WALI KOTA CIREBON
PROVINSI JAWA BARAT

PERATURAN WALI KOTA CIREBON
NOMOR 58 TAHUN 2023

TENTANG
SISTEM MANAJEMEN KEAMANAN INFORMASI

DENGAN RAHMAT TUHAN YANG MAHA ESA

WALI KOTA CIREBON,

Menimbang :

a. bahwa untuk melaksanakan Sistem Pemerintahan Berbasis Elektronik di lingkungan Pemerintah Daerah Kota Cirebon, perlu dilakukan pengelolaan keamanan informasi untuk melindungi kerahasiaan, keutuhan dan ketersediaan aset informasi dari berbagai macam ancaman keamanan informasi, baik dari pihak internal maupun eksternal;
b. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, maka perlu menetapkan Peraturan Wali Kota Cirebon tentang Sistem Manajemen Keamanan Informasi.

Mengingat :

1. Pasal 18 ayat (6) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;
2. Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi (Lembaran Negara Republik Indonesia Tahun 1999 Nomor 154, Tambahan Lembaran Negara Republik Indonesia Nomor 3881), sebagaimana telah beberapa kali diubah, terakhir dengan Undang-Undang Nomor 6 Tahun 2023 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 2 Tahun 2022 tentang Cipta Kerja menjadi Undang-Undang (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 41, Tambahan Lembaran Negara Republik Indonesia Nomor 6856);
3. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843), sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251, Tambahan Lembaran Negara Republik Indonesia Nomor 5952);
4. Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 244, Tambahan Lembaran Negara Republik Indonesia Nomor 5587), sebagaimana

telah beberapa kali diubah, terakhir dengan Undang-Undang Nomor 6 Tahun 2023 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 2 Tahun 2022 tentang Cipta Kerja menjadi Undang-Undang (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 41, Tambahan Lembaran Negara Republik Indonesia Nomor 6856);

5. Undang-Undang Nomor 30 Tahun 2014 tentang Administrasi Pemerintahan (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 292, Tambahan Lembaran Negara Republik Indonesia Nomor 5601), sebagaimana telah beberapa kali diubah, terakhir dengan Undang-Undang Nomor 6 Tahun 2023 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 2 Tahun 2022 tentang Cipta Kerja menjadi Undang-Undang (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 41, Tambahan Lembaran Negara Republik Indonesia Nomor 6856);
6. Undang-Undang Nomor 10 Tahun 2023 tentang Provinsi Jawa Barat (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 57, Tambahan Lembaran Negara Republik Indonesia Nomor 6866);
7. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185, Tambahan Lembaran Negara Republik Indonesia Nomor 6400);
8. Peraturan Presiden Republik Indonesia Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
9. Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi (Berita Negara Republik Indonesia Tahun 2016 Nomor 551);
10. Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian untuk Pengamanan Informasi di Pemerintah Daerah (Berita Negara Republik Indonesia Tahun 2019 Nomor 1054);
11. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 5 Tahun 2020 tentang Pedoman Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2020 Nomor 261);
12. 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);
13. Peraturan Daerah Kota Cirebon Nomor 9 Tahun 2016 tentang Pembentukan Produk Hukum Daerah (Lembaran Daerah Kota Cirebon Tahun 2016 Nomor 9), sebagaimana telah diubah dengan Peraturan Daerah Kota Cirebon Nomor 5 Tahun 2020 tentang Perubahan atas Peraturan Daerah Kota Cirebon Nomor 9 Tahun 2016 tentang Pembentukan Produk Hukum Daerah (Lembaran Daerah Kota Cirebon Tahun 2020 Nomor 5);

