tidak konsisten dan tidak mendukung atau resisten terhadap budaya sadar risiko;
3) pengukuran tingkat kesiapan budaya sadar risiko. Pengukuran ini biasanya menggunakan kuesioner yang disampaikan kepada pemangku kepentingan, baik secara sampel maupun semua populasi. Pengukuran dapat difokuskan antara lain pada komitmen, manfaat/ dampak, pemahaman/ kesadaran, tata cara/ prosedur pelaksanaan dan partisipasi dari pemangku kepentingan terhadap penerapan manajemen risiko SPBE; dan
4) penyusunan rencana kegiatan budaya sadar risiko. Rencana kegiatan yang tepat disusun dengan mempertimbangkan sumber daya yang tersedia di Pemerintah Kota Salatiga seperti anggaran, waktu, sarana prasarana, SDM pelaksana, peserta dan metode pelaksanaan.

f. Pelaksanaan kegiatan budaya sadar risiko difokuskan pada implementasi rencana kegiatan budaya sadar risiko, yaitu:
1) Melakukan komunikasi kepada pemangku kepentingan. Sebelum melaksanakan rencana kegiatan budaya sadar risiko, rencana tersebut perlu dikomunikasikan kepada pemangku kepentingan dengan memberikan alasan-alasan yang rasional agar mendapatkan dukungan pelaksanaan oleh pemangku kepentingan; dan

2) mengelola hambatan/ kendala, dalam pelaksanaan kegiatan budaya sadar risiko, kendala-kendala yang terjadi agar dikelola dengan baik agar tujuan dari kegiatan dapat dicapai.

g. Pemantauan dan evaluasi kegiatan budaya sadar risiko ditujukan untuk meningkatkan budaya sadar risiko melalui perbaikan berkelanjutan. Pelaksanaan pemantauan dan evaluasi difokuskan pada:
   1) pengukuran perubahan tingkat dukungan, kesadaran dan pemahaman dari pemangku kepentingan terhadap penerapan manajemen risiko SPBE. Pengukuran terkait hal ini dapat dilakukan melalui pengumpulan dan analisis umpan balik dari pemangku kepentingan dengan cara supervisi ke unit-unit para pemangku kepentingan. Hasil analisis selanjutnya digunakan untuk memutakhirkan tingkat dukungan, kesadaran dan pemahaman dari pemangku kepentingan serta memberikan saran-saran perbaikan terhadap kegiatan budaya sadar risiko;
   2) pemutakhiran rencana kegiatan budaya sadar risiko. Rencana kegiatan budaya sadar risiko dilakukan pemutakhiran berdasarkan saran-saran perbaikan dengan tetap mempertimbangkan ketersediaan sumber daya yang dimiliki oleh Pemerintah Kota Salatiga; dan
   3) pelaksanaan perbaikan berkelanjutan, rencana kegiatan budaya sadar risiko yang telah dimutakhirkan dilaksanakan melalui langkah ke dua di atas sehingga mencapai peningkatan budaya sadar risiko.

BAB III
Keamanan Sumber Daya Manusia

A. Tujuan

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

B. Ruang Lingkup

Ruang lingkup kebijakan keamanan sumber daya manusia, terdiri dari:

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

C. Kebijakan

1. Calon pegawai di lingkungan Pemerintah Kota Salatiga dan pegawai dari pihak eksternal, harus melalui proses *screening* untuk memastikan bahwa mereka sesuai dengan tugas dan tanggung jawab yang akan mereka dapatkan.
2. Proses *screening* perlu mencakup verifikasi terhadap latar belakang kandidat sesuai dengan peraturan hukum perundang- undangan serta etika yang ada.
3. Pegawai dalam lingkungan Pemerintah Kota Salatiga dan pegawai dari pihak eksternal yang dalam aktivitas pekerjaannya memiliki akses ke aset informasi dan aset pengolahan dan penyimpanan informasi dalam lingkungan Pemerintah Kota Salatiga harus menandatangani perjanjian kerahasiaan (*non-disclosure agreement*) dengan memperhatikan tingkat sensitivitas dari aset yang diakses.
4. Setiap pegawai internal maupun eksternal harus mematuhi seluruh kebijakan dan prosedur Perangkat Daerah/ Unit Kerja terkait keamanan informasi.
5. Setiap pegawai internal maupun eksternal harus diberikan informasi yang memadai terkait tugas dan tanggung jawab terkait keamanan informasi yang mereka miliki.
6. Program peningkatan kesadaran keamanan informasi (*awareness*) secara berkelanjutan untuk menjaga dan meningkatkan kesadaran keamanan informasi dari pegawai harus dilaksanakan.
7. Setiap pelanggaran terhadap kebijakan dan prosedur terkait keamanan informasi harus ditindaklanjuti dan apabila diperlukan, tindakan pendisiplinan harus diambil sesuai dengan peraturan yang berlaku.
8. Tanggung jawab dan kewajiban terkait keamanan informasi yang tetap berlaku setelah pemberhentian atau perubahan status kepegawaian harus didefinisikan, dikomunikasikan dan ditegakkan kepada pegawai internal maupun eksternal.
9. Hal ini mencakup tanggung jawab keamanan informasi yang tercakup dalam perjanjian kerja seperti:
    a. seluruh aset organisasi harus dikembalikan setelah pemberhentian kepegawaian;
    b. seluruh hak akses organisasi harus dinonaktifkan atau dihapus setelah pemberhentian kepegawaian; dan
    c. seluruh hak akses organisasi harus disesuaikan setelah perubahan status kepegawaian.

BAB IV
Pengelolaan Aset

A. Tujuan

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

B. Ruang Lingkup

Ruang lingkup kebijakan terkait pengelolaan aset, terdiri atas:

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

C. Kebijakan

1. Kepala Dinas Komunikasi dan Informatika Kota Salatiga menetapkan pemilik aset informasi di setiap unit Perangkat Daerah, beserta perangkat fisik pengolah informasi yang terkait.
2. Pemilik aset informasi memiliki tanggung jawab untuk:
   a. mengidentifikasi seluruh aset informasi dan fasilitas pengolahan dan penyimpanan informasi;
   b. mendokumentasikannya dalam daftar inventaris aset smki, serta senantiasa memperbaharui daftar inventaris aset SMKI tersebut sesuai kondisi terkini; dan
   c. memastikan bahwa setiap aset telah diklasifikasikan dan dilindungi secara memadai.
3. Aset pengolahan dan penyimpanan informasi yang diinventarisasi adalah aset dalam bentuk:
   a. perangkat keras, meliputi perangkat keras yang digunakan untuk mengolah dan menyimpan informasi dalam bentuk fisik maupun elektronik, yang mencakup namun tidak terbatas pada komputer, *notebook*, server, *hard disk drive*, USB *disk*;
   b. perangkat lunak, meliputi perangkat lunak yang digunakan untuk mengolah informasi dalam bentuk elektronik, yang mencakup namun tidak terbatas pada sistem operasi, aplikasi, dan database;
   c. perangkat jaringan, meliputi perangkat keras dan lunak yang digunakan untuk membentuk dan infrastruktur jaringan telekomunikasi, yang mencakup namun tidak terbatas pada *hub*, *switch*, *router*, *firewall*, IDS, IPS, dan *network monitoring tools*;
   d. perangkat pendukung meliputi perangkat digunakan untuk mendukung operasional perangkat pengolahan dan penyimpanan informasi yang mencakup namun tidak terbatas pada genset, UPS (*Uninterruptible Power Supply*), AC, rak server, lemari penyimpanan informasi dan CCTV;
   e. data dan informasi, meliputi data pribadi umum, data pribadi yang bersifat spesifik, informasi manajemen administrasi pemerintah, informasi manajemen keuangan pemerintah, informasi sumber daya manusia pemerintah, informasi manajemen rantai pasok pemerintah, manajemen teknologi informasi pemerintah, informasi mengenai urusan dan layanan yang dijalankan oleh pemerintah, serta data dan informasi lainnya yang dianggap penting;

f. layanan, meliputi layanan yang digunakan untuk mendukung operasional perangkat pengolahan dan penyimpanan informasi yang mencakup namun tidak terbatas pada layanan jaringan komunikasi, layanan hosting dan co-location, layanan pemeliharaan perangkat dan sistem, dan layanan pemasangan infrastruktur; dan
g. sumber daya manusia meliputi personil baik internal maupun eksternal yang terlibat dalam pengolahan dan penyimpanan informasi.

4. Pemilik aset dapat mendelegasikan tugas pengamanan dan pemeliharaan aset kepada kustodian aset, namun tanggung jawab akhir terhadap aset tetap berada pada pemilik aset.
5. Aset pengolahan dan penyimpanan informasi harus secara berkala dipelihara dengan memadai.
6. Apabila dalam pemeliharaan aset pengolahan dan penyimpanan informasi tersebut harus menggunakan jasa pihak ketiga penyedia, maka:
   a. kontrak pemeliharaan perlu dibuat dengan pihak ketiga penyedia jasa yang kompeten dan relevan; dan
   b. peralatan yang dibawa keluar untuk pemeliharaan harus diperiksa untuk mencegah kebocoran informasi.
7. Dalam proses penghapusan aset harus dilakukan secara aman dengan metode yang dapat mencegah kebocoran informasi seperti menghancurkan secara fisik hard disk drive.
8. Semua aset informasi dan pengolahan dan penyimpanan informasi milik Pemerintah Kota Salatiga harus dikembalikan setelah personil pengguna tidak memiliki hubungan kepegawaian lagi dengan Pemerintah Kota Salatiga, misalnya karena pengunduran diri, pensiun.
9. Ketentuan dalam proses pengembalian aset tersebut mencakup:
   a. pengembalian aset harus terdokumentasi secara formal;
   b. untuk pengembalian aset yang disebabkan oleh terhentinya status kepegawaian, informasi yang tersimpan dalam aset harus di-*backup* dan informasi yang tersimpan dalam aset harus dihapus secara aman, antara lain dengan *secure format* atau melakukan instalasi ulang sistem operasi secara menyeluruh; dan
   c. media penyimpanan backup informasi harus diamankan secara fisik, antara lain dengan menyimpan dalam lemari terkunci dengan akses yang terbatas.
10. Aset pengolahan informasi, seperti komputer dan laptop yang akan digunakan kembali baik oleh pihak internal maupun eksternal harus diperiksa untuk menjamin tidak ada informasi sensitif yang tersimpan dalam aset tersebut.
11. Perangkat Daerah harus mendefinisikan klasifikasi aset informasi dengan mempertimbangkan sebagai berikut:
    a. aset informasi harus diklasifikasikan berdasarkan tingkat sensitivitas informasi serta tingkat kritikalitas sistem, yang meliputi:
       1) Klasifikasi aset informasi secara berkala; dan
       2) Pengguna yang diizinkan mengakses aset informasi terkait.
    b. Pemberian label klasifikasi informasi harus dilakukan secara konsisten terhadap seluruh aset informasi.
    c. Klasifikasi aset informasi dan seberapa tingkat kerahasiaan aset informasi, didefinisikan sesuai ketentuan peraturan perundang-undangan, diuraikan sebagai berikut:

1) Publik
Aset informasi Publik merupakan aset informasi yang bersifat terbuka dan dapat diakses oleh setiap pengguna informasi publik.
2) Internal
Aset Informasi Internal merupakan aset informasi yang telah terdistribusi secara luas di lingkungan internal instansi/ lembaga yang penyebarannya hanya secara internal dan penyebarannya tidak menimbulkan kerugian signifikan. Contohnya Panduan penggunaan sistem dan aplikasi, kebijakan dan prosedur SMKI, dan dokumen *Business Continuity Plan* (BCP).
3) Rahasia (*Confidential*)
Aset Informasi yang sangat peka dan berisiko tinggi yang pembocoran atau penyalahgunaan akses terhadapnya bisa mengganggu kelancaran operasional secara temporer atau mengganggu citra dan reputasi instansi. Contohnya *user* id, *password*, *Personal Identification Number* (PIN), *log* sistem, hasil *penetration test*, *internet protocol*.

12. Untuk kepentingan penyelenggaraan pengelolaan aset informasi dalam kebijakan SMKI perlu diberikan penjelasan contoh-contoh aset informasi rahasia dan internal, seperti berikut:
    a. rahasia (*confidentiality*), seperti *User* ID, *password*, *Personal Identification Number* (PIN), *log* sistem, hasil *penetration testing*, data konfigurasi sistem, *Internet Protocol*, dan lain-lain.
    b. internal (*internal use only*), seperti panduan penggunaan sistem dan aplikasi, kebijakan dan prosedur SMKI dan lain-lain.
13. Setiap pemilik informasi harus memperhatikan keamanan informasi yang tersimpan dalam media penyimpanan informasi antara lain:
    a. dalam hal data yang tersimpan di dalam media bersifat rahasia, perlu diberikan proteksi kata sandi untuk melindungi data;
    b. dalam hal tidak lagi dibutuhkan atau digunakan, seluruh data yang tersimpan di dalam media harus sepenuhnya dihapus sehingga tidak lagi dapat dipulihkan;
    c. data yang tersimpan di dalam media yang akan dibuang harus mendapatkan perlakuan khusus guna meminimalkan terjadinya kebocoran informasi kepada pihak yang tidak sah, yaitu:
        1) data yang tersimpan di dalam media yang memuat informasi rahasia harus dibuang dengan cara dihancurkan atau dibakar; dan
        2) data yang tersimpan di dalam media yang memuat informasi lainnya harus dilakukan penghapusan total dengan cara-cara tertentu yang tidak lagi dapat dipulihkan.

14. Panduan terkait pelabelan dan penanganan aset informasi berdasarkan klasifikasi aset informasi adalah sebagai berikut:

Klasifikasi Tipe	**Publik**	**Internal**	**Rahasia**
Dokumen dan catatan (*record*) dalam bentuk non elektronik	Tidak diperlukan penanganan khusus	Diberi label "*Internal*"	Diberi label "*Rahasia*"

Klasifikasi Tipe	**Publik**	**Internal**	**Rahasia**
Map penyimpan dokumen	Tidak diperlukan penanganan khusus	Tidak diperlukan penanganan khusus	Diberi label "*Rahasia*"
Amplop pengiriman surat internal (di dalam kantor)	Tidak diperlukan penanganan khusus	Tidak diperlukan penanganan khusus	Amplop diberi label "*Rahasia*"
Amplop pengiriman surat eksternal (ke luar kantor)	Tidak diperlukan penanganan khusus	Pada amplop ditandai "*Internal*"	1. Menggunakan 2 amplop, dimana amplop pertama dimasukkan kedalam amplop kedua; 2. Pada amplop pertama ditandai "*Rahasia*", dan pada amplop kedua ditandai "*Rahasia*".
Dokumen dan catatan (*record*) dalam bentuk elektronik	Tidak diperlukan penanganan khusus	Memberikan label "Internal" pada bagian awal dari nama *file* atau pada bagian tertentu dari *file properties*	Memberikan label "Rahasia" pada bagian awal dari nama *file* atau pada bagian tertentu dari *file properties*
Publikasi/ Distribusi	Tidak ada pembatasan	1. Tersedia untuk personil internal PERANGKAT DAERAH pemilik informasi. 2. Distribusi kepada pihak eksternal dibatasi berdasarkan kebutuhan pekerjaan maupun operasional di lingkungan Pemerintah Daerah Kota Salatiga. 3. Distribusi kepada pihak	1. Distribusi kepada pihak eksternal sangat dibatasi untuk kebutuhan pekerjaan. 2. Apabila memungkinkan, informasi rahasia tidak disalin oleh pihak eksternal (*eyes only*). 3. Distribusi kepada pihak eksternal perlu seizin pemilik Informasi. 4. Sensitivitas dan kritikalitas informasi perlu

Klasifikasi Tipe	Publik	Internal	Rahasia
		eksternal perlu seizin pemilik informasi. 4. Sensitivitas dan kritikalitas informasi perlu diberitahukan kepada pihak eksternal.	diberitahukan kepada pihak eksternal. 5. Pihak ketiga harus disertai perjanjian kerahasiaan (NDA - *non disclosure agreement*).
Pencetakan Informasi	Tidak ada pembatasan	Dibatasi hanya untuk kebutuhan internal	-
Surat menyurat internal (di dalam kantor)	Pastikan nama dan alamat tujuan sudah benar	1. Pastikan nama dan alamat tujuan sudah benar. 2. Mengikuti ketentuan penggunaan amplop untuk surat internal.	1. Pastikan nama dan alamat tujuan sudah benar. 2. Mengikuti ketentuan penggunaan amplop untuk surat internal. 3. Menginformasikan kepada penerima akan pengiriman informasi tersebut. 4. Mengkonfirmasi kepada penerima akan penerimaan informasi tersebut.
Surat menyurat eksternal (ke dalam kantor)	Pastikan nama dan alamat tujuan sudah benar	1. Pastikan nama dan alamat tujuan sudah benar. 2. Mengikuti ketentuan penggunaan amplop untuk surat eksternal. 3. Menggunakan jasa kurir pengiriman tercatat dengan tanda pengiriman.	1. Pastikan nama dan alamat tujuan sudah benar. 2. Mengikuti ketentuan penggunaan amplop untuk surat eksternal. 3. Menggunakan jasa kurir pengiriman tercatat dengan tanda pengiriman. 4. Menginformasikan kepada penerima akan

Klasifikasi Tipe	Publik	Internal	Rahasia
			pengiriman informasi tersebut. 5. Mengkonfirmasi kepada penerima akan penerimaan informasi tersebut.
Pengiriman ke pihak internal melalui *email*	Tidak diperlukan penanganan khusus	1. Pengiriman e-mail harus menggunakan *account* email PERANGKAT DAERAH/ Unit Kerja. 2. Pastikan alamat email tujuan sudah benar. 3. Pengiriman informasi, termasuk *forwarding*/ meneruskan email hanya boleh dilakukan oleh pemilik informasi.	1. Pengiriman e-mail harus menggunakan *account* email PERANGKAT DAERAH/ Unit Kerja. 2. Memberi *password* pada informasi yang dikirim melalui email dan *password* diinformasikan kepada penerima secara terpisah. 3. Tidak mencantumkan informasi rahasia di *body text e- mail*. 4. Pengiriman informasi, termasuk *forwarding*/ meneruskan email hanya boleh dilakukan oleh pemilik informasi.
Pengiriman ke pihak eksternal melalui *email*	1. Pengiriman e-mail harus menggunakan *account* email PERANGKAT DAERAH/ Unit Kerja. 2. Tidak diperlukan penangana	1. Pengiriman e-mail harus menggunakan *account* email PERANGKAT DAERAH/ Unit Kerja. 2. Pastikan alamat email tujuan sudah benar.	1. Tidak disarankan menggunakan e-mail untuk mengirim informasi dengan klasifikasi ini. 2. Pengiriman e-mail harus menggunakan *account* email PERANGKAT DAERAH/ Unit Kerja.

Klasifikasi Tipe	Publik	Internal	Rahasia
	n khusus		3. Memberi *password* pada informasi yang dikirim melalui email dan *password* diinformasikan kepada penerima
Penyimpanan informasi *hardcopy*	Tidak diperlukan penanganan khusus	Tidak diperlukan penanganan khusus	Disimpan secara aman dalam tempat penyimpanan yang terkunci
Penyimpanan informasi *softcopy*	Tidak diperlukan penanganan khusus	Tidak diperlukan penanganan khusus	1. Penyimpanan pada komputer atau media penyimpanan harus yang menggunakan *password*. 2. *File* yang disimpan harus diberi *password*. 3. Media penyimpanan eksternal (*external hard disk*, atau *flashdisk*) harus disimpan pada tempat penyimpanan yang terkunci.
Penyimpanan pada pihak ketiga	Tidak diperlukan penanganan khusus	Harus disertai dengan perjanjian kerahasiaan (*non disclosure agreement* - NDA)	Harus disertai dengan perjanjian kerahasiaan (*non disclosure agreement* - NDA)
Penghancuran (*disposal*)	1. Tidak diperlukan penanganan khusus. 2. Masih dapat digunakan kembali sebagai kertas untuk pekerjaan (*scrap*	1. Memperhatikan masa retensi informasi yang disetujui oleh pemilik informasi. 2. Masih dapat digunakan kembali sebagai kertas untuk pekerjaan (*scrap paper*).	1. Memperhatikan masa retensi informasi yang disetujui oleh pemilik informasi. 2. Dihancurkan dengan metode pemusnahan dan informasi tidak dapat diakses kembali.

Klasifikasi Tipe	Publik	Internal	Rahasia
	paper).		
Pengamanan pada komputer penyimpan informasi	Tidak diperlukan penanganan khusus	1. *Screensaver Lock* harus aktif jika meninggalkan komputer/terminal. 2. *Sign-off* komputer/ terminal kerja.	1. *Screensaver Lock* harus aktif jika meninggalkan komputer/terminal. 2. *Sign-off* komputer/ terminal kerja jika tidak digunakan atau pulang kerja. 3. File perlu di enkripsi / *password*.
Kehilangan atau kebocoran informasi	Tidak diperlukan penanganan khusus	Harus dilaporkan kepada pemilik informasi	Harus dilaporkan kepada pemilik informasi dan unit kerja pengelola insiden keamanan informasi di lingkungan Pemerintah Kota.

15. Informasi yang dianggap kritikal oleh Perangkat Daerah harus di-backup secara memadai untuk menjamin ketersediaannya.
16. Hal yang perlu dipertimbangkan dalam proses *backup* informasi meliputi:
    a. pemilik informasi bertanggung jawab untuk menentukan informasi yang membutuhkan *backup*, frekuensi dan metode backup serta waktu retensi untuk setiap backup informasi yang ada;
    b. pernyataan formal terkait informasi yang dibutuhkan untuk di-*backup* beserta metode dan frekuensi dari *backup* harus ditentukan bersama dengan personil yang bertugas melaksanakan proses *backup* serta harus dinyatakan secara jelas dalam sebuah rencana *backup* resmi;
    c. *backup* informasi harus disimpan sesuai dengan masa retensi dari informasi utama;
    d. masa retensi harus dinyatakan secara jelas dalam rencana *backup*; dan
    e. perlindungan terhadap *backup* informasi harus dilakukan berdasarkan klasifikasi dari informasi utama.
17. Perangkat Daerah menyediakan akses internet dan email kepada pegawainya hanya untuk kebutuhan pekerjaan dan operasional Pemerintah Kota Salatiga.
18. Ketentuan dalam penggunaan internet dan email adalah sebagai berikut:
    a. pengguna dilarang menggunakan akses internet dan email Perangkat Daerah untuk kegiatan melanggar hukum dan aktivitas yang dapat membahayakan keamanan jaringan Pemerintah Kota Salatiga;

b. pengguna dilarang untuk menggunakan akses internet dan email Perangkat Daerah untuk mengakses, mendistribusikan, mengunggah dan/ atau mengunduh:
   1) materi pornografi;
   2) materi bajakan seperti, perangkat lunak, *file* musik dan video/ film;
   3) materi yang melecehkan, mendiskriminasikan, yang membakar emosi atau menimbulkan kebencian atau membuat pernyataan palsu atau yang bersifat merusak mengenai orang lain;
   4) situs yang dapat menimbulkan risiko serangan *malware*, penyusupan atau *hacking* ke jaringan Pemerintah Kota Salatiga.

19. Pengguna disarankan untuk tidak membagi informasi pribadi melalui situs internet atau media sosial.
20. Pengguna dilarang untuk mendistribusikan informasi Pemerintah Kota Salatiga yang bersifat rahasia tanpa izin dari pemilik informasi.
21. Pesan penyangkalan ini harus dituliskan pada akhir setiap e-mail. "*Pesan ini mungkin berisi informasi rahasia dan hanya ditujukan kepada pihak yang dituju. Apabila anda bukanlah pihak yang dituju, anda dilarang untuk mengungkapkan, menyebarkan atau menyalin isi email ini. Apabila anda mendapatkan email ini tanpa sengaja mohon segera hubungi pengirim email dan hapus email ini segera. Pemerintah Kota Salatiga tidak bertanggung jawab untuk pengiriman informasi ini secara lengkap dan tepat dan juga tidak bertanggung jawab untuk keterlambatan dalam pengiriman email ini.*"
22. Dinas Komunikasi Informatika Kota Salatiga yang mengelola akun email Perangkat Daerah berhak untuk mem-*blok* akun *email* Pemerintah Kota Salatiga pada saat terdapat bukti memadai terkait penyalahgunaan dan/ atau pelanggaran keamanan.

BAB V
Pengendalian Akses

A. Tujuan

Tujuan dari kebijakan ini, mencakup:

1. Membatasi akses terhadap informasi serta fasilitas fisik (*data center*);
2. Memastikan sistem dan aplikasi diakses oleh pengguna yang telah diotorisasi, serta mencegah akses oleh yang tidak berhak; dan
3. Memastikan pengguna bertanggung jawab untuk melindungi informasi autentikasi sensitif masing-masing.

B. Ruang Lingkup

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

1. Persyaratan pengendalian akses;
2. Pengendalian akses jaringan;
3. Pengelolaan akses pengguna;
4. Tanggung jawab pengguna; dan
5. Pengendalian akses atas sistem dan aplikasi.

C. Kebijakan

1. Persyaratan Pengendalian Akses pada suatu sistem meliputi:
   a. akses ke aset informasi serta aset pengolahan dan penyimpanan informasi dalam lingkungan Pemerintah Kota Salatiga harus dikendalikan menggunakan metode pengendalian akses yang memadai;
   b. pemberian hak akses dikelola secara formal pada seluruh siklusnya, mulai dari proses pengajuan, persetujuan serta pencabutan, serta dilaksanakan oleh para pihak terkait sesuai jenjang kewenangannya;
   c. pengguna yang mengakses sistem informasi dalam lingkungan Pemerintah Kota Salatiga diharuskan untuk mengautentikasi dirinya dengan menggunakan kombinasi *user* ID dan informasi autentikasi pribadi seperti *password* atau PIN;
   d. pengembangan aturan pemberian akses perlu mempertimbangkan:
      1) klasifikasi dari informasi;
      2) kritikalitas dari aset yang digunakan untuk mendukung operasional bisnis;
      3) prasyarat hukum perundang-undangan, kontraktual serta keamanan yang relevan;
      4) didasarkan atas prinsip *need to know* dan *need to use*, yaitu disesuaikan dengan kebutuhan pekerjaan dan operasional dalam lingkungan Pemerintah Kota Salatiga;
   e. aturan pemberian akses harus dikembangkan dan didokumentasikan oleh setiap pemilik sistem dalam bentuk daftar atau matriks akses;
   f. peninjauan terhadap aturan pemberian akses harus dilakukan oleh pemilik aset/ sistem secara berkala tergantung tingkat kritikalitas sistem tersebut;
   g. peninjauan terhadap hak akses pengguna harus didokumentasikan secara formal; dan
   h. setiap penyimpangan yang ditemukan dalam proses peninjauan harus segera diperbaiki dengan cara menyesuaikan atau mencabut hak akses yang menyimpang.

2. Pengendalian akses jaringan di lingkungan Perangkat Daerah, meliputi:
   a. penggunaan layanan jaringan (*network services*) hanya diperbolehkan secara terbatas, sesuai kebutuhan ketugasan dan kepentingan Perangkat Daerah, layanan lainnya yang tidak diperlukan harus dinonaktifkan;
   b. jaringan komunikasi dalam lingkungan Perangkat Daerah harus dipisahkan kedalam domain jaringan yang terpisah sesuai dengan kebutuhan bisnis dan operasional, dalam rangka untuk mengamankan jaringan internal Perangkat Daerah dan aset di jaringan tersebut;
   c. akses secara *remote* ke jaringan internal Perangkat Daerah dari jaringan publik harus sangat dibatasi baik dari perangkat yang digunakan maupun waktu untuk kebutuhan *troubleshooting* dan harus dilakukan melalui *secure channel*, antara lain dengan menggunakan teknologi VPN; dan
   d. pemberian akses pengguna terhadap jaringan, baik LAN maupun WAN, dilakukan melalui mekanisme formal.
3. Pengelolaan akses terhadap pengguna di Perangkat Daerah harus memenuhi ketentuan sebagai berikut:
   a. pemilik Aset Informasi harus memiliki manajemen identitas pengguna yang mencakup proses pendaftaran dan terminasi pengguna, yang didalamnya termasuk:
      1) identitas pengguna (*user account*) harus unik, melekat ke setiap individu tunggal, sehingga setiap tindakan pengguna dapat dipertanggungjawabkan;
      2) tidak diizinkan menggunakan satu identitas pengguna yang digunakan secara bersama-sama oleh lebih dari satu individu, kecuali untuk tujuan tertentu yang sebelumnya harus mendapatkan persetujuan dari pihak berwenang; dan
      3) memastikan secara berkala bahwa tidak ada identitas pengguna yang terduplikasi atau redundan sehingga seluruh identitas pengguna aktif adalah sesuai dengan pegawai Perangkat Daerah aktif.
   b. pendaftaran, modifikasi dan pencabutan hak akses pengguna mencakup proses pembuatan *user* ID, memberikan hak akses kepada *user* ID serta mencabut hak akses dan *user* ID.
   c. pendaftaran, modifikasi dan pencabutan hak akses pengguna harus disetujui oleh atasan dari pengguna yang memohon hak akses tersebut dan pemilik informasi dan/ atau sistem. Persetujuan tersebut harus diberikan sesuai dengan aturan pemberian akses.
   d. identitas pengguna harus diotorisasi secara formal oleh pejabat berwenang pada pemilik aset informasi. Akses atas sistem dan aplikasi hanya dapat diaktifkan jika proses otorisasi telah selesai.
   e. identitas pengguna pada sistem, seperti *user* ID, harus bersifat unik untuk memungkinkan mengidentifikasi dan meminta pertanggungjawaban pengguna.
   f. pemberian informasi autentikasi suatu pengguna yang bersifat rahasia harus dilakukan melalui proses formal yang mencakup:
      1) informasi autentikasi perdana yang diberikan untuk pertama kalinya adalah bersifat sementara, dimana pengguna wajib menggantinya pada kesempatan pertama mengakses sistem atau aplikasi;
      2) informasi autentikasi bawaan (*default*) dari penyedia barang/ jasa harus segera diganti pada saat instalasi sistem atau aplikasi;

g. pemilik Aset harus melakukan tinjauan secara berkala atas seluruh hak akses pengguna secara berkala, dengan tambahan tinjauan insidental yang dilakukan pada saat:
   1) terjadinya proses kepegawaian, seperti promosi, mutasi, terminasi; dan
   2) terjadinya perubahan struktur organisasi.
h. hak akses khusus (*privileged access rights*) dari sistem informasi dalam lingkungan Perangkat Daerah, seperti administrator, *root*, hak akses untuk memodifikasi database atau hak akses untuk membuat, memodifikasi atau mencabut pengguna dalam sistem aplikasi, harus sangat dibatasi kepada personil yang terotorisasi.
i. Hak akses khusus harus disetujui dan didokumentasikan secara formal.
j. alokasi dari hak akses khusus harus ditinjau secara berkala dan setiap terdapat perubahan dalam status penggunaan akses tersebut.
k. setiap penyimpangan yang ditemukan dalam proses peninjauan harus segera diperbaiki dengan menyesuaikan atau menghapus hak akses khusus yang menyimpang.
l. apabila memungkinkan, hak akses khusus harus dialokasikan secara individual dan tidak di-share. Hal ini dilakukan untuk menjamin akuntabilitas dari pengguna khusus.
m. apabila hak akses khusus tidak bisa dialokasikan secara individual, kontrol tambahan seperti *dual custody*, harus diimplementasikan untuk menghindari penyalahgunaan.
n. jejak audit (*log*) untuk hak akses khusus pada sistem informasi dalam lingkungan Pemerintah Kota Salatiga harus diaktifkan.

4. Setiap pengguna harus mempunyai tanggung jawab dalam penggunaan *User* ID dan *password* yaitu:
   a. pengguna harus menjaga kerahasiaan dan keamanan password pribadi atau kelompok serta informasi autentikasi rahasia lainnya;
   b. pengguna harus segera mengganti informasi autentikasi rahasia jika terindikasi bahwa informasi tersebut telah diketahui oleh orang lain;
   c. *password* yang diberikan untuk pertama kalinya adalah bersifat sementara, dimana pengguna wajib menggantinya pada kesempatan pertama pada saat mengakses sistem atau aplikasi;
   d. *password* untuk mengakses sistem informasi dalam lingkungan Perangkat Daerah harus memiliki karakteristik sebagai berikut:
      1) memiliki panjang minimum 8 karakter;
      2) mengandung kombinasi huruf besar, huruf kecil dan nomor;
      3) tidak terdiri dari kata atau nomor yang mudah ditebak seperti password, admin, 12345678 atau abc123; dan
      4) tidak terdiri dari informasi pribadi seperti ulang tahun pengguna, nama perusahaan atau nama pengguna;
   e. *password* untuk mengakses sistem informasi dalam lingkungan Pemerintah Kota Salatiga harus diganti paling sedikit setiap 3 (tiga) bulan sekali;
   f. pada saat penggantian, *password* sebelumnya tidak boleh digunakan kembali sampai setelah 3 siklus pergantian *password*;
   g. prosedur login dari sistem harus menjamin keamanan dari *password* dengan cara:
      1) tidak menampilkan *password* yang dimasukkan;
      2) tidak menyediakan pesan bantuan pada saat proses login yang dapat membantu pengguna yang tidak berwenang;
   h. pengguna wajib menggunakan kata sandi yang berbeda untuk keperluan ketugasan dan pribadi.

5. Pengendalian akses sistem dan aplikasi yang dikelola oleh Perangkat Daerah meliputi:
   a. pemilik aset informasi harus memastikan bahwa sistem dan aplikasi dibawah pengelolaannya memiliki fasilitas manajemen hak akses pengguna, manajemen kata sandi yang baik, serta mekanisme autentikasi pengguna yang aman;
   b. fasilitas manajemen hak akses pengguna harus mampu membatasi akses informasi sesuai ketugasannya (*role based access control*);
   c. Hak akses untuk kebutuhan audit harus dibatasi hanya hak akses *read only*;
   d. fasilitas manajemen kata sandi harus memastikan dihasilkannya kata sandi yang berkualitas, yaitu:
      1) menegakkan akuntabilitas pengguna melalui penggunaan identitas pengguna tunggal untuk setiap individu;
      2) memberikan fasilitas penggantian kata sandi mandiri;
      3) membantu memberikan rekomendasi kata sandi yang berkualitas;
      4) mewajibkan pengguna untuk mengganti kata sandi pada saat pertama kali *login*;
      5) mewajibkan pengguna untuk mengganti kata sandi secara berkala;
      6) menyimpan riwayat kata sandi pengguna dan mencegah agar pengguna tidak menggunakan kata sandi yang sebelumnya telah digunakan;
      7) tidak menampilkan kata sandi saat sedang dientrikan; dan
      8) kata sandi disimpan dalam bentuk terlindungi (dienkripsi), demikian juga pada saat kata sandi ditransmisikan.
   e. mekanisme autentikasi pengguna perlu dirancang agar meminimalkan peluang terjadinya akses yang tidak sah, yaitu:
      1) kata sandi tidak ditransmisikan melalui jaringan secara *plaintext*;
      2) memiliki mekanisme penguncian sistem sementara sebagai perlindungan terhadap *brute force attacks*;
      3) adanya pencatatan terhadap seluruh upaya autentikasi yang sukses dan gagal;
      4) adanya pembatasan jumlah akses pengguna yang sama secara simultan;
   f. Parameter autentikasi pengguna disesuaikan dengan klasifikasi aset informasi sebagai berikut:

Parameter autentikasi	**Rahasia & Internal**	**Publik**
Jumlah gagal *login* sebelum	3 kali	10 kali
Durasi *timeout* sebelum	5 menit	16 menit

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

7. Perangkat Daerah yang mengelola aplikasi harus memastikan bahwa *source code* dikelola dan disimpan secara memadai baik yang dikembangkan oleh internal Perangkat Daerah maupun yang dikembangkan oleh penyedia jasa aplikasi.
8. Apabila *source code* dari penyedia jasa aplikasi tidak dapat diserahkan kepada pengelola aplikasi, Perangkat Daerah bersama penyedia jasa aplikasi tersebut harus mempertimbangkan *escrow agreement* untuk memastikan kelangsungan operasional sistem aplikasi jika ada pengembangan selanjutnya.
9. Pengendalian terhadap akses ke *source code* aplikasi sebagai berikut:
   a. Untuk sistem aplikasi yang dikembangkan secara internal dan/ atau dibeli dengan *source code*, pengendalian akses harus diimplementasikan untuk mencegah akses tanpa izin ke *source code* tersebut.
   b. Pengendalian tersebut mencakup:
      1) Tidak menyimpan *source code* pada sistem operasional;
      2) Menyimpan *source code* pada lokasi fisik yang aman dari ancaman akses tanpa izin maupun ancaman kerusakan karena kondisi lingkungan;
      3) Membatasi akses secara fisik maupun *logical* ke *source code* program hanya kepada pengembang dan personil yang berwenang;
      4) Mengimplementasikan metode *versioning* dan proses manajemen perubahan untuk menjamin integritas dari *source code* aplikasi.

BAB VI
Keamanan Fisik dan Lingkungan

A. Tujuan

Tujuan dari kebijakan keamanan fisik dan lingkungan, diantaranya adalah untuk:

1. Mencegah akses atas aset informasi dan aset pengolahan dan penyimpanan informasi secara fisik oleh pihak yang tidak berwenang pada lingkungan Pemerintah Kota Salatiga; dan
2. Mencegah terjadinya kerusakan atau gangguan pada aset informasi dan aset pengolahan dan penyimpanan informasi pada lingkungan Pemerintah Kota Salatiga.

B. Ruang Lingkup

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

C. Kebijakan

1. Setiap area yang didalamnya terdapat informasi dan fasilitas pengolahan informasi Perangkat Daerah harus dilindungi dengan menerapkan pengamanan fisik pada perimeter area tersebut.
2. Setiap area harus merupakan akses terbatas, dimana akses masuk hanya diberikan bagi personil yang telah mendapatkan otorisasi. Mekanisme pembatasan ini dapat dilakukan aturan penerimaan tamu yang diterapkan berdasarkan kritikalitas area tersebut.
3. Untuk area *Data center*, *disaster recovery center* dan ruang arsip Perangkat Daerah harus dilindungi dengan menerapkan pengamanan fisik pada perimeter area tersebut dengan kriteria:
   a. konstruksi dinding, atap dan lantai yang kuat;
   b. pintu akses menuju area harus dilengkapi dengan mekanisme kontrol akses, seperti: *access door lock*;
   c. pintu dan jendela harus senantiasa dalam kondisi terkunci, khususnya pada saat tanpa penjagaan;
   d. perangkat CCTV perlu terpasang pada sisi eksterior dan interior area;
   e. tidak diperbolehkan menyimpan bahan-bahan berbahaya yang mudah terbakar;
   f. area bongkar muat atau penerimaan barang harus diamankan dan dipantau untuk mencegah akses tanpa izin ke *data center*, *disaster recovery center* dan ruang arsip Pemerintah Kota Salatiga; dan
   g. delivery dari barang harus dilaporkan dan diperiksa sebelum barang tersebut dapat dipindahkan dari area bongkar muat atau penerimaan barang ke *data center*, *disaster recovery center* dan ruang arsip Pemerintah Kota Salatiga.
4. Pengendalian akses pengunjung ke dalam area di lingkungan Perangkat Daerah harus memperhatikan keamanan fisik yang meliputi:
   a. kunjungan ke dalam area tersebut harus disetujui secara formal oleh pengelolaan area tersebut;
   b. selama kunjungan di dalam area tersebut, pengunjung harus senantiasa didampingi oleh petugas yang telah mendapatkan otorisasi;
   c. kartu identitas pengunjung perlu diverifikasi, disimpan oleh petugas selama kunjungan, dan dikembalikan sesudah selesai kunjungan; dan

d. setiap pengunjung ke dalam area harus tercatat, mencakup jam masuk dan keluar, serta selalu dimonitor kesesuaiannya dengan rekaman CCTV.