14. Peraturan Daerah Kota Cirebon Nomor 5 Tahun 2022 tentang Penyelenggaraan Komunikasi dan Informatika, Statistik serta Persandian (Lembaran Daerah Kota Cirebon Tahun 2022 Nomor 5, Tambahan Lembaran Daerah Kota Cirebon Nomor 120);
15. Peraturan Daerah Kota Cirebon Nomor 3 Tahun 2023 tentang Urusan Pemerintahan yang Diselenggarakan oleh Pemerintah Daerah Kota Cirebon (Lembaran Daerah Kota Cirebon Tahun 2023 Nomor 3, Tambahan Lembaran Daerah Nomor128);
16. Peraturan Wali Kota Cirebon Nomor 29 Tahun 2021 tentang Kedudukan, Struktur Organisasi, Tugas dan Fungsi, serta Tata Kerja Dinas Komunikasi, Informatika dan Statistik Kota Cirebon (Berita Daerah Kota Cirebon Tahun 2021 Nomor 29), sebagaimana telah diubah dengan Peraturan Wali Kota Cirebon Nomor 96 Tahun 2021 tentang Perubahan atas Peraturan Wali Kota Cirebon Nomor 29 Tahun 2021 tentang Kedudukan, Struktur Organisasi, Tugas dan Fungsi, serta Tata Kerja Dinas Komunikasi, Informatika dan Statistik Kota Cirebon (Berita Daerah Kota Cirebon Tahun 2021 Nomor 99);
17. Peraturan Wali Kota Cirebon Nomor 61 Tahun 2021 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik Pada Pemerintah Daerah Kota Cirebon (Berita Daerah Kota Cirebon Tahun 2021 Nomor 61), sebagaimana telah diubah dengan Peraturan Wali Kota Cirebon Nomor 1 Tahun 2023 tentang Perubahan atas Peraturan Wali Kota Cirebon Nomor 61 Tahun 2021 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik Pada Pemerintah Daerah Kota Cirebon (Berita Daerah Kota Cirebon Tahun 2023 Nomor 1);

MEMUTUSKAN :

Menetapkan : PERATURAN WALI KOTA TENTANG SISTEM MANAJEMEN KEAMANAN INFORMASI

BAB I
KETENTUAN UMUM
Bagian Kesatu
Pengertian

Pasal 1

Dalam Peraturan Wali Kota ini yang dimaksud dengan:
1. Daerah Kota adalah Daerah Kota Cirebon.
2. Pemerintah Daerah Kota adalah Wali Kota sebagai unsur penyelenggara pemerintah daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan daerah otonom.
3. Wali Kota adalah Wali Kota Cirebon.
4. Wakil Wali Kota adalah Wakil Wali Kota Cirebon.
5. Sekretariat Daerah adalah Sekretariat Daerah Kota Cirebon.
6. Perangkat Daerah adalah unsur Pembantu Wali Kota dan Dewan Perwakilan Rakyat Daerah dalam Penyelenggaraan urusan pemerintahan yang menjadi kewenangan Daerah.

7. Informasi adalah sebuah keterangan, pernyataan, gagasan, atau tanda-tanda yang mengandung nilai, makna, dan pesan, baik data, fakta maupun penjelasannya yang dapat dilihat, didengar, dan dibaca yang disajikan dalam berbagai kemasan dan format sesuai dengan perkembangan teknologi informasi dan komunikasi secara elektronik ataupun non elektronik.
8. Teknologi Informasi adalah suatu teknik yang digunakan untuk mengolah, memproses, mendapatkan, menyusun, menyimpan, memanipulasi data dengan berbagai cara untuk menghasilkan informasi yang berkualitas dan dapat digunakan keperluan pribadi, bisnis, pemerintahan serta merupakan salah satu cara yang strategis untuk pengambilan keputusan.
9. Teknologi Informasi dan Komunikasi yang selanjutnya disingkat TIK adalah sebuah media atau alat bantu yang digunakan untuk memperoleh suatu informasi maupun memberikan informasi kepada orang lain serta dapat digunakan untuk alat berkomunikasi baik satu arah atau dua arah.
10. Sistem adalah kumpulan komponen atau elemen-elemen yang saling berhubungan satu sama lain untuk mencapai suatu tujuan tertentu.
11. Keamanan informasi adalah suatu kondisi untuk melindungi aset yang dimiliki organisasi dari berbagai ancaman pihak internal maupun eksternal untuk menjamin kelanjutan proses bisnis, mengurangi risiko bisnis, serta terjaganya aspek kerahasiaan, integritas dan ketersediaan dari informasi.
12. Sistem Manajemen Keamanan Informasi yang selanjutnya disingkat SMKI adalah sistem manajemen yang meliputi kebijakan, organisasi, perencanaan, penanggung jawab, proses, dan sumber daya yang mengacu pada pendekatan risiko bisnis untuk menetapkan, mengimplementasikan, mengoperasikan, me*monitoring*, mengevaluasi, mengelola, dan meningkatkan keamanan informasi.
13. Aset Informasi adalah unit informasi yang dapat dipahami, dibagi, dilindungi dan dimanfaatkan secara efektif.
14. Aset Pengolahan Informasi adalah suatu perangkat, baik elektronik maupun non-elektronik yang dapat digunakan untuk membuat dan menyunting informasi.
15. Penyimpanan Informasi adalah suatu proses menyimpan informasi dengan menggunakan media, baik elektronik maupun non-elektronik.
16. Perangkat keras adalah semua jenis peranti atau komponen komputer yang bagian fisiknya dapat dilihat secara kasat mata dan dirasakan langsung.
17. Perangkat lunak adalah satu atau sekumpulan program komputer, prosedur, dan/atau dokumentasi yang terkait dalam pengoperasian sistem elektronik.
18. Perangkat lunak sistem adalah jenis perangkat lunak yang digunakan untuk menjalankan atau mengoperasikan perangkat keras, diantaranya yaitu sistem operasi, pemroses bahasa, dan *driver*.