5. Perangkat Daerah harus memperhatikan aspek pengamanan terhadap perangkat yang digunakan melalui:
   a. seluruh perangkat harus ditempatkan di lokasi yang aman, sedemikian rupa sehingga terlindungi dari terjadinya pencurian, akses oleh pihak yang tidak berwenang, kebakaran, air, debu, dan sebagainya;
   b. seluruh perangkat di dalam area harus dipelihara, diinspeksi sesuai spesifikasi perawatan berkala oleh pihak yang berwenang untuk menjamin keberlangsungan efektivitas fungsionalnya;
   c. pemeliharaan yang dilakukan oleh pihak ketiga, harus dilaksanakan sesuai dengan kesepakatan tingkat layanan (*service level agreement*/ SLA) yang menjabarkan tingkat pemeliharaan dan kinerja yang harus dipenuhi pihak ketiga;
   d. bagi pemeliharaan yang tidak dapat dilakukan di lokasi kantor Perangkat Daerah, maka informasi rahasia dan kritikal yang tersimpan dalam peralatan tersebut harus dipindahkan terlebih dahulu;
   e. pemeliharaan perangkat yang mengharuskan dibawa dari luar area harus atas persetujuan pejabat berwenang.
   f. peralatan pengolahan dan penyimpanan informasi yang tidak digunakan lagi oleh Pemerintah Kota Salatiga, baik karena rusak, diganti, atau karena sebab lainnya harus dipastikan tidak lagi menyimpan informasi sensitif dan kritikal; dan
   g. media penyimpan informasi yang sudah tidak digunakan lagi harus dihancurkan, atau dihapus isinya agar tidak bisa dibaca dan digunakan lagi oleh pihak yang tidak berwenang.

6. Khusus pengamanan area fisik di *data center* harus mempertimbangkan hal-hal sebagai berikut:
   a. seluruh perangkat harus ditempatkan di lokasi yang aman, sedemikian rupa sehingga terlindungi dari terjadinya kebakaran, kebocoran, debu, dan sebagainya;
   b. seluruh perangkat di dalam *data center* harus dipelihara, diinspeksi sesuai spesifikasi perawatan berkala oleh pihak yang kompeten dan berwenang sesuai dengan rekomendasi dari pembuat perangkat tersebut;
   c. *data center* harus dilengkapi dengan UPS (*Uninterruptible Power Supply*), generator listrik cadangan, perangkat pemadam kebakaran, dan diusahakan terdapat perlindungan kejut listrik (petir, tegangan tidak stabil);
   d. *data center* dan *disaster recovery center* dilengkapi dengan sistem sensor deteksi asap, air, suhu dan kelembaban, yang dapat terpantau;
   e. parameter temperatur dan kelembaban berikut perlu dijaga untuk data center meliputi:
      1) temperatur antara 18° - 26° celcius;
      2) kelembaban (rh) antara 40% - 60%.
   f. kabel listrik dan jaringan telekomunikasi yang membawa data atau mendukung layanan sistem informasi harus dilindungi dari penyambungan yang tidak sah (penyadapan) atau kerusakan.

BAB VII
Keamanan Operasional Sistem Informasi

A. Tujuan

Tujuan dari kebijakan keamanan operasional sistem informasi adalah untuk:

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

B. Ruang Lingkup

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

C. Kebijakan

1. Aktivitas operasional terkait fasilitas pengolahan informasi serta fasilitas komunikasi harus memiliki prosedur yang terdokumentasi dengan baik;
2. Prosedur operasional tersebut harus tersedia bagi pengguna yang memerlukannya;
3. Seluruh perubahan pada fasilitas pengolahan informasi yang dapat berimplikasi pada keamanan informasi, perlu diperlakukan secara terkendali, mencakup antara lain:
   a. menyusun perencanaan mengenai perubahan yang mungkin terjadi serta melakukan pengujian terkait terpenuhinya persyaratan keamanan;
   b. melakukan kajian atas implikasi keamanan informasi yang mungkin terjadi;
   c. mengajukan persetujuan secara formal atas perubahan yang akan dilakukan; dan
   d. mencatat seluruh perubahan yang telah dilakukan.
4. kinerja dan utilisasi atas fasilitas pengolahan informasi harus senantiasa dipantau dengan alat bantu peringatan dini, dioptimalkan pemanfaatannya, serta diproyeksikan kebutuhan kapasitasnya untuk masa yang akan datang.
5. untuk mengurangi risiko perubahan tanpa izin atau penyalahgunaan hak akses, pemisahan fasilitas pengembangan, pengujian, dan operasional harus dilakukan.
6. setiap sistem informasi di lingkungan Perangkat Daerah harus terlindungi dari *malware* secara memadai melalui:
   a. instalasi dari perangkat lunak *antivirus* pada sistem informasi;
   b. memblok akses ke *website* yang dapat menimbulkan ancaman kepada sistem informasi;
   c. program peningkatan kesadaran bagi personil organisasi untuk menangani ancaman *malware*; dan
   d. setiap insiden terkait dengan *malware* harus dilaporkan kepada administrator sistem dan dikategorikan sebagai insiden keamanan informasi.

7. seluruh aset informasi yang berada di dalam fasilitas pengolahan informasi wajib dilakukan *backup*, dengan persyaratan berikut:
   a. *backup* mencakup aplikasi, *database*, dan *system image*;
   b. frekuensi *backup* dilakukan secara harian, bulanan, dan tahunan;
   c. salinan *backup* harus disimpan secara aman sesuai dengan periode retensi. periode retensi *backup* adalah 1 tahun, dimana:
      1) *backup* harian disimpan selama 31 hari;
      2) *backup* bulanan disimpan selama 12 bulan;
   d. seluruh hasil *backup* harus dilakukan uji *restore* secara berkala;
   e. media *backup* disimpan pada perangkat *storage* yang terpisah dari perangkat pengolahan informasi utama;
   f. *backup* merupakan tanggung jawab pengelola *data center*, sedangkan pengujian *restore* merupakan tanggung jawab pemilik aset informasi;
   g. parameter *backup* disesuaikan dengan klasifikasi sistem sebagai berikut:

Parameter Backup	**Klasifikasi Sistem**	
	Vital	***Sensitive/ Non-Sensitive***
Cakupan *Backup*	Aplikasi, *Database*	Aplikasi, *Database*
Frekuensi *Backup* (*Recovery Point*)	Harian	Bulanan
Pengujian *Restore*	Triwulanan	Semesteran

8. sistem harus dikonfigurasi untuk melakukan pencatatan (*logging*) atas seluruh aktivitas pengguna, jaringan, sistem, aplikasi, *error* yang terjadi (*exceptions*). Pemilik aset informasi harus menganalisis *log* terkait pola-pola penggunaan yang tidak wajar.
9. fasilitas pencatatan *log* dan informasi *log* yang dicatat harus dilindungi dari penghapusan dan akses oleh pihak yang tidak berwenang.
10. semua fasilitas pemrosesan informasi yang terhubung ke jaringan internal Perangkat Daerah harus di sinkronisasi dengan sumber waktu yang akurat dan telah disepakati.
11. proses dan prosedur untuk mengendalikan instalasi perangkat lunak pada sistem operasional harus ditetapkan dan diimplementasikan untuk memastikan terjaganya kerahasiaan, integritas dan ketersediaan informasi.
12. instalasi *software* harus dilakukan oleh administrator sistem yang relevan.
13. pemilik aset informasi wajib melakukan upaya-upaya identifikasi atas kelemahan teknis (*vulnerabilities*) dari seluruh aset informasi dibawah pengelolaannya, serta melakukan tindakan pengendalian yang sesuai untuk meminimalkan resiko atas hilangnya aset informasi. Tindakan pengendalian dapat berupa penonaktifan fitur tertentu, perbaikan/ *upgrade* sistem, aplikasi, atau *patching*.
14. setiap sistem informasi di lingkungan Perangkat Daerah dapat dilakukan proses audit yang mencakup proses verifikasi terhadap sistem informasi dan/ atau informasi Perangkat Daerah dengan mempertimbangkan sebagai berikut:
    a. harus direncanakan dan dikelola dengan baik untuk meminimalisasi gangguan terhadap proses bisnis;

b. setiap proses audit yang membutuhkan akses kepada sistem informasi dan/ atau informasi Perangkat Daerah harus disetujui oleh pemilik dari sistem dan/ atau informasi tersebut;
c. hak akses untuk kebutuhan audit harus dibatasi hanya hak akses *read only*; dan
d. instalasi dari *tools* yang digunakan untuk proses audit hanya dapat dilakukan oleh personil yang berwenang yaitu administrator jaringan dan sistem TI di Perangkat Daerah, dan harus segera dihapus setelah proses audit telah selesai dilakukan.

BAB VIII
Keamanan Komunikasi

A. Tujuan

Tujuan dari kebijakan keamanan komunikasi, antara lain untuk:

1. Memastikan perlindungan atas informasi pada jaringan komunikasi beserta fasilitas pendukung pengolahan informasi; dan
2. Menjaga keamanan informasi yang dipertukarkan, baik di dalam OPD maupun di luar OPD.

B. Ruang Lingkup

Ruang lingkup dari kebijakan keamanan komunikasi antara lain untuk:

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

C. Kebijakan

1. Jaringan internal Perangkat Daerah harus diamankan untuk menjamin:
   a. pencegahan akses tanpa izin ke jaringan, layanan jaringan dan fasilitas pemrosesan informasi dalam jaringan;
   b. keamanan dari informasi milik organisasi yang dikirimkan melalui jaringan; dan
   c. integritas dan ketersediaan dari layanan jaringan organisasi.
2. Tugas dan tanggung jawab untuk pengelolaan jaringan dan keamanan harus dialokasikan dan apabila memungkinkan dipisahkan dari penanggung jawab operasional sistem aplikasi dan *data center*.
3. Konfigurasi dari jaringan, perangkat aktif dan perangkat keamanan jaringan harus ditinjau secara berkala untuk:
   a. memastikan kesesuaian dengan kondisi terkini; dan
   b. mengidentifikasi kerawanan pada jaringan, layanan jaringan dan fasilitas pemrosesan informasi dalam jaringan.
4. Jaringan internal Perangkat Daerah harus dipisahkan dari jaringan eksternal dengan menggunakan *security gateway* atau *firewall* dan harus dikonfigurasikan untuk:
   a. memfilter *traffic* tanpa izin maupun *traffic* yang mencurigakan; dan
   b. apabila memungkinkan memfilter dan mencegah infeksi malware ke jaringan internal;
5. Koneksi ke *security gateway* atau firewall harus di autentikasikan, diotorisasi dan diamankan dengan metode pengamanan yang sesuai, misalnya dengan *virtual private network* (VPN), *secure shell* (SSH) atau metode kriptografi.
6. Kebijakan dan *log firewall* harus ditinjau paling sedikit 1 (satu) kali dalam tiga bulan.
7. Koneksi eksternal harus diputuskan secara otomatis setelah tidak aktif selama 5 menit.
8. Akses dari jaringan eksternal yang dilakukan oleh vendor pihak ketiga hanya dapat diberikan untuk kebutuhan *troubleshooting* dan harus secara formal disetujui dan didokumentasikan dan harus dibatasi waktunya sesuai dengan kebutuhan dari akses.
9. Jaringan internal perusahaan harus disegmentasi baik secara fisik maupun *logical* untuk meningkatkan keamanan dan untuk mengendalikan akses dan *traffic* jaringan berdasarkan kritikalitas dari sistem dalam jaringan Perangkat Daerah.

10. Segmentasi jaringan harus ditinjau paling sedikit 1 (satu) kali dalam tiga bulan untuk menjamin kesesuaian dengan prasyarat keamanan terkini.
11. *Routing* jaringan harus dilakukan berdasarkan pengendalian terhadap alamat sumber dan tujuan.
12. Tanggung jawab untuk merubah *routing* jaringan hanya diberikan kepada administrator jaringan yang diberi izin.
13. Aturan untuk *routing* harus ditinjau paling tidak satu kali dalam tiga bulan untuk mendeteksi dan mengoreksi adanya kesalahan atau routing tanpa otorisasi.
14. Perangkat jaringan harus ditempatkan pada lokasi yang aman untuk menghindari akses tanpa izin dan ancaman fisik maupun lingkungan.
15. Akses, baik fisik maupun *logical* ke perangkat jaringan harus dibatasi untuk tujuan administrasi dan pemeliharaan jaringan.
16. *Port* dan layanan jaringan, baik fisik maupun logical, yang tidak digunakan tidak boleh diaktifkan.
17. Akses ke *port* yang digunakan untuk kebutuhan diagnostic dan konfigurasi perangkat jaringan dan keamanan jaringan, seperti *console port*, harus sangat dibatasi dan diberikan kepada:
    a. administrator jaringan dan keamanan jaringan Perangkat Daerah;
    b. pihak ketiga yang telah disetujui dan bekerja untuk kepentingan Perangkat Daerah;
    c. aplikasi monitoring jaringan dan keamanan jaringan yang telah disetujui.
18. Semua perangkat jaringan harus dapat diidentifikasi secara fisik maupun *logical* dengan penamaan yang disepakati dan konsisten.
19. Perangkat jaringan yang dimiliki oleh pihak eksternal harus secara memadai dipisahkan dari perangkat jaringan milik Perangkat Daerah.
20. Mekanisme keamanan, tingkat layanan dan prasyarat lain untuk semua layanan jaringan harus diidentifikasi dan dimasukkan kedalam perjanjian layanan jaringan.
21. Akses ke layanan jaringan Perangkat Daerah hanya diberikan kepada personil yang terotorisasi berdasarkan prinsip *need to have*.
22. Penggunaan pihak ketiga penyedia layanan jaringan harus dimonitor untuk menjamin kesesuaian dengan prasyarat keamanan Perangkat Daerah.
23. Layanan jaringan organisasi harus diamankan menggunakan metode yang dapat mencakup metode autentikasi atau metode kriptografi yang kuat untuk menjamin keamanan dari pengiriman informasi menggunakan jaringan dan layanan jaringan.
24. Terkait aspek pertukaran informasi melalui fasilitas jaringan komunikasi, Perangkat Daerah harus memperhatikan perjanjian kerahasiaan merupakan perikatan formal antara pemilik aset informasi dengan penerima informasi, yang ketentuan di dalamnya memuat:
    a. pemberian izin penggunaan informasi dari pemilik aset informasi kepada penerima informasi untuk keperluan dan periode waktu yang spesifik, dimana pihak penerima informasi wajib menjaga kerahasiaan informasi serta mengupayakan pencegahan terjadinya kebocoran atau penyebaran informasi secara tidak sah;
    b. hak dari pemilik aset informasi untuk melakukan audit dan pemantauan aktivitas penerima informasi berkaitan dengan penggunaan informasi sensitif; dan
    c. konsekuensi yang harus ditanggung penerima informasi apabila terjadi pelanggaran atas perjanjian kerahasiaan.

BAB IX
Akuisisi, Pengembangan dan Pemeliharaan Sistem

A. Tujuan

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

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

B. Ruang Lingkup

Ruang lingkup dari kebijakan akuisisi, pengembangan dan pemeliharaan sistem adalah untuk:

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

C. Kebijakan

1. Perangkat Daerah Kerja harus menetapkan dan mendokumentasikan secara jelas persyaratan keamanan informasi yang relevan sebelum pengembangan, perluasan, atau pengadaan sistem informasi baru.
2. Persyaratan keamanan harus diidentifikasi secara jelas di dalam dokumen persyaratan dan spesifikasi perangkat lunak (*Software Requirement and Specification*).
3. Spesifikasi ini harus disetujui oleh pemilik informasi, pemilik proses bisnis dan pengembang sistem, sebelum fase pengkodean (*coding*) dalam pengembangan sistem.
4. Informasi yang digunakan oleh aplikasi Perangkat Daerah yang ditransmisikan melalui jaringan publik (internet) harus diamankan dari aktivitas penipuan, kemungkinan adanya perselisihan kontrak, dan pengungkapan dan/ atau perubahan informasi tanpa izin.
5. Pengamanan informasi terhadap informasi yang ditransmisikan melalui sistem informasi yang digunakan dapat mencakup namun tidak terbatas pada:
   a. Proses autentikasi dan otorisasi terhadap pengguna aplikasi;
   b. Perlindungan untuk memastikan kerahasiaan dan integritas informasi yang dipertukarkan melalui jaringan publik;
   c. Perlindungan terhadap session transaksi untuk menghindari duplikasi dan/atau modifikasi;
   d. Mengamankan jalur komunikasi antara pihak-pihak yang terlibat
6. Keamanan dalam proses pengembangan dan dukungan yang perlu dipertimbangkan oleh Perangkat Daerah meliputi:
   a. aturan untuk pengembangan sistem harus ditetapkan dan diimplementasikan untuk proses pengembangan sistem di Perangkat Daerah yang mencakup:
      1) pengamanan dari lingkungan pengembangan, seperti pemisahan lingkungan pengembangan baik secara fisik dan/ atau *logical*, pengendalian akses, pengelolaan perubahan;
      2) panduan secure *coding*;
      3) pengendalian versi aplikasi;
      4) penyimpanan dari *source code*;
      5) metode pengujian untuk mengidentifikasi dan memperbaiki *vulnerability*.

7. Perubahan terhadap sistem selama siklus pengembangan sistem harus dikendalikan melalui proses manajemen perubahan yang berlaku di Perangkat Daerah;
8. Apabila platform operasional, misalnya sistem operasi, *database* dan/ atau middleware, dari sistem informasi Perangkat Daerah mengalami perubahan, aplikasi kritikal Perangkat Daerah harus ditinjau dan diuji untuk memastikan tidak ada dampak buruk terhadap operasional dan keamanan organisasi;
9. Perangkat Daerah harus menetapkan lingkungan pengembangan yang aman untuk pengembangan dan integrasi sistem Perangkat Daerah. Hal ini dapat mencakup namun tidak terbatas pada:
   a. Pemisahan lingkungan pengembangan baik secara fisik dan/ atau *logical*;
   b. Pengendalian akses; dan
   c. Perpindahan data dari dan ke lingkungan pengembangan.
10. Perangkat Daerah harus mengawasi aktivitas pengembangan sistem yang dialihdayakan (*outsourced*). Hal ini dapat mencakup:
    a. perjanjian terkait lisensi dan kepemilikan sistem;
    b. pengujian penerimaan sistem untuk menguji kualitas dan akurasi dari sistem;
    c. prasyarat dokumentasi untuk sistem;
    d. perjanjian dengan pihak ketiga sebagai penjamin;
    e. hak untuk melakukan audit proses pengembangan dan kontrol yang diimplementasikan oleh vendor.
11. Pengujian dari fitur keamanan sistem harus dilakukan pada saat pengembangan sistem informasi Perangkat Daerah;
12. Pengujian ini dilakukan berdasarkan prasyarat keamanan sistem yang telah ditetapkan;
13. Kriteria dan jadwal untuk pengujian penerimaan sistem harus ditetapkan untuk sistem informasi baru, *upgrade* dan versi baru dari sistem informasi Perangkat Daerah;
14. Pengujian penerimaan sistem harus dilakukan sesuai dengan kriteria dan jadwal yang ditetapkan.
15. Pengamanan terhadap data hasil pengujian perlu diperhatikan sebagai berikut:
    a. data untuk pengujian sistem harus dipilih secara hati-hati untuk menghindari pengungkapan atau perubahan informasi sensitif oleh pihak yang tidak berhak, serta melindung dari kemungkinan kerusakan dan kehilangan informasi;
    b. *masking data* harus dilakukan apabila data operasional yang sensitif digunakan untuk keperluan pengujian;
    c. data operasional yang digunakan untuk keperluan pengujian harus dihapus segera setelah proses pengujian telah selesai dilaksanakan.

BAB X
Hubungan Kerja dengan Pemasok (Supplier)

A. Tujuan

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

B. Ruang Lingkup

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

C. Kebijakan

1. Perangkat Daerah harus mempertimbangkan aspek keamanan informasi dalam hubungan dengan pemasok mulai dari pemilihan, penunjukan, monitoring, evaluasi, sampai dengan terminasi.
2. Pemilihan dari penyedia jasa Perangkat Daerah harus mengikuti kriteria berikut:
   a. kompetensi, pengalaman dan catatan dari organisasi;
   b. kepastian dari kemampuan penyedia jasa untuk menyediakan layanan; dan
   c. kepastian dari kemampuan penyedia jasa untuk menjaga ketersediaan dari penyediaan layanan pada saat kondisi normal atau kondisi bencana (apabila terjadi bencana alam atau kegagalan dalam penyediaan layanan).
3. Berdasarkan pengelompokan pemasok yang telah bekerjasama, Perangkat Daerah wajib mendefinisikan pembatasan aset dan aset informasi apa saja yang diperbolehkan untuk diakses oleh setiap kelompok pemasok, serta senantiasa memantau akses yang telah dilakukan.
4. Perangkat Daerah menetapkan persyaratan keamanan informasi bagi setiap pemasok yang mengakses aset informasi, serta senantiasa memantau kepatuhan pemasok terhadap persyaratan tersebut. Pemasok yang menangani aset informasi dengan klasifikasi rahasia perlu menandatangani Perjanjian Kerahasiaan.
5. Kewajiban supplier dan tingkat layanan harus ditetapkan secara formal dalam kontrak kerja;
6. Perangkat Daerah harus memastikan pengelolaan delivery layanan dari pemasok dengan memperhatikan:
   a. layanan yang diserahkan kepada Perangkat Daerah oleh pihak supplier harus secara berkala dipantau, dan ditinjau;
   b. proses pemantauan dilakukan untuk memverifikasi kesesuaian dari tingkat layanan yang diberikan dan prasyarat keamanan informasi dengan perjanjian kerja;
   c. proses peninjauan dilakukan untuk mengidentifikasi problem terkait penyediaan layanan dan aspek keamanan informasi dalam penyediaan layanan oleh supplier; dan
   d. peninjauan dari penyediaan layanan oleh supplier harus dilaksanakan paling sedikit satu kali dalam tiga bulan.
7. Perangkat Daerah dapat melakukan audit terhadap penyediaan layanan yang diberikan pemasok;
8. Ketentuan dalam pelaksanaan audit kepada pemasok sebagai berikut:
   a. tanggung jawab untuk mengaudit tingkat layanan dimiliki oleh pihak, baik internal maupun eksternal, yang memiliki independensi dari pengguna layanan yang diberikan oleh supplier dan ditunjuk secara formal;

b. audit terhadap penyediaan layanan oleh supplier harus dilakukan paling sedikit satu kali dalam satu tahun; dan
c. setiap ketidaksesuaian yang ditemukan dalam proses peninjauan dan audit harus dikelola dan ditindaklanjuti.

9. Perubahan terhadap layanan yang diberikan oleh supplier harus dikelola, dengan memperhatikan kritikalitas dari proses bisnis pengguna layanan dan layanan yang diberikan oleh supplier;
10. Perubahan terhadap layanan yang diberikan oleh supplier harus dipastikan tidak akan mengganggu aspek kerahasiaan dari informasi Perangkat Daerah serta integritas dan ketersediaan dari informasi dan layanan Perangkat Daerah;
11. Perubahan terhadap layanan yang diberikan oleh supplier harus disetujui oleh manajemen Perangkat Daerah yang relevan dan diformalisasikan dalam kontrak kerja.

BAB XI
Penanganan Insiden Keamanan Informasi

A. Tujuan

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

B. Ruang Lingkup

Ruang lingkup dari kebijakan penanganan insiden keamanan informasi, adalah:

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

C. Kebijakan

1. Kejadian keamanan informasi adalah sebuah kejadian pada sistem, layanan ataupun jaringan yang dapat mengindikasikan adanya pelanggaran keamanan informasi atau kegagalan keamanan atau kejadian yang mungkin memiliki keterkaitan dengan keamanan informasi.
2. Kelemahan keamanan informasi adalah sebuah kelemahan yang teridentifikasi pada sistem, layanan atau jaringan yang dapat dieksploitasi oleh pihak yang tidak bertanggung jawab dan dapat menyebabkan pelanggaran terhadap kebijakan keamanan informasi.
3. Insiden keamanan informasi adalah kejadian keamanan informasi yang tidak diinginkan dan tidak diperkirakan dimana kejadian tersebut menimbulkan gangguan terhadap operasional bisnis dan mengancam keamanan informasi.
4. Guna memastikan proses penanganan insiden yang responsif dan efektif, perlu dikembangkan berbagai prosedur yang mencakup:
   a. perencanaan dan persiapan penanganan insiden;
   b. pemantauan, analisis, dan pelaporan atas insiden;
   c. pencatatan atas aktivitas penanganan insiden;
   d. penanganan bukti forensik;
   e. penilaian dan pengambilan keputusan atas insiden dan kelemahan keamanan informasi; dan
   f. pemulihan insiden.
5. Seluruh pegawai dan pihak ketiga wajib melaporkan berbagai kejadian insiden keamanan informasi maupun yang masih bersifat dugaan atas kelemahan keamanan informasi sesegera mungkin, sesuai prosedur pelaporan insiden yang berlaku.
6. Setiap kejadian insiden keamanan informasi harus dianalisis, diklasifikasikan, dan ditentukan skala prioritas penanganannya. Penanganan insiden serta pemulihannya dilakukan berdasarkan klasifikasi dan prioritas yang telah ditetapkan.
7. Perangkat Daerah harus mengklasifikasikan insiden keamanan informasi untuk memprioritaskan penanganan insiden. Klasifikasi insiden tersebut adalah sebagai berikut:
   a. insiden keamanan informasi diklasifikasikan berdasarkan dampaknya menjadi berikut:
      1) mayor, apabila insiden tersebut menyebabkan terhentinya proses operasional pekerjaan Perangkat Daerah;
      2) minor, apabila insiden tersebut menyebabkan gangguan yang tidak menghentikan proses operasional pekerjaan Perangkat Daerah.

b. insiden keamanan informasi diklasifikasikan berdasarkan tingkat kepentingannya menjadi berikut:
   1) *emergency*, apabila insiden tersebut dapat atau telah menghentikan proses operasional Perangkat Daerah dan/ atau insiden tersebut mempengaruhi secara langsung pimpinan dalam lingkungan Perangkat Daerah;
   2) *normal*, apabila insiden tersebut insiden tersebut tidak menghentikan proses operasional Perangkat Daerah dan/ atau insiden tersebut mempengaruhi secara langsung pimpinan dalam lingkungan Perangkat Daerah.

8. Setiap insiden keamanan informasi harus ditangani dengan baik untuk mencegah meluasnya insiden, untuk memulihkan layanan atau informasi yang mungkin hilang dan untuk meminimalisasi dampak dari insiden.
9. Setiap tindakan yang diidentifikasi untuk menangani kejadian, kelemahan dan insiden keamanan informasi harus dikonsultasikan kepada koordinator CSIRT (*Cyber Security Incident Response Team*) dan/ atau personil yang kompeten dan relevan dengan kejadian, kelemahan dan insiden keamanan informasi.
10. Setiap tindakan penanganan kejadian, kelemahan dan insiden keamanan informasi harus didokumentasikan dengan baik

BAB XII
Kelangsungan Usaha (Business Continuity)

A. Tujuan

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

B. Ruang Lingkup

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

1. Keberlanjutan keamanan informasi; dan
2. Redundansi fasilitas pengolahan informasi.

C. Kebijakan

1. Perangkat Daerah harus menetapkan, mendokumentasikan, mengimplementasikan dan memelihara proses, prosedur dan kontrol yang diperlukan untuk menjamin keberlanjutan keamanan informasi sesuai prasyarat yang telah ditetapkan pada saat dan setelah terjadinya gangguan besar atau bencana.
2. Perangkat Daerah harus memverifikasi kontrol keberlanjutan keamanan informasi yang telah ditetapkan dan diimplementasikan secara berkala untuk menjamin kesesuaian dan efektivitasnya pada saat dan setelah terjadinya gangguan besar atau bencana.
3. Perangkat Daerah harus menetapkan prasyarat untuk keberlanjutan keamanan informasi dan diintegrasikan dengan prasyarat keberlanjutan bisnis organisasi untuk menjamin keberlanjutan dari keamanan informasi di Perangkat Daerah, pada saat dan setelah terjadinya gangguan besar atau bencana.
4. Prasyarat keamanan informasi dapat diintegrasikan pada siklus proses *business continuity management* (BCM) yang mencakup:
   a. memahami kebutuhan organisasi;
   b. menentukan strategi BCM;
   c. mengembangkan dan mengimplementasikan rencana penanggulangan/ keberlanjutan bisnis; dan
   d. pengujian, pemeliharaan dan peninjauan rencana penanggulangan/ keberlanjutan bisnis.
4. Aspek redundansi harus ditetapkan untuk fasilitas pengolahan informasi dan sarana pendukungnya untuk memastikan ketersediaan dari proses bisnis dan operasional Perangkat Daerah serta pemberian layanan Perangkat Daerah kepada pelanggan.
5. Apabila prasyarat redundan tidak dapat dipenuhi, maka proses alternatif perlu ditetapkan untuk menjamin ketersediaan dari proses bisnis dan operasional Perangkat Daerah serta *delivery* dari layanan Perangkat Daerah kepada pelanggan.
6. Fasilitas pengolahan informasi beserta sarana pendukungnya yang telah memenuhi aspek redundansi harus diuji secara berkala untuk menjamin kesesuaian dari fungsinya.
7. Guna menjamin ketersediaan layanan serta keamanan informasi dalam kondisi darurat (misalnya: bencana alam) pada lokasi utama, perlu adanya redundansi terhadap fasilitas pengolahan informasi yang disebut sebagai fasilitas *backup site*.
8. *Backup site* yang dimaksud dapat berupa lokasi kerja pengganti atau *disaster recovery center* (DRC) bagi alternatif area *data center*.

9. Ketentuan dalam pengelolaan terkait *Backup Site* meliputi:
   a. lokasi *backup site* secara geografis memiliki probabilitas kejadian bencana alam yang minimal;
   b. *backup site* ditujukan sebagai media penyimpanan *backup* alternatif, serta sebagai fasilitas pengolahan informasi alternatif;
   c. terpenuhinya pemulihan layanan operasional sepenuhnya pada fasilitas *backup site* sesuai kerangka parameter *recovery time objective* (RTO);
   d. pengelola backup site beserta Pemilik Aset Informasi melakukan uji keberlangsungan secara berkala dibawah koordinasi penanggung jawab kelangsungan bisnis, minimal 1 kali dalam setahun, untuk menguji kesiapan seluruh pihak dalam hal:
      1) memindahkan operasional ke fasilitas *backup site*;
      2) memulihkan operasional aplikasi beserta data sesuai parameter *recovery point objective* (RPO) yang telah ditetapkan.

BAB XIII
Kepatuhan

A. Tujuan

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

B. Ruang Lingkup

Ruang lingkup dari kebijakan mengenai kepatuhan, antara lain:

1. Kepatuhan dengan prasyarat hukum dan kontraktual; dan
2. Peninjauan keamanan informasi.

C. Kebijakan

1. Pemerintah Kota Salatiga berkomitmen untuk menjaga kepatuhan terhadap setiap prasyarat keamanan informasi yang relevan. Prasyarat keamanan informasi yang dimaksud mencakup prasyarat hukum, regulasi dan kontraktual;
2. Seluruh prasyarat hukum, regulasi dan kontraktual yang terkait dengan keamanan informasi dan berlaku bagi Perangkat Daerah harus diidentifikasikan, didokumentasikan dan dipelihara;
3. Perangkat Daerah harus mematuhi hak atas kekayaan intelektual yang terkait dengan material yang digunakan oleh Perangkat Daerah seperti:
4. Dokumen-dokumen penting Perangkat Daerah harus dilindungi dari kehilangan, pemalsuan, kerusakan, atau penyalahgunaan sesuai dengan peraturan perundangan, regulasi, dan persyaratan kontrak dan bisnis;
5. Perangkat Daerah harus memastikan privasi dan perlindungan terhadap informasi terkait dengan pribadi (*personally identifiable information*) sesuai dengan prasyarat hukum, perundangan, regulasi dan kontraktual;
6. Kepala Perangkat Daerah harus secara rutin memantau dan meninjau kepatuhan dari personil, proses kerja dan pemrosesan informasi dalam area tanggung jawabnya terhadap kebijakan dan standar keamanan informasi Perangkat Daerah serta prasyarat keamanan informasi yang berlaku;
7. Pada saat terjadi ketidaksesuaian, pimpinan Perangkat Daerah bertanggung jawab untuk menangani ketidaksesuaian yang terjadi sesuai dengan kebijakan terkait penanganan ketidaksesuaian dan peningkatan SMKI;
8. Sistem informasi Perangkat Daerah harus ditinjau untuk menganalisis kepatuhan teknis dengan kebijakan dan standar keamanan yang berlaku serta dengan prasyarat keamanan informasi yang relevan dan berlaku, paling tidak satu kali dalam satu tahun;
9. Apabila diperlukan, peninjauan tersebut dapat melibatkan personil yang memiliki kualifikasi di bidang keamanan informasi untuk mendapatkan pemahaman yang mendalam mengenai risiko keamanan informasi yang mungkin muncul dari pengecualian tersebut.

BAB XIV
Keamanan Data dan Informasi

A. Tujuan

B. Ruang Lingkup

Ruang lingkup kebijakan keamanan data dan informasi, antara lain sebagai berikut:

1. Kerahasiaan;
2. Keaslian;
3. Keutuhan;
4. Kenirsangkalan; dan
5. Ketersediaan.

C. Referensi

1. *International Standardization Organisation and International Electrotechnical Commission* ISO/ IEC 27001 : 2013, Annex 8.2 *Information Classification*;
2. *International Standardization Organisation and International Electrotechnical Commission* ISO/ IEC 27001 : 2013, Annex 9.4.3 *Password Management System*
3. *International Standardization Organisation and International Electrotechnical Commission* ISO/ IEC 27001 : 2013, Annex 10.1.1 *Policy on the use of Cryptographic Control*;
4. *National Institute of Standards and Technology* NIST 1800-17c, *Authentication Factor*
5. *National Institute of Standards and Technology* NIST 800-63-3, *Digital Identity Guidelines*
6. *National Institute of Standards and Technology* NIST 800-60v1r1 - *Government Resource Management Function and Information Types*

D. Kebijakan

1. Kerahasiaan

a. Penetapan klasifikasi informasi;
   1) Proses penetapan klasifikasi informasi, mengacu pada Bab IV Pengelolaan Aset;
   2) Data dan informasi yang diinventarisasi adalah data dan informasi dalam bentuk:
      a) Data Pribadi Umum, meliputi Nama Lengkap, Jenis Kelamin, Kewarganegaraan, Agama, Data Pribadi yang dikombinasikan untuk mengidentifikasi seseorang;
      b) Data Pribadi yang Bersifat Spesifik, meliputi Data Biometrik, Genetika, tentang kehidupan/ orientasi seksual, Pandangan Politik, Catatan Kejahatan, Data Anak, Data keuangan Pribadi, dan atau Data Lainnya sesuai ketentuan Perundang-undangan;
      c) Informasi mengenai manajemen Administrasi Pemerintah meliputi fasilitas, sarana dan prasarana, dan sejenisnya;
      d) Informasi mengenai manajemen Keuangan Pemerintah meliputi Akuntansi Keuangan, Kontrol Keuangan, Pembayaran, Aset dan Liabilitas, Laporan Keuangan, Pendapatan dan Pengeluaran, dan sejenisnya;
      e) Informasi mengenai manajemen Sumber Daya Manusia Pemerintah meliputi Strategi Sumber Daya, Rekrutmen Karyawan, Organisasi dan Jabatan, Performa Karyawan, Pengembangan Sumber Daya Manusia, dan sejenisnya;
      f) Informasi mengenai manajemen Rantai Pasok Pemerintah meliputi Informasi Penyedia Barang dan Jasa, Inventarisasi, Logistik, Layanan, dan sejenisnya;

g) Informasi mengenai manajemen Teknologi Informasi Pemerintah meliputi Pengembangan TI, Manajemen Perubahan TI, Pemeliharaan TI, Infrastruktur TI, Keamanan Informasi TI, Data-data yang telah melewati masa retensi, Manajemen Jaringan, dan sejenisnya;
h) Informasi mengenai urusan dan layanan yang dijalankan oleh pemerintah kota salatiga; dan
i) Data dan Informasi lainnya yang dianggap penting dan/ atau diatur dalam ketentuan perundang-undangan.

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

c. Penerapan pembatasan akses terhadap data dan informasi
1) Persyaratan Pengendalian Akses pada suatu sistem meliputi:
a) akses ke aset informasi serta aset pengolahan dan penyimpanan informasi dalam lingkungan Pemerintah Kota Salatiga harus dikendalikan menggunakan metode pengendalian akses yang memadai;
b) pemberian hak akses dikelola secara formal pada seluruh siklusnya, mulai dari proses pengajuan, persetujuan serta pencabutan, serta dilaksanakan oleh para pihak terkait sesuai jenjang kewenangannya;
c) pengguna yang mengakses sistem informasi dalam lingkungan Pemerintah Kota Salatiga diharuskan untuk mengautentikasi dirinya dengan menggunakan kombinasi *user* ID dan informasi autentikasi pribadi seperti *password* atau PIN;
d) pengembangan aturan pemberian akses perlu mempertimbangkan:
(1) klasifikasi dari informasi;
(2) kritikalitas dari aset yang digunakan untuk mendukung operasional bisnis;
(3) prasyarat hukum perundang-undangan, kontraktual serta keamanan yang relevan;
(4) didasarkan atas prinsip *need to know* dan *need to use*, yaitu disesuaikan dengan kebutuhan pekerjaan dan operasional dalam lingkungan Pemerintah Kota Salatiga;

e) aturan pemberian akses harus dikembangkan dan didokumentasikan oleh setiap pemilik sistem dalam bentuk daftar atau matriks akses;
f) peninjauan terhadap aturan pemberian akses harus dilakukan oleh pemilik aset/ sistem secara berkala tergantung tingkat kritikalitas sistem tersebut;
g) peninjauan terhadap hak akses pengguna harus didokumentasikan secara formal; dan
h) setiap penyimpangan yang ditemukan dalam proses peninjauan harus segera diperbaiki dengan cara menyesuaikan atau mencabut hak akses yang menyimpang.