19. Perangkat lunak aplikasi adalah jenis perangkat lunak yang dirancang untuk mencapai kebutuhan pengguna tertentu, diantaranya yaitu pengolah kata, *spreadsheet*, dan *web browser.*
20. *Data Center* atau Pusat Data adalah suatu fasilitas untuk menempatkan sistem komputer dan perangkat-perangkat terkait, seperti sistem komunikasi data dan penyimpanan data.
21. *Computer Security Insident Response Team* yang selanjutnya disingkat CSIRT adalah sebuah organisasi atau tim yang bertanggungjawab untuk menerima, meninjau dan menanggapi laporan dan aktivitas insiden keamanan siber. Tim ini dibentuk dengan tujuan untuk melakukan penyelidikan komprehensif dan melindungi sistem atau data atas insiden keamanan siber yang terjadi pada organisasi.

Bagian Kedua
Maksud dan Tujuan

Pasal 2

(1) Peraturan Wali Kota ini dimaksudkan sebagai pedoman pengelolaan SMKI secara terpadu untuk memastikan terjaganya aspek kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*) pada informasi.
(2) Pengelolaan SMKI sebagaimana dimaksud pada ayat (1), meliputi infrastruktur jaringan komputer, perangkat lunak, dan sumber daya manusia.
(3) Peraturan Wali Kota ini bertujuan untuk memberikan pedoman atau panduan umum kepada seluruh Perangkat Daerah di lingkungan Pemerintah Daerah Kota dalam hal mengelola kebijakan dan standar Sistem Manajemen Keamanan Informasi secara terpadu.

Bagian Ketiga
Ruang Lingkup

Pasal 3

Ruang lingkup Peraturan Wali Kota ini meliputi:
a. pengamanan Informasi;
b. sumber daya;
c. standar dan prosedur pengendalian;
d. manajemen risiko;dan
e. mekanisme penyelenggaraan.

BAB II
PENGAMANAN INFORMASI

Pasal 4

Pengamanan informasi yang diatur dalam Peraturan Wali Kota ini meliputi:
a. aset informasi;
b. aset pengolahan informasi;dan
c. penyimpanan informasi.

Pasal 5

Aset Informasi sebagaimana dimaksud dalam Pasal 4 huruf a, merupakan aset dalam bentuk:

a. fisik, meliputi informasi yang tercetak, tertulis dan tersimpan dalam bentuk fisik seperti di atas kertas, papan tulis, spanduk, atau di dalam buku dan dokumen;dan
b. elektronik, meliputi informasi tercetak, tertulis dan tersimpan dalam bentuk elektronik seperti *database*, pada *file* didalam komputer, ditampilkan pada *website*, layar komputer dan dikirimkan melalui jaringan telekomunikasi.

Pasal 6

Aset pengolahan informasi sebagaimana dimaksud dalam Pasal 4 huruf b, berupa:

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

Pasal 7

Penyimpanan informasi sebagaimana dimaksud dalam Pasal 4 huruf c, menggunakan media:

a. elektronik, meliputi antara lain *server* dan media penyimpanan;dan
b. non elektronik, meliputi antara lain lemari, rak, laci, *filling cabinet*, dan lain-lain.