2) Pengelolaan akses terhadap pengguna di Perangkat Daerah harus memenuhi ketentuan sebagai berikut:
   a) pemilik Aset Informasi harus memiliki manajemen identitas pengguna yang mencakup proses pendaftaran dan terminasi pengguna, yang didalamnya termasuk:
      (1) identitas pengguna (*user account*) harus unik, melekat ke setiap individu tunggal, sehingga setiap tindakan pengguna dapat dipertanggungjawabkan;
      (2) tidak diizinkan menggunakan satu identitas pengguna yang digunakan secara bersama-sama oleh lebih dari satu individu, kecuali untuk tujuan tertentu yang sebelumnya harus mendapatkan persetujuan dari pihak berwenang; dan
      (3) memastikan secara berkala bahwa tidak ada identitas pengguna yang terduplikasi atau redundan sehingga seluruh identitas pengguna aktif adalah sesuai dengan pegawai Perangkat Daerah aktif.
   b) pendaftaran, modifikasi dan pencabutan hak akses pengguna mencakup proses pembuatan user ID, memberikan hak akses kepada user ID serta mencabut hak akses dan user ID.
   c) pendaftaran, modifikasi dan pencabutan hak akses pengguna harus disetujui oleh atasan dari pengguna yang memohon hak akses tersebut dan pemilik informasi dan/ atau sistem. Persetujuan tersebut harus diberikan sesuai dengan aturan pemberian akses.
   d) identitas pengguna harus diotorisasi secara formal oleh pejabat berwenang pada pemilik aset informasi. Akses atas sistem dan aplikasi hanya dapat diaktifkan jika proses otorisasi telah selesai.
   e) identitas pengguna pada sistem, seperti user ID, harus bersifat unik untuk memungkinkan mengidentifikasi dan meminta pertanggungjawaban pengguna.
   f) pemberian informasi autentikasi suatu pengguna yang bersifat rahasia harus dilakukan melalui proses formal yang mencakup:
      (1) informasi autentikasi perdana yang diberikan untuk pertama kalinya adalah bersifat sementara, dimana pengguna wajib menggantinya pada kesempatan pertama mengakses sistem atau aplikasi;
      (2) informasi autentikasi bawaan (*default*) dari penyedia barang/ jasa harus segera diganti pada saat instalasi sistem atau aplikasi;

g) pemilik Aset harus melakukan tinjauan secara berkala atas seluruh hak akses pengguna secara berkala, dengan tambahan tinjauan insidental yang dilakukan pada saat:
   (1) terjadinya proses kepegawaian, seperti promosi, mutasi, terminasi; dan
   (2) terjadinya perubahan struktur organisasi.
h) hak akses khusus (*privileged access rights*) dari sistem informasi dalam lingkungan Perangkat Daerah, seperti administrator, *root*, hak akses untuk memodifikasi database atau hak akses untuk membuat, memodifikasi atau mencabut pengguna dalam sistem aplikasi, harus sangat dibatasi kepada personil yang terotorisasi.
i) Hak akses khusus harus disetujui dan didokumentasikan secara formal.
j) alokasi dari hak akses khusus harus ditinjau secara berkala dan setiap terdapat perubahan dalam status penggunaan akses tersebut.
k) setiap penyimpangan yang ditemukan dalam proses peninjauan harus segera diperbaiki dengan menyesuaikan atau menghapus hak akses khusus yang menyimpang.
l) apabila memungkinkan, hak akses khusus harus dialokasikan secara individual dan tidak di-share. Hal ini dilakukan untuk menjamin akuntabilitas dari pengguna khusus.
m) apabila hak akses khusus tidak bisa dialokasikan secara individual, kontrol tambahan seperti *dual custody*, harus diimplementasikan untuk menghindari penyalahgunaan.

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

2. Keaslian

a. Mekanisme Verifikasi;
   1) Setiap pihak yang akan mengakses data dan informasi harus melalui proses verifikasi untuk mengetahui kebenaran dan keaslian pihak yang akan mengakses data dan informasi tersebut;
   2) Faktor verifikasi dapat meliputi:
      a) *Something you know*
         Faktor ini mengacu pada sesuatu yang diketahui oleh satu pihak meliputi *password*, jawaban atas pertanyaan keamanan, *Personal Identification Number* (PIN), tanda tangan, dan sejenisnya.
      b) *Something you have*
         Faktor ini mengacu pada informasi yang dimiliki secara fisik, Meliputi *One-Time Password*, Token, Kartu Identitas, dan sejenisnya.
      c) *Something you are*
         Faktor ini mengacu pada informasi yang dimiliki oleh pihak terkait secara biologis dan identik, Meliputi sidik jari, kepalan tangan, bagian mata (retina dan atau iris), suara, wajah, dan sejenisnya.

b. Mekanisme Validasi; dan
   1) Setelah melalui proses Verifikasi, berikutnya dilanjutkan dengan proses validasi yang dilakukan untuk menguji bahwa pihak yang akan mengakses data dan informasi adalah valid dan bukan pihak yang tidak terotorisasi.
   2) Proses validasi dilakukan minimal menggunakan 2 (dua) faktor verifikasi untuk memastikan kebenarannya.

c. Mekanisme Sistem *Hash Function*.
   1) *Hashing* adalah proses pengamanan/ enkripsi satu arah (*one way encryption*) menggunakan teknik kriptografi dengan memanfaatkan proses matematis yang dapat mengubah data dan/ atau informasi menjadi hash (satu deret kode yang merepresentasikan data/ atau informasi dan bersifat unik antara satu dengan yang lainnya).
   2) Algoritma Hashing yang dapat digunakan antara lain (namun tidak terbatas pada): MD5, SHA (1,3,256, & 512), Bcrypt, dan lain sebagainya.
   3) Data dan Informasi dengan tingkat kritikalitas yang tinggi, pada saat disimpan dan atau ditransmisikan melalui sistem harus melalui proses *Hashing*.

3. Keutuhan

a. Pendeteksian modifikasi terhadap data dan informasi diperoleh dengan menerapkan sistem *log* atau *audit trail.*
b. Sistem *log* atau *audit trail* dapat mencatat hal-hal berikut, meliputi:
   1) Penanda Waktu terhadap kegiatan yang terjadi
   2) Kegiatan yang dilakukan terhadap data dan informasi
   3) Aktor yang melakukan kegiatan
   4) Lingkungan, Sistem, atau lokasi yang digunakan seperti OS, Nama Mesin, dan sejenisnya.
   5) Perubahan apa yang terjadi pada data dan atau informasi
c. Tanda tangan yang digunakan di lingkungan Pemerintah Kota Salatiga merupakan Tanda Tangan Elektronik (TTE) bersertifikasi.
d. TTE harus memenuhi persyaratan:
   1) dibuat dengan menggunakan jasa penyelenggara sertifikat elektronik; dan
   2) dibuktikan dengan sertifikat elektronik.
e. Bentuk dari TTE, antara lain:
   1) *scan* tanda tangan ASN di lingkungan Pemerintah Kota Salatiga yang berwenang dan terkait dengan naskah dinas yang ditandatangani;
   2) proses *scan* berupa tanda tangan basah yang dipindai/ *scan* dengan mesin *scanner*; dan
   3) ukuran *scan* adalah 150 x 120 pixel dengan ukuran file 1 MB.
f. TTE sebagai alat autentikasi dan verifikasi atas:
   1) identitas penandatangan; dan
   2) keaslian (*authentication*), keutuhan (*integrity*) dan kenirsangkalan (*non-repudiation*) dokumen elektronik.
g. TTE memiliki kekuatan hukum dan akibat hukum yang sah, jika:
   1) data pembuatan TTE terkait hanya kepada Penanda Tangan;
   2) data pembuatan TTE pada saat proses penandatanganan hanya berada dalam kuasa Penanda Tangan;
   3) segala perubahan terhadap TTE yang terjadi setelah waktu penandatanganan dapat dapat diketahui;
   4) segala perubahan terhadap informasi elektronik yang terkait dengan TTE setelah waktu penandatanganan diketahui;
   5) terdapat cara tertentu yang dipakai untuk mengidentifikasi penanda tangan; dan
   6) Terdapat cara tertentu untuk menunjukkan bahwa penandatangan telah memberikan persetujuan terhadap informasi elektronik yang terkait.
h. Proses penandatanganan wajib dilakukan mekanisme untuk memastikan data pembuatan TTE dengan ketentuan:
   1) masih berlaku, tidak dibatalkan atau tidak ditarik;
   2) tidak dilaporkan hilang;

3) Tidak dilaporkan berpindah tangan kepada pihak yang tidak berhak; dan
4) berada dalam kuasa penanda tangan.

i. Sebelum dilakukan penandatanganan, informasi elektronik yang akan ditandatangani wajib diketahui dan dipahami oleh penanda tangan.
j. Persetujuan penandatangan terhadap informasi elektronik yang akan ditandatangani dengan TTE wajib menggunakan mekanisme afirmasi dan/ atau mekanisme lain yang memperlihatkan maksud dan tujuan penanda tangan untuk terikat dalam suatu transaksi elektronik.
k. Penggunaan TTE di lingkungan Pemerintah Kota Salatiga diterapkan pada Naskah Dinas yang termasuk dalam dokumen elektronik.
l. Jenis naskah dinas yang menggunakan TTE ditetapkan dengan keputusan Wali Kota.
m. Bentuk/ visualisasi dan letak TTE mengacu pada ketentuan mengenai tata naskah dinas di lingkungan Pemerintah Kota Salatiga.
n. Naskah dinas yang sudah ditandatangani secara elektronik harus mencantumkan lembaga jasa penyelenggara Sertifikat Elektronik.

4. Kenirsangkalan

Untuk penerapan sistem tanda tangan elektronik yang tersertifikasi, mengacu pada angka 3 Keutuhan.

5. Ketersediaan

a. Penerapan Pencadangan Berkala
1) Data dan Informasi yang dianggap kritikal oleh Perangkat Daerah harus di-*backup* secara memadai untuk menjamin ketersediaannya.
2) seluruh data dan informasi yang berada di dalam fasilitas pengolahan informasi wajib dilakukan *backup*, dengan persyaratan berikut:
a) *backup* mencakup data dan informasi;
b) frekuensi *backup* dilakukan secara harian, bulanan, dan tahunan;
c) salinan *backup* harus disimpan secara aman sesuai dengan periode retensi. periode retensi *backup* adalah 1 tahun, dimana:
(1) *backup* harian disimpan selama 31 hari;
(2) *backup* bulanan disimpan selama 12 bulan;
d) media *backup* disimpan pada perangkat *storage* yang terpisah dari perangkat pengolahan informasi utama;
e) *backup* merupakan tanggung jawab pengelola *data center*, sedangkan pengujian *restore* merupakan tanggung jawab pemilik aset informasi;
3) Hal yang perlu dipertimbangkan dalam proses *backup* informasi meliputi:
a) pemilik informasi bertanggung jawab untuk menentukan informasi yang membutuhkan *backup*, frekuensi dan metode backup serta waktu retensi untuk setiap backup informasi yang ada;
b) pernyataan formal terkait informasi yang dibutuhkan untuk di-*backup* beserta metode dan frekuensi dari *backup* harus ditentukan bersama dengan personil yang bertugas melaksanakan proses *backup* serta harus dinyatakan secara jelas dalam sebuah rencana *backup* resmi;

c) *backup* informasi harus disimpan sesuai dengan masa retensi dari informasi utama;
d) masa retensi harus dinyatakan secara jelas dalam rencana *backup*; dan
e) perlindungan terhadap *backup* informasi harus dilakukan berdasarkan klasifikasi dari informasi utama.

b. Penerapan Sistem Pemulihan
1) informasi yang dianggap kritikal oleh Perangkat Daerah harus dapat di-*restore* sewaktu-waktu.
2) *restore* data dapat dilakukan saat data di sistem utama mengalami kerusakan, kecelakaan atau bencana alam.
3) seluruh hasil *backup* harus dilakukan uji *restore* secara berkala.

c. Perencanaan Ketersediaan Data dan Informasi
Pelaksanaan perencanaan ketersediaan untuk data dan informasi dilakukan sesuai dengan Kebijakan pada Bab XII Kelangsungan Usaha (*Business Continuity*).

BAB V
Keamanan Aplikasi

A. Tujuan

Tujuan dari kebijakan keamanan aplikasi antara lain untuk:

B. Ruang Lingkup

Ruang lingkup kebijakan keamanan aplikasi, antara lain sebagai berikut:

1. Keamanan Aplikasi Berbasis *Website*
   a. autentikasi;
   b. manajemen sesi;
   c. persyaratan kontrol akses;
   d. validasi input;
   e. kriptografi pada verifikasi statis;
   f. penanganan eror dan pencatatan *log*;
   g. proteksi data;
   h. keamanan komunikasi;
   i. pengendalian kode berbahaya;
   j. logika bisnis;
   k. *file*;
   l. keamanan API dan *web service*; dan
   m. keamanan konfigurasi.
2. Keamanan Aplikasi Berbasis *Mobile*
   a. penyimpanan data dan persyaratan privasi;
   b. kriptografi;
   c. autentikasi dan manajemen sesi;
   d. komunikasi jaringan;
   e. interaksi *platform*;
   f. kualitas kode dan pengaturan *build*; dan
   g. ketahanan.

C. Referensi

1. *The Open Web Application Security Project* (OWASP) *Application Security Verification Standard* 4.0.3;
2. *The Open Web Application Security Project* (OWASP) *Mobile Application Security Verification Standard* Version v1.4.2;
3. *The Open Web Application Security Project* (OWASP) *File Upload Cheat Sheet*;
4. *The Open Web Application Security Project* (OWASP) *Input Validation Cheat Sheet*;

D. Kebijakan

1. Kebijakan Umum

Aplikasi harus diuji keamanannya setiap periode tertentu yang dilakukan dengan:

a. Pengidentifikasian standar keamanan yang belum diterapkan;
b. Memastikan pengkodean pemrograman aplikasi yang telah dan/ atau akan dibuat tidak memiliki kerawanan atau celah keamanan;
c. Melakukan pemindaian otomatis dan/ atau pengujian penetrasi sistem terhadap aplikasi(*penetration testing*);
d. Mengidentifikasi kerentanan dan mengelola ancaman sejak awal siklus pengembangan Aplikasi; dan
e. Menganalisis kerentanan Aplikasi.

2. Keamanan Aplikasi Berbasis *Website*

a. Autentikasi

1) Setiap pengguna harus mempunyai tanggung jawab dalam penggunaan *User* ID dan *password* yaitu:

a) pengguna harus menjaga kerahasiaan dan keamanan password pribadi atau kelompok serta informasi autentikasi rahasia lainnya;

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

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

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

(1) memiliki panjang minimum 8 karakter;

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

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

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

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

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

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

(1) tidak menampilkan *password* yang dimasukkan;

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

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

i) Mekanisme pemulihan kata sandi, antara lain adalah:

(1) Pengguna yang lupa akan kata sandinya harus mengirim surat permohonan setel ulang kata sandi kepada pengelola sistem;

(2) Berdasarkan surat tersebut pengelola sistem, mengakses bagian *user management* pada sistem tersebut dan mereset *password* akun pengguna terkait. Setelah itu pengelola sistem mengirimkan e-*mail* yang berisikan informasi *password* baru dari akun pengguna terkait;

j) Pengendalian akses sistem dan aplikasi yang dikelola oleh Perangkat Daerah meliputi:

(1) pemilik aset informasi harus memastikan bahwa sistem dan aplikasi dibawah pengelolaannya memiliki fasilitas manajemen hak akses pengguna, manajemen kata sandi yang baik, serta mekanisme autentikasi pengguna yang aman;

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

(3) Hak akses untuk kebutuhan audit harus dibatasi hanya hak akses *read only*;

(4) fasilitas manajemen kata sandi harus memastikan dihasilkannya kata sandi yang berkualitas, yaitu:
   (a) menegakkan akuntabilitas pengguna melalui penggunaan identitas pengguna tunggal untuk setiap individu;
   (b) memberikan fasilitas penggantian kata sandi mandiri;
   (c) membantu memberikan rekomendasi kata sandi yang berkualitas;
   (d) mewajibkan pengguna untuk mengganti kata sandi pada saat pertama kali login;
   (e) mewajibkan pengguna untuk mengganti kata sandi secara berkala;
   (f) menyimpan riwayat kata sandi pengguna dan mencegah agar pengguna tidak menggunakan kata sandi yang sebelumnya telah digunakan;
   (g) tidak menampilkan kata sandi saat sedang dientrikan; dan
   (h) kata sandi disimpan dalam bentuk terlindungi (dienkripsi), demikian juga pada saat kata sandi ditransmisikan.

(5) mekanisme autentikasi pengguna perlu dirancang agar meminimalkan peluang terjadinya akses yang tidak sah, yaitu:
   (a) kata sandi tidak ditransmisikan melalui jaringan secara *plaintext*;
   (b) memiliki mekanisme penguncian sistem sementara sebagai perlindungan terhadap *brute force attacks*;
   (c) adanya pencatatan terhadap seluruh upaya autentikasi yang sukses dan gagal;
   (d) adanya pembatasan jumlah akses pengguna yang sama secara simultan;

(6) Parameter autentikasi pengguna disesuaikan dengan klasifikasi aset informasi sebagai berikut:

Parameter autentikasi	**Rahasia & Internal**	**Publik**
Jumlah gagal *login* sebelum	3 kali	10 kali
Durasi *timeout* sebelum	5 menit	16 menit

b. Manajemen Sesi
   1) Sesi merupakan representasi interaksi antara *peramban* dan *server;*
   2) Sesi merupakan kombinasi dari *client-side session* ID dan *server-side session* data:
      a) *client-side session* ID, dapat berupa parameter URL, *cookie* atau HTTP *request header*; dan
      b) *server-side session* data, dapat berupa file maupun basis data.
   3) Aplikasi tidak menguak/ membocorkan token sesi pada parameter URL;
   4) Aplikasi menghasilkan token sesi yang baru pada setiap proses autentikasi pengguna;
   5) Token sesi harus terdiri dari paling tidak 64-bit entropi/ keacakan yang artinya memiliki 2^64 kemungkinan;

6) Aplikasi hanya menyimpan token sesi di browser dengan menggunakan metode yang aman, seperti secured cookies;
7) Aplikasi hanya boleh menghasilkan token sesi yang dienkripsi menggunakan algoritma kriptografi yang aman;
8) Menggunakan pengendali sesi untuk proses manajemen sesi yang meliputi:
   a) Token sesi yang sudah habis/ selesai masa pakainya tidak dapat digunakan kembali;
   b) Dalam hal autentikator mengizinkan pengguna untuk melanjutkan login selama beberapa saat (*keep login*), harus dipastikan terdapat mekanisme re-autentikasi yang dilakukan secara periodik baik pada saat aktif digunakan, maupun pada saat diam/ *idle*;
   c) Sesi dinyatakan selesai apabila tidak ada aktivitas pada aplikasi dalam waktu 5-10 menit;
   d) Terdapat proses validasi dan pencantuman *session* id;
   e) Terdapat pelindungan terhadap duplikasi dan mekanisme persetujuan pengguna;
   f) menggunakan pengendali sesi yang disediakan oleh kerangka kerja aplikasi;
   g) mengatur pembuatan dan keacakan token sesi yang dihasilkan oleh pengendali sesi;
   h) mengatur kondisi dan jangka waktu habis sesi;
   i) perlindungan terhadap lokasi dan pengiriman token untuk sesi terautentikasi; dan
   j) perlindungan terhadap duplikasi dan mekanisme persetujuan pengguna.
   k) Pada saat sukses ketika penggantian password (termasuk penggatian karena *reset/ recovery*), terdapat pilihan untuk menonaktifkan seluruh sesi yang sedang berjalan;
   l) Pengguna dapat melihat dan keluar/ *logout* dari setiap sesi dan/ atau perangkat yang sedang aktif;
9) Sesi dapat diimplementasikan menggunakan *Cookie*, dan tetap harus dikelola dengan baik dengan menerapkan:
   a) Token Sesi yang diimplementasikan menggunakan *Cookie* harus diikuti dengan pemasangan atribut *"secure",* dan *"HttpOnly"* ;
   b) Token Sesi yang diimplementasikan menggunakan *Cookie*, harus memanfaatkan atribut "*SameSite*" untuk alasan keamanan;
   c) Token Sesi yang diimplementasikan menggunakan *Cookie,* memanfaatkan imbuhan/ *prefix "__Host-"*, sehingga *Cookie* hanya dikirimkan kepada host yang sudah memasang inisial tersebut;
   d) Harus dipastikan bahwa aplikasi-aplikasi yang terpublikasi dalam satu *domain,* tidak dapat menguak informasi terkait *Cookie*/ Sesi satu sama lain.
10) Sesi dapat diimplementasikan menggunakan Token, dan tetap harus dikelola dengan baik dengan memperhatikan hal-hal berikut:
   a) Manajemen Sesi berbasis Token meliputi JWT (Java Web Token), OAuth, dan SAML;
   b) Memastikan aplikasi dapat mengizinkan pengguna untuk menarik kembali/ me-*revoke* token OAuth yang berasal dari hubungan aplikasi yang terpercaya;

c) Memastikan aplikasi yang menggunakan token sesi dengan jenis *stateless,* menggunakan tanda tangan digital, enkripsi, dan upaya lainnya untuk melindungi token dari *tampering,* dan upaya serangan lainnya

11) Sesi juga dapat diimplementasikan menggunakan fitur *federated re-authentication* dengan memanfaatkan konsep *Relying Party (RP)* atau *Credential Service Provider (CSP).* Pastikan keamanan dalam menggunakan fitur ini tercapai dengan memperhatikan hal-hal berikut:
   a) Pastikan bahwa *RP* menetapkan batas maksimum untuk waktu autentikasi kepada *CSP,* dan pastikan bahwa CSP me-autentikasi ulang pada saat pengguna tidak menggunakan sesi tersebut dalam jangkaa waktu tertentu;
   b) Pastikan bahwa CSP memberitahukan kepada RP terkait kegiatan autentikasi yang terakhir dilakukan, untuk mengizinkan RP untuk menentukan apakah perlu dilakukan autentikasi ulang kepada pengguna.