BAB III
SUMBER DAYA

Pasal 8

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

BAB IV
STANDAR DAN PROSEDUR PENGENDALIAN

Pasal 9

(1) Setiap Perangkat Daerah harus menyusun standar dan prosedur pengendalian kegiatan teknologi informasi yang memenuhi prasyarat keamanan informasi.
(2) Prasyarat keamanan informasi sebagaimana dimaksud pada ayat (1), digunakan untuk mengimplementasikan tindakan dalam mengelola risiko yang meliputi aspek sebagai berikut:
    a. pengendalian umum;
    b. pengendalian organisasi keamanan informasi;
    c. keamanan sumber daya manusia;
    d. pengelolaan aset;
    e. pengendalian akses;
    f. kriptografi;
    g. keamanan fisik dan lingkungan;
    h. keamanan operasional;

i. keamanan komunikasi;
j. keamanan dalam proses akuisisi, pengembangan dan pemeliharaan sistem informasi;
k. hubungan kerja dengan pihak ketiga atau penyedia jasa atau barang;
l. penanganan insiden keamanan informasi;
m. kelangsungan kegiatan;dan
n. kepatuhan.

(3) Uraian lebih lanjut sebagaimana dimaksud pada ayat (2), tercantum dalam Lampiran yang merupakan bagian yang tidak terpisahkan dari Peraturan Wali Kota ini.

Pasal 10

(1) Setiap Perangkat Daerah bertanggung jawab dalam memastikan kegiatan operasional teknologi informasi yang stabil dan aman.
(2) Penyelenggaraan pemrosesan transaksi pada operasional teknologi informasi harus memenuhi prinsip kehati-hatian.
(3) Setiap Perangkat Daerah penyelenggara teknologi informasi wajib mengidentifikasi dan memantau aktivitas operasional teknologi informasi untuk memastikan efektifitas, efesiensi, dan keamanan dari aktivitas tersebut antara lain:
a. menerapkan perimeter fisik dan lingkungan di area kerja dan *Data Center;*
b. mengendalikan hak akses secara memadai sesuai kewenangan yang ditetapkan;
c. menerapkan pengendalian terhadap informasi yang diproses;
d. memastikan ketersediaan dan kecukupan kapasitas layanan jaringan komunikasi baik yang dikelola secara internal maupun oleh pihak lain penyedia jasa;
e. melakukan pemantauan kegiatan operasional Teknologi Informasi termasuk *audit trail*/riwayat;dan
f. melakukan pemantauan terhadap aplikasi yang digunakan oleh Perangkat Daerah maupun pengguna.

BAB V
MANAJEMEN RISIKO

Pasal 11

(1) Setiap Perangkat Daerah penyelenggara teknologi informasi wajib melakukan proses manajemen risiko dalam menerapkan SMKI.
(2) Proses manajemen risiko sebagaimana dimaksud pada ayat (1), meliputi:
a. identifikasi;
b. pengukuran;
c. pemantauan;dan
d. pengendalian atas risiko terkait penggunaan Teknologi Informasi.
(3) Manajemen risiko sebagaimana dimaksud pada ayat (2), meliputi:
a. pengembangan sistem;
b. operasional teknologi informasi;
c. jaringan komunikasi;

d. penggunaan perangkat komputer;
e. pengendalian terhadap informasi;dan
f. penggunaan pihak ketiga sebagai penyedia jasa teknologi informasi.

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

BAB VI
MEKANISME PENYELENGGARAAN

Pasal 12

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

Pasal 13

(1) Setiap Perangkat Daerah harus menerapkan prinsip pengendalian terhadap aktivitas teknologi informasi melalui proses evaluasi dan *monitoring* secara berkala.
(2) Setiap Perangkat Daerah wajib melakukan kegiatan pemantauan dan tindakan koreksi penyimpangan terhadap kontrol keamanan informasi yang berada di bawah tanggung jawabnya meliputi :
a. kegiatan pemantauan secara terus menerus;dan
b. pelaksanaan fungsi pemeriksaan internal yang efektif dan menyeluruh.
(3) Perangkat Daerah penyelenggara teknologi informasi berdasarkan hasil audit, umpan balik dan evaluasi terhadap pengendalian keamanan informasi yang dilakukan, wajib meningkatkan efektivitas SMKI secara berkesinambungan melalui perbaikan terhadap akibat penyimpangan kegiatan teknologi informasi.
(4) Hasil dari tindakan perbaikan dan peningkatan sebagaimana dimaksud pada ayat (3), harus dilaporkan kepada Kepala Perangkat Daerah dan didokumentasikan.