12) Memastikan bahwa aplikasi mampu melindungi Sesi dari segala upaya eksploitasi/ upaya serangan yang berupaya untuk mendapatkan sesi oleh pihak yang tidak sah.

c. Persyaratan Kontrol Akses;
   1) Batasi akses aplikasi ke pengguna yang berwenang;
   2) Menerapkan *segregation of duties/* pembatasan tugas dan tanggung jawab*;*
   3) Fasilitas manajemen hak akses pengguna harus mampu membatasi akses informasi sesuai ketugasannya (*role based access control*);
   4) Hak akses untuk kebutuhan audit harus dibatasi hanya hak akses *read only*;
   5) Menggunakan *Multi Factor Authentication (MFA)* untuk menanggulangi akses yang tidak sah; dan
   6) Pastikan penerapan kontrol akses memiliki ketahanan yang kuat dalam melindungi akses dari upaya-upaya serangan

d. Validasi, sanitasi, dan pengkodean inputan
   Penerapan validasi, sanitasi dan pengkodean yang tepat akan mengurangi jenis kerentanan aplikasi terhadap injeksi. Untuk itu perlu memperhatikan hal-hal berikut, meliputi:
   1) Validasi Inputan;
   2) Sanitasi dan *Sandboxing;*
   3) Sandikan/ kodekan keluaran serta upaya pencegahan injeksi;
   4) *Memory*, *string*, dan kode yang tidak terkelola; dan
   5) Pencegahan Deserialisasi.

e. kriptografi pada verifikasi statis;
   Memastikan aplikasi menerapkan hal-hal berikut, meliputi:
   1) Klasifikasi Data
      a) Memastikan data pribadi tersimpan dengan mekanisme enkripsi yang kuat;
      b) Memastikan data kesehatan tersimpan dengan mekanisme enkripsi yang kuat;
      c) Memastikan data keuangan seperti tersimpan dengan mekanisme enkripsi yang kuat;
   2) Algoritma
      a) Seluruh modul kriptografi harus dipastikan dapat menangani eror dengan baik;

b) Memastikan bahwa algoritma kriptografi yang dipakai, menggunakan library yang sudah teruji alih-alih menggunakan kode yang dibangun sendiri;
c) Memastikan bahwa nomor acak, algoritma enkripsi, panjang kunci, dan hal-hal yang terkait dengan kriptografi dapat dikonfigurasi, diperbarui, dan diubah sewaktu-waktu jika ditemukan kerentanan;
d) Memastikan bahwa tidak menggunakan algoritma kriptografi yang sudah diindikasi tidak aman;

3) Nilai Acak
a) Memastikan bahwa seluruh nilai acak, nama file acak, dan keacakan lainnya, harus dipastikan aman dan tidak dapat ditebak oleh pihak lain;
b) Memastikan bahwa seluruh nilai acak memiliki nilai entropi yang baik

4) Manajemen Rahasia
a) Memastikan seluruh pelaksanaan manajemen rahasia; dan
b) Memastikan material *key* tidak terekspos dalam aplikasi.

f. Penanganan Eror dan Pencatatan *Log*
1) Terdapat kotak pesan yang ditampilkan pada layar pengguna ketika terjadi kesalahan. Contohnya "Terjadi Kesalahan! Silakan muat ulang halaman";
2) Memastikan bahwa aplikasi tidak mencatat kredensial atau detil pembayaran. Token sesi hanya boleh disimpan pada *log* dalam bentuk *hash* yang tidak dapat diubah;
3) Memastikan bahwa aplikasi tidak mencatat data sensitif lainnya seperti yang ditentukan berdasarkan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi;
4) Memastikan bahwa aplikasi mencatat *event* terkait keamanan termasuk *event* autentikan yang berhasil dan gagal, kegagalan kontrol akses, kegagalan deserialisasi, dan kegagalan validasi input;
5) Memastikan bahwa setiap *log event* mencakup informasi diperlukan yang akan memungkinkan penyelidikan mendetail tentang garis waktu saat suatu peristiwa terjadi;
6) Memastikan bahwa semua keputusan autentikan dicatat, tanpa menyimpan token atau kata sandi sesi yang sensitif. Ini harus mencakup permintaan dengan metadata relevan yang diperlukan untuk investigasi keamanan;
7) Memastikan bahwa semua keputusan kontrol akses dapat dicatat dan semua keputusan yang gagal juga dicatat. Ini harus mencakup permintaan dengan metadata relevan yang diperlukan untuk investigasi keamanan;
8) Memastikan bahwa semua komponen *logging* menyandi data dengan benar untuk mencegah injeksi *log*;
9) Memastikan bahwa *log* keamanan dilindungi dari akses dan modifikasi yang tidak sah;
10) Memastikan bahwa sumber waktu disinkronkan ke waktu dan zona waktu yang benar, dalam hal ini Waktu Indonesia Barat (WIB);
11) Memastikan bahwa pesan umum ditampilkan saat terjadi kesalahan yang tidak terduga atau saat ada masalah keamanan, dapat ditampilkan dengan ID unik yang dapat digunakan personel pendukung untuk penyelidikan;
12) Memastikan bahwa penanganan pengecualian digunakan di seluruh basis kode untuk memperhitungkan kondisi *error* yang diharapkan maupun yang tidak diharapkan; dan

13) Memastikan bahwa personel yang akan menangani semua permasalahan terakhir telah ditetapkan, karena personel tersebut akan menangani *error* yang tidak dapat ditangani oleh pihak lain.

g. Proteksi Data
   1) Melakukan identifikasi untuk perlindungan Data Umum, Data di Sisi *Client*, dan Data Sensitif;
   2) Memastikan data terlindungi dari akses yang tidak sah;
   3) Memastikan kegiatan pertukaran, penghapusan, dan audit informasi dilakukan;
   4) Memastikan pelaksanaan kegiatan penentuan jumlah parameter;
   5) Memastikan data disimpan dengan aman;
   6) Penentuan metode untuk menghapus dan pengeksporan data sesuai permintaan pengguna; dan
   7) Pembersihan memori setelah tidak digunakan.

h. Keamanan Komunikasi
   1) Memastikan penggunaan komunikasi yang terenkripsi seperti penggunaan TLS;
   2) Memastikan koneksi masuk, keluar, dari, dan ke sisi *Client* maupun *Server* diamankan menggunakan enkripsi;
   3) Memastikan penggunaan algoritma enkripsi yang aman, serta pengujiannya; dan
   4) Pengaturan dan konfigurasi sertifikat elektronik yang diterbitkan oleh penyelenggara sertifikat elektronik.

i. Pengendalian Kode Berbahaya
   1) Memastikan penggunaan alat analisis kode yang dapat mendeteksi kode yang berpotensi berbahaya, seperti fungsi waktu, operasi *file* yang tidak aman, dan koneksi jaringan;
   2) Memastikan bahwa *source code* aplikasi dan *library* pihak ketiga tidak berisi *phone home* atau kemampuan pengumpulan data yang tidak sah. Jika fungsionalitas tersebut ada, maka izin pengguna untuk mengoperasikan harus didapatkan sebelum pengguna mengumpulkan data apapun;
   3) Memastikan aplikasi tidak meminta izin yang tidak perlu atau berlebihan untuk fitur atau sensor terkait dengan privasi, seperti kontak, kamera, mikrofon atau aplikasi;
   4) Memastikan bahwa *source code* aplikasi dan *library* pihak ketiga tidak berisi *back door*, seperti *hardcode* atau akun atau kunci tambahan yang tidak terdokumentasi, kode *obfuscation*, *blob* biner yang tidak terdokumentasi, *rootkit* atau *anti-debugging*, fitur *debug* yang tidak aman atau sudah ketinggalan zaman, tidak aman, atau terdapat fungsionalitas tersembunyi yang dapat digunakan dengan jahat jika ditemukan;
   5) Memastikan bahwa *source code* aplikasi dan *library* pihak ketiga tidak mengandung bom waktu dengan mencari fungsi terkait tanggal dan waktu;
   6) Memastikan bahwa *source code* aplikasi dan *library* pihak ketiga tidak mengandung kode berbahaya, seperti *salami attacks*, *logic bypasses*, atau *logic bombs*;
   7) Memastikan bahwa *source code* aplikasi dan *library* pihak ketiga tidak mengandung *Easter eggs* atau fungsionalitas yang tidak diinginkan lainnya;
   8) Memastikan bahwa aplikasi memiliki fitur *auto-update* server atau *client*, pembaruan harus diperoleh melalui saluran yang aman dan ditandatangani secara digital. Kode pembaruan harus memvalidasi tanda tangan elektronik pembaruan sebelum menginstal atau menjalankan proses pembaruan; dan

9) Memastikan bahwa aplikasi menerapkan perlindungan integritas, seperti penandatanganan kode atau *subresources integrity*. Aplikasi tidak boleh memuat atau menjalankan kode dari sumber tidak terpercaya, seperti memuat penyertaan, modul, *plugin*, kode, atau pustaka dari sumber tidak terpercaya atau dari internet.

j. Logika Bisnis

1) Memastikan bahwa aplikasi hanya akan memproses alur logika bisnis untuk pengguna yang sama dalam urutan langkah yang berurutan tanpa melewatkan langkah apapun;
2) Memastikan bahwa aplikasi hanya akan memproses alur logika bisnis dengan setiap langkahnya diproses secara realistis, yaitu transaksi tidak dikirimkan terlalu cepat (diluar batas wajar);
3) Memastikan bahwa aplikasi memiliki batasan yang sesuai untuk tindakan atau transaksi bisnis tertentu yang diterapkan dengan benar berdasarkan per pengguna;
4) Memastikan bahwa aplikasi memiliki kontrol anti-otomatisasi untuk melindungi dari panggilan berlebihan seperti eksfiltrasi data massal, permintaan logika bisnis, unggahan file, atau penolakan serangan layanan;
5) Memastikan bahwa aplikasi memantau kejadian atau aktivitas yang tidak biasa dari perspektif logika bisnis. Sebagai contoh, upaya untuk melakukan tindakan yang tidak sesuai urutan atau tindakan yang tidak akan dilakukan oleh pengguna biasa; dan
6) Memastikan bahwa aplikasi memiliki sistem peringatan yang dapat dikonfigurasi ketika serangan otomatis atau aktivitas yang tidak biasa terdeteksi.

k. *File*

Berikut merupakan hal-hal yang harus dilakukan dalam rangka mencapai implementasi pengunggahan *file* yang aman:

1) Memastikan bahwa aplikasi tidak akan menerima *file* berukuran lebih dari 2mb yang dapat memenuhi *storage* atau menyebabkan *denial of service*;
2) Memastikan bahwa aplikasi memvalidasi *file* kompresi (contohnya zip, rar, docx, dll.). Pemeriksaan tersebut mencakup *path file*, tingkat kompres *file*, jumlah maksimum *file* dan perkiraan ukuran setelah *unzip*;
3) Memastikan bahwa kuota ukuran *file* dan jumlah maksimal *file* tiap pengguna ditetapkan untuk memastikan kalau *storage* tidak dapat dipenuhi oleh 1 (satu) pengguna dengan banyaknya *file* atau dengan besaran dari *file*-nya;
4) Memastikan *file* yang didapatkan dari sumber tidak terpercaya divalidasi menjadi tipe yang diharapkan berdasarkan konten dari *file* tersebut;
5) Memastikan bahwa metadata nama *file* yang dikirimkan pengguna tidak digunakan secara langsung oleh sistem atau *framework* sistem *file*, dan bahwa API URL digunakan untuk melindungi dari serangan *path traversal*;
6) Memastikan bahwa metadata nama *file* yang dikirimkan pengguna divalidasi atau diabaikan untuk mencegah pengungkapan, pembuatan, pembaruan, atau penghapusan *file* lokal (*Local File Inclusion*/ LFI);
7) Memastikan bahwa metadata nama *file* yang dikirimkan pengguna divalidasi atau diabaikan untuk mencegah pengungkapan atau eksekusi *file* jarak jauh melalui *Remote File Inclusion* (RFI) atau serangan *Server-side Request Forgery* (SSRF);

8) Memastikan bahwa metadata *file* yang tidak terpercaya tidak digunakan secara langsung dengan API atau *library* sistem, untuk melindungi dari injeksi perintah OS;
9) Memastikan bahwa aplikasi tidak menyertakan dan menjalankan fungsionalitas dari sumber yang tidak terpercaya, seperti jaringan distribusi konten yang tidak terpercaya, *library* JavaScript, *library* noda npm, atau *server-side* DLL;
10) Memastikan bahwa *file* yang diperoleh dari sumber tidak terpercaya disimpan di luar *web root*, dengan akses terbatas;
11) Memastikan bahwa *file* yang diperoleh dari sumber tidak terpercaya dipindai oleh pemindai antivirus untuk mencegah pengunggahan dan penyajian konten berbahaya yang diketahui;
12) Memastikan bahwa *server* dikonfigurasi untuk hanya melayani *file* dengan ekstensi *file* tertentu untuk mencegah informasi yang tidak disengaja dan kebocoran *source code*. Misalnya *file backup* (misalnya .bak), *file* kompresi (.zip, .rar, dan sebagainya) dan ekstensi lain yang biasa digunakan oleh *editor* harus diblokir kecuali diperlukan;
13) Memastikan bahwa permintaan langsung ke *file* yang diunggah tidak akan pernah dijalankan sebagai konten HTML/ JavaScript;
14) Memastikan bahwa *server web* atau aplikasi dikonfigurasikan dengan daftar dari sumber daya atau sistem tempat *server* dapat mengirimkan permintaan atau memuat data/ *file*.
15) Ketentuan pengunggahan *file*
    a) Ekstensi *file* yang diperbolehkan hanyalah .doc, .docx, .xls, .xlsx, .txt, .jpg, .jpeg, .png, dan .pdf;
    b) Panjang maksimal dari nama *file* 25 karakter;
    c) Karakter yang tidak dapat digunakan berupa:
        (1) < (*less than*);
        (2) > (*greater than*);
        (3) : (*colon*);
        (4) ‘ (*single quote*)
        (5) " (*double quote*);
        (6) / (*forward slash*);
        (7) \ (*backslash*);
        (8) | (*vertical bar or pipe*);
        (9) ? (*question mark*); dan
        (10) * (*asterisk*);
    d) Ukuran maksimal dari *file* yang dapat diunggah adalah 30mb;
16) Pihak yang dapat melakukan pengunggahan *file* ke aplikasi hanyalah pihak yang sudah diberi kewenangan;
17) Nama *file* yang sudah terunggah harus di-*rename* untuk mencegah adanya risiko akses *file* langsung dan nama *file* yang ambigu untuk menghindari *filter* (seperti *test*.jpg, .asp atau / ../ ../ ../ *test*.jpg). Contohnya nama *file* yang terunggah adalah *test*.jpg, ubah nama *file* tersebut menjadi JAI1287uaisdjhf.jpg atau dengan nama *file* yang *random*;
18) Simpan *file* pada *server* yang berbeda. Jika tidak memungkinkan, simpan *file* di luar *webroot* dalam hal terdapat akses publik ke *file*. Gunakan *handler* yang dipetakan ke nama *file* di dalam aplikasi (contoh someid->file.ext);
19) Jalankan *file* melalui antivirus atau *sandbox* (jika tersedia) untuk memvalidasi bahwa *file* tersebut tidak berisi data berbahaya;

20) Pastikan bahwa setiap *library* yang digunakan dikonfigurasi dengan aman dan terus diperbarui;
21) *File* yang diunggah harus dianalisis untuk konten berbahaya (*anti-malware*, analisis statis, dll.);
22) *Path* dari *file* diputuskan oleh *server* bukan oleh pengguna;

l. *Keamanan* API dan Layanan *Web*
   1) Keamanan layanan *web* secara umum
      a) Memastikan seluruh komponen aplikasi menggunakan teknik pengkodean dan pengurai (*parsers*) untuk menghindari eksploitasi;
      b) Memastikan bahwa URL API tidak mengekspos informasi sensitif;
      c) Memastikan keputusan untuk mengautorisasi pengguna didukung baik dari URI maupun *resource level;*
      d) Memastikan penolakan *request* yang mengandung konten yang tidak diharapkan dengan *header* yang sesuai.
   2) Layanan *Web* RESTful
      a) Memastikan pilihan metode RESTful HTTP yang diaktifkan hanya yang sesuai dengan kebutuhan, dan membatasi pengguna normal dapat mengakses metode DELETE dan PUT;
      b) Memastikan validasi JSON sebelum menerima inputan;
      c) Memastikan layanan Web RESTful yang memanfaatkan *Cookies* terlindungi dari serangan CSRF;
      d) Memastikan layanan REST memeriksa kesesuaian tipe konten/ *Content-type* yang masuk;
      e) Memastikan pesan pada *header* dan *payload* adalah benar-benar sesuai dan tidak mengalami modifikasi atau perubahan.
   3) Layanan *Web* SOAP
      a) Memastikan validasi skema XSD dilakukan untuk memastikan format XML yang benar;
      b) Memastikan bahwa isi muatan/ *payload* ditandai dengan WS-Security untuk memastikan reliabilitas dan keaslian data yang dikirimkan dari *client* dan *service*
   4) GraphQL
      a) Memastikan *query* mengizinkan list atau kombinasi antara pembatasan *depth*/ kedalaman dan jumlah, hal ini digunakan untuk mencegeh GraphQL diserang menggunakan DoS;
      b) Memastikan GraphQL atau layer autorisasi data diimplementasikan pada layer *business logic* daripada di layer GraphQL

m. Keamanan Konfigurasi
   1) Melakukan konfigurasi pada server sesuai dengan rekomendasi server aplikasi dan kerangka kerja aplikasi yang digunakan;
   2) Melakukan pendokumentasian, *backup* konfigurasi, dan semua file dependensi;
   3) Melakukan penghapusan fitur, hasil dokumentasi, hasil sampel, dan konfigurasi yang sudah tidak diperlukan;
   4) Melakukan validasi terhadap integritas aset jika aset dapat diakses melalui eksternal; dan
   5) Menggunakan respon aplikasi dan konten yang aman.

3. Keamanan Aplikasi Berbasis *Mobile*

a. Penyimpanan data dan persyaratan privasi

Dalam hal penyimpanan data dan persyaratan privasi, aplikasi pemerintah berbasis *mobile* harus memenuhi kriteria berikut ini meliputi:

1) Fasilitas sistem penyimpan kredensial yang aman wajib digunakan untuk menyimpan data yang sensitif seperti data pribadi, kredensial pengguna aplikasi dan/ atau kunci enkripsi atau kriptografi;
2) Tidak boleh ada data sensitif yang disimpan selain di kontainer aplikasi dan/ atau fasilitas sistem penyimpanan kredensial yang aman;
3) Tidak boleh ada data sensitif yang disimpan/ atau ditulis dalam *log* aplikasi;
4) Tidak boleh ada data sensitif yang dibagikan dengan pihak ketiga, kecuali telah melalui persetujuan dan memang bagian dari arsitektur aplikasi;
5) *Keyboard cache* harus dalam keadaan tidak aktif ketika digunakan untuk memproses data sensitif;
6) Tidak boleh ada data sensitif yang terekspos keluar pada saat proses mekanisme pertukaran data;
7) Tidak boleh ada data sensitif seperti *password*, PIN, atau OTP yang terekspos melalui *user interface*;
8) Tidak boleh ada data sensitif yang ikut terbackup pada saat pelaksanaan *backup* oleh sistem operasi perangkat *mobile*;
9) Aplikasi harus menyingkirkan data sensitif dari tampilan pada saat berpindah ke *background*;
10) Aplikasi hanya dapat menyimpan data sensitif di *memory* pada jangka waktu yang dibutuhkan, dan *memory* dibersihkan setelahnya;
11) Aplikasi harus mampu mendesak pengguna untuk memenuhi standar minimum *device-access-security,* seperti penerapan *password* atau PIN pada perangkat;
12) Aplikasi memiliki kemampuan untuk mengedukasi/ menginfokan kepada pengguna tentang bagaimana praktik terbaik atau *best practice* untuk menangani jenis data tertentu;
13) Tidak boleh ada data sensitif yang disimpan secara lokal pada perangkat *mobile*. Penyimpanan data sensitif sebaiknya hanya diterima langsung dari *endpoint* ketika dibutuhkan, dan hanya dikelola di memori (RAM);
14) Jika dalam hal data sensitif tetap dibutuhkan untuk disimpan secara lokal, maka harus dipastikan penyimpanannya menerapkan mekanisme enkripsi dengan menggunakan kunci yang berasal dari *hardware* penyimpanan yang mana memerlukan autentikasi untuk mengaksesnya; dan
15) Data dan/ atau informasi yang dihasilkan oleh aplikasi harus dibersihkan dari media penyimpanan lokal pada saat terjadi banyak kegagalan saat autentikasi.

b. Kriptografi

Dalam hal kriptografi aplikasi pemerintah berbasis *mobile* harus memenuhi kriteria berikut ini meliputi:

1) Aplikasi tidak disarankan bergantung pada kriptografi simetris dengan kunci yang di *hardcoded* sebagai dasar enkripsi;
2) Aplikasi menerapkan kriptografi-primitif (kriptografi level rendah yang digunakan untuk membangun algoritma kriptografi yang lebih tinggi) yang sudah terbukti;

3) Aplikasi menggunakan kriptografi-primitif yang sesuai untuk kebutuhan-kebutuhan khusus dari aplikasi, serta dikonfigurasikan dengan parameter-parameter yang sesuai dengan *best practice*;
4) Aplikasi tidak dapat menggunakan algoritma atau protokol kriptografi yang telah rentan terhadap masalah keamanan;
5) Aplikasi tidak dapat menggunakan ulang kunci kriptografi yang sama untuk beberapa tujuan; dan
6) Seluruh nilai *random/* acak, harus dibangun menggunakan metode pengacakan yang benar-benar aman (tidak menggunakan *library* yang sudah ada).

c. Autentikasi dan Manajemen Sesi
1) Menerapkan beberapa bentuk autentikasi seperti autentikasi nama pengguna/ kata sandi yang dilakukan pada *remote endpoint*;
2) Apabila *stateful* manajemen sesi digunakan, *remote endpoint* dapat menggunakan *session identifier* secara acak untuk mengautentikasi permintaan klien tanpa mengirimkan kredensial pengguna;
3) Apabila autentikasi *stateless* berbasis token digunakan, maka harus dipastikan bahwa *server* menyediakan token yang telah ditandatangani menggunakan algoritma yang aman;
4) Harus dipastikan bahwa *remote endpoint* memutus sesi yang ada saat pengguna sudah *log out*;
5) Harus ada pengaturan sandi pada *remote endpoint*;
6) Pembatasan terhadap jumlah percobaan *login* pada *remote endpoint*;
7) Sesi pada *remote endpoint* dibatalkan apabila pengguna tidak aktif selama periode yang ditentukan dan token akses telah kedaluwarsa; dan
8) Metode otorisasi harus ditentukan dan diterapkan pada *remote endpoint*.

d. Komunikasi Jaringan
1) Data yang ditransmisikan melalui jaringan, dienkripsi menggunakan *Transport Layer Security* (TLS);
2) Konfigurasi TLS disesuaikan dengan *best practice* yang masih relevan dengan kondisi saat ini, atau sebisa mungkin diterapkan semaksimal mungkin jika sistem operasi perangkat *mobile* tidak dapat mendukung sepenuhnya;
3) Aplikasi mampu memverifikasi sertifikat X.509 dari *endpoint* yang diterima secara *remote* jika *secure channel* tersedia. Sertifikat yang diterima hanya sertifikat yang ditandai oleh CA yang dipercaya;
4) Aplikasi menyimpan sertifikatnya sendiri, atau menyematkan atau "*pin*" sertifikat dan/ atau *public key* dari *endpoint*. Selanjutnya aplikasi tidak membuat koneksi dengan *endpoint* yang menawarkan sertifikat dan/ atau *key* lain, meskipun telah ditandai oleh CA yang dipercaya;
5) Aplikasi tidak hanya mengandalkan pada satu kanal komunikasi yang tidak aman (seperti email atau SMS) untuk operasi yang bersifat *critical*, seperti pada saat kegiatan pendaftaran, dan *recovery/* pemulihan akun; dan
6) Aplikasi dapat bergantung/ atau mempercayai kepada konektivitas yang terkini, dan *library security*.

e. Interaksi *Platform*
   1) Aplikasi hanya meminta sedikit izin/ *permission* yang sangat dibutuhkan saja;
   2) Seluruh masukan/ *input* yang berasal dari sumber eksternal dan pengguna harus divalidasi dan jika perlu dibersihkan, termasuk data yang diterima melalui *User Interface*, mekanisme pemrosesan yang menggunakan komunikasi seperti URL, dan sumber jaringan;
   3) Aplikasi tidak mengekspor fungsi yang sensitif melalui fasilitas pemrosesan yang menggunakan komunikasi;
   4) Penggunaan JavaScript pada WebView dinonaktifkan, kecuali jika diperlukan secara eksplisit;
   5) JavaScript pada WebView harus dinonaktifkan kecuali sangat dibutuhkan;
   6) WebView dikonfigurasi untuk hanya mengizinkan *protocol handler* yang dibutuhkan saja, seperti HTTPS. Seharusnya *handler* yang berpotensi membahayakan dinonaktifkan;
   7) Jika metode *native* aplikasi terekspose hingga ke WebView, pastikan bahwa WebView hanya memproses JavaScript yang terkandung di dalam *package* aplikasi;
   8) Aplikasi mampu bertahan dari serangan *screen overlay*; dan
   9) *Cache*, penyimpanan, dan sumber daya (JavaScript, dll.) yang termuat dalam WebView harus dibersihkan sebelum WebView tersebut dimusnahkan.

f. Kualitas Kode dan Pengaturan *Build*
   1) Aplikasi ditandatangani dan disediakan dengan sertifikat yang valid, yang kunci privatnya dilindungi dengan benar;
   2) Aplikasi telah dibuat dalam mode rilis, dengan tingkat yang sesuai untuk versi rilis (misalnya *non-debuggable*, dsb.);
   3) Kode *debugging* dan kode bantuan pengembang harus dihapuskan. Aplikasi tidak mencatat kesalahan yang bertele-tele atau pesan *debug*;
   4) Semua komponen pihak ketiga yang digunakan oleh aplikasi *mobile* (seperti *library* dan *framework*) diidentifikasi dan diperiksa untuk mengetahui kerentanannya;
   5) Aplikasi menangkap dan menangani semua eror yang memungkinkan untuk ditangani;
   6) Dalam kode yang tidak dikelola, memori dialokasikan, dibebaskan, dan digunakan dengan aman; dan
   7) Mengaktifkan fitur keamanan gratis yang sudah disediakan oleh *toolchain* seperti *byte-code minification*, *stack protection*, PIE *support* dan *automatic reference counting*.

g. Ketahanan
   1) Aplikasi dapat mendeteksi dan/ atau merespon terhadap perangkat yang sudah di-*root* atau di-*jailbreak* dengan memberi peringatan kepada pengguna atau langsung menghentikan aplikasi;
   2) Aplikasi mencegah *debugging* dan/atau mendeteksi, dan merespons terhadap *debugger* yang terpasang. Semua protokol *debug* yang tersedia harus ditangani;
   3) Aplikasi dapat mendeteksi dan/ atau merespon perubahan pada *executable file* dan data kritikal dalam *sandbox*-nya sendiri dengan melakukan penolakan terhadap perubahan tersebut;
   4) Aplikasi dapat mendeteksi dan/ atau merespon terhadap keberadaan *tools* dan *frameworks reverse engineering* yang banyak digunakan di dalam perangkat;
   5) Aplikasi dapat mendeteksi dan/ atau merespon terhadap dijalankannya aplikasi menggunakan *emulator*;

6) Aplikasi dapat mendeteksi dan/ atau merespon terhadap perubahan kode dan data di ruang memori;
7) Aplikasi menerapkan fungsi *device binding* menggunakan beberapa properti unik dari perangkat; dan
8) Aplikasi menerapkan metode *obfuscation*, contohnya enkripsi.

BAB XVI
Keamanan Sistem Penghubung Layanan

A. Tujuan

B. Ruang Lingkup

Ruang lingkup kebijakan sistem penghubung layanan, antara lain sebagai berikut:

1. keamanan interoperabilitas data dan informasi;
2. kontrol sistem integrasi;
3. kontrol perangkat *integrator*;
4. keamanan API dan *web service*; dan
5. keamanan migrasi.

C. Referensi

D. Kebijakan

1. Keamanan Interoperabilitas Data dan Informasi

a. Prinsip-prinsip Interoperabilitas Data dan Informasi, antara lain:
   1) aman dan handal, merupakan kemampuan sistem elektronik untuk melindungi terhadap gangguan dan ancaman secara fisik dan non-fisik serta beroperasinya sesuai dengan kebutuhan dari penggunanya.
   2) dapat digunakan kembali (*reusable*), merupakan karakteristik dari komponen yang dibangun dan dikembangkan agar dapat dimanfaatkan secara berulang tanpa perlu dikembangkan lagi oleh pihak yang membutuhkan.
   3) dapat dibaca (*readable*), merupakan kemampuan untuk mengakses dan memahami komponen Interoperabilitas Data dan Informasi.
   4) dapat dikembangkan lebih lanjut secara mandiri, merupakan karakteristik dari komponen Interoperabilitas Data dan Informasi yang memberi kemudahan bagi pengembangan lebih lanjut tanpa perlu melibatkan pengembang awal.
   5) dapat diperiksa (*auditable*), merupakan karakteristik dari komponen interoperabilitas Data dan Informasi yang memberikan kemudahan bagi yang memiliki kewenangan untuk melakukan pengamatan, verifikasi, pengujian dan pemeriksaan
   6) dapat diukur kinerjanya, merupakan karakteristik yang memberikan kemudahan bagi yang memiliki kewenangan untuk melakukan pengukuran keandalan, kinerja, kualitas, kesesuaian dengan peruntukan dan saran.
   7) dapat diawasi dan dinilai tingkat pemanfaatannya, merupakan komponen yang memberikan kemudahan bagi yang memiliki kewenangan untuk melakukan pengukuran berjalannya fungsi sebagaimana mestinya, jumlah layanan yang dimanfaatkan dalam rangka mengukur efektivitas dan efisiensi.
   8) dapat dibagi pakaikan antara sistem elektronik yang berbeda karakteristik, merupakan komponen digunakan untuk memastikan terjadi pemanfaatan bersama oleh penyelenggara Sistem Elektronik dan Sistem Elektronik yang berbeda, sehingga terwujudnya keseragaman, keterpaduan dan efisiensi.

b. Penerapan sistem tanda tangan elektronik tersertifikasi mengacu kepada Bab XIV Tanda Tangan Elektronik;

c. Penerapan sistem enkripsi data mengacu kepada Bab XV Data dan Informasi bagian Kebijakan Nomor 2;

d. Proses memastikan data dan informasi selalu dapat diakses otoritasnya mengacu kepada Bab XV Data dan Informasi bagian Kebijakan - D.5 Ketersediaan;

e. Penerapan sistem *hash function* pada *file* mengacu pada Bab XV Data dan Informasi bagian Kebijakan - D.1 Kerahasiaan.

2. Kontrol Sistem Integrasi

a. Memastikan adanya penerapan protokol *secure socket layer* atau protokol *transport layer security* versi terkini pada sesi pengiriman data dan informasi;
b. Memastikan adanya penerapan *internet protocol security* untuk mengamankan transmisi data dalam jaringan berbasis *transmission control protocol/ internet protocol*;
c. Memastikan adanya penerapan sistem anti *distributed denial of service*;
d. Memastikan adanya penerapan autentikasi untuk memverifikasi identitas eksternal antar Layanan SPBE yang terhubung;
e. Memastikan penerapan manajemen keamanan sesi;
f. Memastikan penerapan pembatasan akses pengguna berdasarkan otorisasi yang telah ditetapkan;
g. Memastikan penerapan validasi input;
h. Memastikan penerapan kriptografi pada verifikasi statis;
i. Memastikan penerapan sertifikat elektronik pada *web authentication*;
j. Memastikan penerapan penanganan eror dan pencatatan *log*;
k. Memastikan penerapan proteksi data dan jalur komunikasi;
l. Memastikan penerapan pendeteksi virus untuk memeriksa beberapa konten *file*;
m. Memastikan penetapan perjanjian tingkat layanan dengan standar paling rendah 95% (sembilan puluh lima per seratus*)*; dan
n. Memastikan sistem integrasi tidak memiliki kerentanan yang berpotensi menjadi celah peretas.

3. Kontrol Perangkat *Integrator*

a. Memastikan penggunaan sistem operasi dan perangkat lunak dengan *security patches* terkini;
b. Memastikan penggunaan antivirus dan anti-*spyware* terkini;
c. Memastikan fitur keamanan pada peramban *web* diaktifkan;
d. Menerapkan *firewall* dan *host-based intrusion detection systems*;
e. Memastikan pencegahan terhadap instalasi perangkat lunak yang belum terverifikasi;
f. Memastikan pencegahan terhadap akses situs yang tidak sah; dan
g. Memastikan sistem *recovery* dan *restore* pada integrator telah diaktifkan.

4. Keamanan API dan *Web Service*

Mengacu ke Bab XVI Keamanan Aplikasi Bagian - Keamanan Aplikasi berbasis *Website* nomor 12 - Keamanan API dan *Web Service*.

5. Keamanan Migrasi

a. Memastikan migrasi data dilakukan secara bertahap dan terprogram oleh sistem;
b. Memastikan aplikasi yang menggunakan sistem basis data yang lama tetap dipertahankan sampai sistem pendukung basis data baru dapat berjalan atau berfungsi dengan normal;
c. Memastikan pendokumentasian format sistem basis data lama secara rinci;
d. Memastikan dilakukannya pencadangan seluruh data yang tersimpan pada sistem sebelum melakukan migrasi data;
e. Memastikan penerapan teknik kriptografi pada proses penyimpanan dan pengambilan data; dan

f. Memastikan dilakukannya validasi data ketika proses migrasi data telah selesai.

BAB XVII
Keamanan Jaringan Intra

A. Tujuan

B. Ruang Lingkup

Ruang lingkup kebijakan keamanan jaringan intra, antara lain sebagai berikut:

1. aspek administrasi keamanan jaringan intra;
2. kontrol akses dan autentikasi;
3. persyaratan perangkat dan aplikasi keamanan jaringan intra;
4. kontrol keamanan *gateway*;
5. kontrol keamanan *access point* pada jaringan nirkabel; dan
6. kontrol konfigurasi *access point* pada jaringan nirkabel.

C. Referensi

D. Kebijakan

1. Administrasi Keamanan Jaringan Intra

a. Penyusunan dan Evaluasi Dokumen Arsitektur Jaringan Intra Pemerintah
   a) Pemerintah Kota Salatiga wajib memiliki Arsitektur Infrastruktur yang didalamnya memuat Arsitektur Jaringan Intra Pemerintah.
   b) Penyusunan Arsitektur Jaringan Intra Pemerintah, terdiri atas:
      a) penyelarasan Sistem Pemerintah Berbasis Elektronik (SPBE) dengan Visi dan Misi;
      b) mendefinisikan arahan strategik;
      c) melakukan analisis kondisi SPBE saat ini;
      d) melakukan analisis kondisi SPBE ideal; dan
      e) pendefinisian peta jalan SPBE.
   c) Proses evaluasi Arsitektur Jaringan Intra Pemerintah, meliputi:
      a) model tingkat kematangan;
      b) metode penilaian tingkat kematangan SPBE;
      c) kriteria tingkat kematangan SPBE;
      d) metode pelaksanaan penilaian;
      e) kuesioner pemantauan dan evaluasi.

b. Identifikasi Aset Infrastruktur Jaringan
   a) proses identifikasi aset infrastruktur jaringan mengacu kebijakan pengelolaan aset.
   b) aset infrastruktur jaringan yang diidentifikasi, antara lain:
      a) merk perangkat;
      b) model dan tipe;
      c) kegunaan;
      d) *serial number*;
      e) *product number*;
      f) jumlah *port*;
      g) kapasitas dari prosesor, RAM dan *hard disk*;
      h) versi *firmware*;
      i) lokasi rak; dan
      j) tanggal pembelian dan instalasi.

c. Penyusun dan penetapan Standar Operasional Prosedur (SOP) Jaringan Intra, meliputi:
   a) perencanaan jaringan intra;
   b) pengembangan jaringan intra;
   c) pengoperasian jaringan intra; dan
   d) pemeliharaan jaringan intra

2. Kontrol Akses dan Autentikasi

a. Kontrol akses secara fisik dapat dilakukan dengan melakukan:
   1) Memisahkan aset milik penyedia jasa teknologi informasi dengan aset internal milik pemerintah kota salatiga pada tempat yang terpisah; dan
   2) Melakukan pembatasan akses secara fisik kepada perangkat jaringan intra dengan cara meletakkan perangkat di dalam rak yang terkunci.

b. Kontrol akses secara *logic*
   1) Penggunaan akses ke jaringan intra harus dilakukan dengan menerapkan mekanisme autentikasi. Hal ini dapat dilakukan sesuai dengan Kebijakan Pengendalian Akses;
   2) Penerapan keamanan komunikasi pada jaringan intra, seperti segmentasi jaringan, pembatasan protocol, port dan layanan yang tidak digunakan;
   3) Penerapan penyaringan tautan dan pemblokiran akses ke situs yang tidak terpercaya baik dengan mekanisme *blacklist*, *whitelist*, atau mekanisme lainnya yang bertujuan membatasi akses ke situs berbahaya;
   4) Penerapan fungsi *honeypot* sebagai umpan jika terjadi serangan siber, dan memanfaatkan hasil serangan yang masuk untuk menganalisis celah keamanan;
   5) Penerapan *virtual private network* (VPN) dan mengaktifkan fungsi enkripsi pada jalur komunikasi yang digunakan;
   6) Pemberian akses untuk melakukan instalasi perangkat lunak dan/ atau mengubah konfigurasi sistem dalam jaringan intra hanya diberikan pada administrator;
   7) Penerapan *Secure Endpoints;*
   8) Penerapan Pemblokiran layanan yang tidak dikenal;
   9) Penerapan *secure socket layer* atau *transport layer security* versi terkini pada jalur akses Jaringan Intra; dan
   10) Penerapan *server* perantara saat *client* mengakses *server database* dalam rangka pemeliharaan

3. Perangkat dan Aplikasi Keamanan Jaringan Intra

a. Penerapan perangkat *Security information and event management* (SIEM) untuk melakukan *network logging and monitoring;*
b. Penerapan sistem deteksi dini kerentanan keamanan perangkat jaringan dengan menggunakan perangkat *Intrusion Detection System* dan/ atau *Intrusion Prevention System;*
c. Penggunaan perangkat *Firewall;*
d. Penerapan enkripsi pada jaringan komunikasi dengan menggunakan *Virtual Private Network (VPN);*
e. Penerapan pengelolaan infrastruktur jaringan intra dan sistem komputer untuk memastikan keadaan perangkat selalu dalam kondisi terkini;
f. Penggunaan perangkat *Web Application Firewall (WAF)* untuk membatasi akses ke *Website* milik Pemerintah*;*
g. Penerapan *Redundant Device* untuk menjaga *High Availability* pada perangkat jaringan;
h. Penerapan pengunduhan perangkat lunak melalui *enterprise software distribution system;* dan
i. Penerapan sertifikat elektronik yang dijamin oleh penyedia layanan. Hal ini dapat dilakukan dengan mengacu pada Kebijakan Keamanan data dan informasi bagian keaslian.

4. Kontrol Keamanan *Gateway*

a. Penerapan perangkat *Firewall* yang digunakan untuk menyaring dan membatasi lalu lintas data yang masuk pada jaringan intra;
b. Penerapan kontrol keamanan pada fitur akses jarak jauh (*remote access*) pada perangkat *gateway,* yang salah satu penerapannya dapat menggunakan Protokol yang aman, serta hanya dapat diakses oleh pihak yang sudah terdaftar;
c. Penerapan DMZ (*Demilitarized Zone*) pada jaringan intra pemerintah, agar tidak terhubung langsung dengan jaringan publik;
d. Penerapan manajemen lalu lintas data pada *gateway* dilakukan dengan membatasi *bandwidth* berdasarkan kebutuhan; dan
e. Penerapan *hardening* pada *gateway,* seperti membatasi *port* yang aktif hanya yang sesuai dengan kebutuhan, menggunakan protokol yang aman, dan atau menerapkan *port knocking.*

5. Kontrol Keamanan *Access Point* pada Jaringan Nirkabel

a. Melakukan penerapan kontrol keamanan pada *Access Point* dengan menerapkan teknologi enkripsi terkini seperti menggunakan WPA2 Standard dan/ atau WPA3;
b. Melakukan penerapan pembatasan akses dengan mekanisme pendaftaran *Media Access Control (*MAC*) address* pada *address filtering*;
c. Melakukan penerapan *Dedicated Service Set Identifier (SSID)* yang dilakukan dengan menyediakan 1 (satu) SSID pada 1 (satu) device *Access Point;*
d. Melakukan penerapan pembatasan jangkauan radio transmisi dengan menyesuaikan ukuran gedung, bangunan, dan/ atau ruangan. Hal ini dilakukan untuk membatasi pihak-pihak yang dapat terhubung ke jaringan nirkabel;
e. Melakukan penerapan *blacklist* dan/ atau *whitelist* untuk melakukan pembatasan perangkat yang terhubung ke jaringan secara tidak sah;
f. Melakukan penerapan manajemen kerentanan/ *vulnerability* dengan melaksanakan *vulnerability assessment* dan/ atau *penetration testing* secara rutin; dan
g. Memastikan kondisi perangkat *access point* selalu dalam kondisi terkini dengan melakukan *update patch* perangkat lunak.

6. Kontrol Konfigurasi *Access Point* pada Jaringan Nirkabel

a. Melakukan penerapan kata sandi/ atau *password* yang kuat, sesuai dengan karakteristik yang diatur pada Kebijakan Keamanan Aplikasi Berbasis Website bagian Autentikasi.
b. Memastikan penerapan protokol *Authentication*, *Authorization,* dan *Accounting (*AAA) menggunakan Radius dan/ atau Tacacs untuk user *management* atau autentikasi *administrator access point;*
c. Memastikan penerapan akses konfigurasi jarak jauh pada *Access Point* hanya dapat dilakukan dari jaringan internal dengan memanfaatkan *Virtual Private Network* (VPN) yang hanya digunakan saat darurat saja;
d. Memastikan penerapan pemisahan/ segmentasi jaringan baik secara logika maupun fisik untuk pengunjung dan untuk keperluan internal;
e. Memastikan penerapan *hardening*/ atau penguatan keamanan, seperti menonaktifkan layanan, *port*, atau aplikasi yang tidak digunakan.

BAB VIII
Keamanan Pusat Data

A. Tujuan

B. Ruang Lingkup

Ruang lingkup kebijakan keamanan pusat data, antara lain sebagai berikut:

1. persyaratan keamanan fisik dan manajemen pusat data; dan
2. persyaratan koneksi perangkat ke Pusat Data.

C. Referensi

1. SNI 8799-1:2019 tentang Teknologi Informasi - Pusat Data - Bagian 1: Panduan Spesifikasi Teknis Pusat Data;

D. Kebijakan

1. Keamanan Fisik dan Manajemen Pusat Data

a. Lokasi

Lokasi dari Pusat Data harus memenuhi ketentuan berikut, antara lain:

1) Bangunan harus berada pada lokasi yang aman berdasarkan kajian indeks rawa bencana Indonesia;
2) Bangunan harus mempunyai akses jalan yang cukup dan fasilitas parkir;
3) Lokasi sebaiknya berada di kawasan yang memiliki temperatur sekitar yang rendah dan menghindari kawasan yang memiliki kelembapan tinggi.
4) Tidak berada pada lokasi rawa huru hara, seperti perkampungan padat atau kumuh;
5) Jarak dengan arteri lalu lintas, jalan raya utama dan jalur kereta api lebih dari 91 meter; dan
6) Jarak ke bandara utama dan/ atau pelabuhan lebih dari 1,6 kilometer.

b. Persyaratan Bangunan dan Arsitektur

Berikut ini persyaratan bangunan dan arsitektur Pusat Data, antara lain:

1) Ruang komputer tidak berada di bawah are perpipaan (*plumbing*) seperti kamar mandi, toilet, dapur, laboratorium dan ruang mekanik kecuali jika sistem pengendalian air disiapkan;
2) Tiap jendela ruang komputer yang menghadap ke sinar matahari harus ditutup untuk mencegah paparan panas;
3) Bangunan harus memiliki area bongkar muat yang memadai untuk menangani penghantaran barang/ peralatan;
4) Area parkir karyawan dan pengunjung dipisahkan secara fisik dengan pagar;
5) Area parkir dengan area bongkar muat dipisahkan secara fisik dengan pagar; dan
6) Area parkir pengunjung dengan tembok perimeter pusat data dipisahkan dengan penghalang fisik untuk mencegah kendaraan melaju lebih dekat.

c. Kontrol Akses dan Keamanan Fisik Pusat Data

Berikut ini merupakan ketentuan terkait kontrol akses dan keamanan fisik pusat data, antara lain:

1) Memiliki pengamanan fisik di setiap jendela yang memungkinkan akses langsung ke Pusat Data;
2) Pusat Data harus diamankan selama 24 jam, dengan minimal satu orang petugas per *shift*. *Shift* tersebut dibagi sesuai dengan ketentuan pada Dinas Komunikasi dan Informatika Kota Salatiga;

3) Harus ada perangkat sistem pemantau visual (seperti CCTV) untuk memantau dan merekam setiap aktivitas pada ruang komputer, ruang mekanik dan kelistrikan, ruang telekomunikasi dan kawasan kantor;
4) Akses ke dalam ruang komputer menggunakan perangkat yang memiliki mekanisme autentikasi (seperti PIN, kartu gesek, kartu nirkontak atau akses biometrik);
5) Tamu/ pengunjung harus dilengkapi dengan tanda masuk dan tanda pengenal agar dapat masuk ke dalam ruang komputer, ruang mekanikal dan kelistrikan, ruang telekomunikasi dan kawasan kantor. Setiap orang yang masuk ke dalam ruangan sebagaimana dimaksud di atas harus memiliki izin;
6) Menerapkan pengamanan berlapis pada kawasan Pusat Data atau area Pusat Data dengan menerapkan 6 (enam) *layer* keamanan, yaitu:
   a) *Layer* 1, *perimeter defense* (area pintu utama kawasan Pusat Data);
   b) *Layer* 2, *clear zone* (area gedung dan parkir kendaraan);
   c) *Layer* 3, *reception area* (area pintu masuk gedung Pusat Data);
   d) *Layer* 4, *hallway/ gray space* (area menuju pintu utama ruang Pusat Data);
   e) *Layer* 5, Ruang Pusat Data/ *white space* (pintu utama ruang Pusat Data); dan
   f) *Layer* 6, Kabinet Pusat Data/ *white space*) area utama di rak kabinet Pusat Data).

d. Peringatan Kebakaran, Deteksi Asap dan Pemadam Kebakaran

Berikut ini merupakan ketentuan terkait peringatan kebakaran, deteksi asap dan pemadam kebakaran, antara lain:

1) Jumlah dan lokasi pintu darurat kebakaran sesuai dengan peraturan perundangan;
2) Pintu darurat kebakaran harus dapat dibuka ke arah luar;
3) Lampu darurat, tanda keluar dan titik kumpul darurat diletakkan diletakkan pada lokasi sesuai ketentuan perundang-undangan;
4) Dinding dan pintu ke ruang komputer, ruang mekanikal dan kelistrikan, ruang telekomunikasi dan kawasan kritikal lainnya memiliki tingkat terbakar (*fire rating*) sesuai dengan peraturan perundangan;
5) Ruang komputer harus diproteksi dengan sistem deteksi asap;
6) Seluruh sistem deteksi asap bangunan harus diintegrasikan ke satu alarm bersama;
7) Catatan pemeliharaan yang mencakup seluruh aspek yang berkaitan dengan deteksi api dan pemadaman harus tersedia untuk keperluan pemeriksaan;
8) Bukti pelatihan staf pada simulasi pengendalian kebakaran harus tersedia;
9) Pemadam kebakaran harus ditempatkan sesuai ketentuan peraturan perundang-undangan;
10) Semua tanda peringatan kebakaran harus ditempatkan pada posisinya sesuai ketentuan peraturan perundang-undangan;
11) Seluruh sistem pendeteksi dan pemadam kebakaran harus didesain dan dipasang oleh petugas yang memiliki kualifikasi dan didesain sesuai standar internasional/ nasional atau regulasi nasional;

12) Jika ruang komputer, ruang telekomunikasi, dan ruang mekanikal dan kelistrikan memiliki sistem *sprinkler*, maka sistem tersebut harus tipe *pre-action*; dan
13) Jika ruang atau bangunan yang berdekatan dengan lokasi pusat data tidak memiliki sistem *sprinkler*, maka risiko kebakaran harus dikaji.

e. Penyediaan Catu Daya

Berikut ini merupakan ketentuan terkait penyediaan catu daya, antara lain:

1) Kabel daya masuk ke dalam bangunan dan diterminasi di ruang penyambungan listrik yang andal yang berisikan seluruh penyambungan dan pengukuran yang penting;
2) Daya yang tersedia dari penyedia listrik utama harus paling sedikit 20% lebih besar dari proyeksi beban puncak dimana pusat data berada;
3) Tersedianya catu daya listrik alternatif (seperti generator *standby*) dengan kapasitas yang memadai untuk operasional paling sedikit 3 jam selama kejadian gangguan listrik utama;
4) Perangkat TIK (Teknologi Informasi dan Komunikasi) harus diproteksi dengan *Uninterruptible Power Supply* (UPS) atau catu daya cadangan lainnya;
5) Kapasitas penyimpanan energi UPS atau catu daya cadangan lainnya harus memadai untuk memasok beban TIK sehingga cukup waktu bagi catu daya alternatif mencapai keadaan tunak *(steady state*) untuk memikul beban perangkat TIK;
6) Kapasitas UPS harus lebih besar dari proyeksi beban puncak perangkat TIK. Kapasitas beban rata-rata tidak lebih besar dari 80% kapasitas UPS;
7) UPS memiliki sistem pelaporan dan pemantauan kinerja serta sistem peringatan;
8) UPS yang digunakan telah memilki jaminan dari pabrikan untuk dapat berfungsi sesuai spesifikasinya;
9) Bangunan harus dilengkapi dengan sistem proteksi petir;
10) Kabel komunikasi tembaga dari luar gedung diproteksi dengan peredam tegangan lebih (*surge supressor*) sebelum masuk ke ruang komputer; dan
11) Ruang komputer memiliki terminal pembumian (*grounding*) tembaga yang menjadi titik acuan pembumian ruangan tersebut.

f. Penyediaan Pendingin dan Ventilasi

Berikut ini merupakan ketentuan terkait penyediaan pendingin dan ventilasi, antara lain:

1) Ruang Pusat Data dijaga dan dikendalikan oleh temperatur dengan suhu antara 18 - 24°C;
2) Ruang Pusat Data dijaga dan dikendalikan kelembapan ruangannya dengan kelembapan antara 50-55%;
3) Peralatan pengkondisian udara harus dihubungkan ke catu daya utama dan didukung oleh catu daya alternatif; dan
4) Peralatan pengkondisian udara harus dihubungkan ke catu daya utama dan didukung oleh catu daya alternatif. Jika ruang komputer menggunakan sistem ventilasi detektor asap harus terpasang pada saluran udara masuk, dan harus dapat menghentikan udara masuk jika asap terdeteksi.

g. Penyediaan Pengkabelan dan Manajemen Kabel

Berikut ini merupakan ketentuan terkait penyediaan pengkabelan dan manajemen kabel, antara lain:

1) Sistem pengkabelan yang digunakan untuk konektivitas ke setiap rak sesuai dengan standar nasional/ internasional;
2) Seluruh pengkabelan interior dengan tipe tidak mudah terbakar (*low flammability*);
3) Setiap rak memiliki akses ke sistem saluran kabel, di atas atau di bawahnya, yang memungkinkan kabel-kabel dapat ditata secara baik antar rak;
4) Kabel daya satu fase dan kabel data tembaga harus dipisahkan paling sedikit 20cm;
5) Kabel daya tiga fase dan kabel data tembaga harus dipisahkan paling sedikit 60cm;
6) Kabel yang melewati dinding dilindungi terhadap bahaya api sesuai ketentuan peraturan perundang-undangan;
7) Kabel tidak boleh diletakkan di pintu, lantai, atau digantung antar rak;
8) Setiap kabel memiliki label identifikasi yang unik pada kedua ujung awal dan akhir, jika perlu terdapat data pemilik;
9) Setiap rak peralatan memiliki label identifikasi, jika perlu terdapat data pemilik;
10) Kabel input telekomunikasi eksternal dihubungkan di area atau ruang telekomunikasi tersendiri;
11) Jika are telekomunikasi terpisah dari ruang komputer maka harus memiliki sistem pengkondisi udara, proteksi kebakaran, kelistrikan yang sama dengan standar ruang komputer; dan
12) Seluruh item perangkat logam berisi kabel harus dibumikan.

h. Sistem Manajemen dan Pemantauan
1) Ruang komputer memiliki paling sedikit satu sensor temperatur ruang dan satu sensor kelembapan ruang; dan
2) Ruang telekomunikasi dan ruang mekanikal dan kelistrikan memiliki sebuah sensor temperatur dan sensor kelembapan ruang.

i. Aset pada Pusat Data yang dapat didokumentasi antara lain:
1) Perangkat Server;
2) Perangkat Komputer;
3) Perangkat Jaringan; dan
4) Perangkat Pendukung, seperti:
   a) Pengkondisi Suhu dan Kelembapan Udara (AC, Termometer, Hidrometer atau pengkondisi suhu dan kelembapan udara lainnya);
   b) UPS (*Uninterruptible Power Supply*);
   c) Generator;
   d) *Raised Floor*;
   e) Pendeteksi asap/ api/ panas;
   f) Sistem Pemadam Api; dan
   g) CCTV.

j. Informasi yang harus dicatat terhadap aset-aset tersebut antara lain:
1) Lokasi
   a) Bangunan dan lantai;
   b) Lokasi rak dan item utama dari perangkat;
   c) Denah rak; dan
   d) Interkonektivitas fisik dan logik dari peralatan.
2) Nomor Seri
3) Data Pengadaan
4) Kontak Rinci Pabrikan
5) Tanggal Kalibrasi (jika diperlukan)

k. Seluruh konfigurasi dan prosedur operasi harus didokumentasikan termasuk di dalamnya:
   1) Perubahan konfigurasi; dan
   2) *Set-point default*.

l. Daftar kontak harus tersedia dan mencatat seluruh staf pusat data, fungsi dan kontak rinci, pemasok, perusahaan pemeliharaan dan layanan darurat.

m. Setiap perangkat yang membutuhkan pemeliharaan harus memiliki catatan pemeliharaan yang merinci, seperti nama perangkat, tanggal pemeliharaan, hasil dan kontak rinci petugas yang melakukan pemeliharaan.

2. Koneksi Perangkat ke Pusat Data

1. Harus memastikan keamanan dari perangkat yang akan melakukan koneksi ke infrastruktur Pusat Data;
2. Apabila terdapat perangkat terhubung ke Pusat Data secara fisik maupun *logic* yang tidak terotorisasi, maka aksesnya harus segera diputus;
3. Akun dengan tingkat akses administrator tidak boleh mengakses server dan perangkat jaringan utama secara *remote*;
4. Personel yang berhak untuk menggunakan komputer di area Pusat Data hanyalah personel yang diberi wewenang untuk mengelola Pusat Data;
5. *Backup* informasi dan perangkat lunak pada Pusat Data secara berkala;
6. Perangkat komputer Pusat Data harus memiliki antivirus ataupun *anti-malware*;
7. Penggunaan *removable media* (*hard disk*, dsb.) hanya dapat dilakukan pada saat *backup* informasi dan perangkat lunak pada Pusat Data;
8. Harus memastikan pengaktifan konfigurasi *port universal serial bus* telah mendapatkan izin dari personel yang berwenang;
9. Setiap perangkat yang akan terkoneksi ke infrastruktur Pusat Data harus dipastikan menggunakan *internet protocol* (IP) *address* dan *hostname* yang telah ditentukan. Jika perangkat yang terkoneksi ke infrastruktur Pusat Data tidak menggunakan IP *address* dan *hostname* yang telah ditentukan, maka akses perangkat tersebut harus diputus/ diblokir; dan
10. Penerapan *server* perantara saat *client* mengakses *server database* dalam rangka pemeliharaan.

Pj. WALI KOTA SALATIGA,

ttd

SINOENG N. RACHMADI