Pasal 14

(1) Apabila terjadi kebocoran informasi yang mempunyai dampak luas pada Perangkat Daerah terkait, Pemerintah Daerah Kota dapat menunjuk CSIRT untuk melakukan investigasi yang diperlukan.
(2) Apabila terjadi kebocoran informasi sebagaimana dimaksud pada ayat (1), dan tidak dapat di tanggulangi oleh Perangkat Daerah, maka Perangkat Daerah dapat merekomendasikan untuk penyelesaiannya kepada CSIRT Kota Cirebon.
(3) Perangkat Daerah penyelenggara teknologi informasi wajib menyediakan akses kepada auditor keamanan informasi sebagaimana dimaksud pada ayat (1), untuk melakukan pemeriksaan seluruh aspek terkait penyelenggaraan teknologi informasi.

BAB VII
KETENTUAN PENUTUP

Pasal 15

Peraturan Wali Kota ini mulai berlaku pada tanggal diundangkan.

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

Ditetapkan di Cirebon
pada tanggal 6 Juli 2023

WALI KOTA CIREBON,

ttd,

NASHRUDIN AZIS

Diundangkan di Cirebon
pada tanggal 6 Juli 2023

SEKRETARIS DAERAH KOTA CIREBON,

ttd,

AGUS MULYADI

BERITA DAERAH KOTA CIREBON TAHUN 2023 NOMOR 58

Salinan sesuai dengan aslinya,
KEPALA BAGIAN HUKUM,

FERY DJUNAEDI, SH., MH
Pembina Tk. I (IV/b)
NIP. 19711228 199803 1 002

LAMPIRAN
PERATURAN WALI KOTA CIREBON
NOMOR 58 TAHUN 2023
TENTANG
SISTEM MANAJEMEN KEAMANAN INFORMASI

KEBIJAKAN DAN STANDAR SISTEM MANAJEMEN KEAMANAN INFORMASI DI LINGKUNGAN PEMERINTAH DAERAH KOTA

BAB I
PENGENDALIAN UMUM

A. TUJUAN

Kebijakan dan standar Sistem Manajemen Keamanan Informasi yang selanjutnya disingkat SMKI ini disusun dengan tujuan memberikan pedoman atau panduan umum untuk seluruh Perangkat Daerah di lingkungan Pemerintah Daerah Kota dalam hal mengelola kebijakan dan standar Sistem Manajemen Keamanan Informasi secara terpadu, sehingga aset informasi yang dimiliki setiap Perangkat Daerah dapat terlindungi dari aspek kerahasiaan *(confidentiality)*, keutuhan *(integrity)*, dan ketersediaan *(availability)*.

B. RUANG LINGKUP

1. Kebijakan dan standar ini berlaku untuk pengelolaan pengamanan seluruh aset informasi di setiap Perangkat Daerah di lingkungan Pemerintah Daerah Kota Cirebon dan dilaksanakan oleh seluruh unit kerja, seluruh pegawai, baik sebagai pengguna maupun pengelola Teknologi Informasi dan Komunikasi, dan pihak ketiga di lingkungan Pemerintah Daerah Kota.
2. Aset informasi adalah aset dalam bentuk klasifikasi data dan informasi.
3. Data atau dokumen meliputi data keuangan, data kepegawaian, data barang milik negara, dokumen perjanjian kerahasiaan, kebijakan lembaga, prosedur operasional, rencana kelangsungan kegiatan *(business continuity plan)*, hasil audit, dan beberapa dokumen lainnya.
4. Perangkat lunak meliputi perangkat lunak aplikasi, perangkat lunak sistem, dan perangkat bantu pengembangan sistem.
5. Perangkat keras meliputi perangkat komputer, perangkat jaringan dan komunikasi, *removable media*, perangkat pendukung dan perangkat infrastruktur lainnya.
6. Aset tak berwujud *(intangible)* meliputi pengetahuan, pengalaman, keahlian, citra dan reputasi.

C. KEBIJAKAN

1. Perangkat Daerah bertanggung jawab untuk mengidentifikasikan persyaratan dan kebutuhan keamanan informasi dari pihak-pihak yang berkepentingan terhadap Keamanan Informasi di lingkungan kerjanya.
2. Perangkat Daerah bertanggung jawab mengatur pelaksanaan pengamanan dan perlindungan aset informasi di lingkungan kerjanya.
3. Perangkat Daerah bertanggung jawab melaksanakan pengamanan aset informasi di lingkungan kerjanya.
4. Setiap Perangkat Daerah bertanggung jawab meningkatkan pengetahuan, keterampilan dan kepedulian terhadap keamanan informasi pada seluruh pengguna di lingkungan kerjanya.
5. Setiap Perangkat Daerah menerapkan manajemen risiko keamanan informasi yang setidaknya mencakup kajian terhadap pemenuhan persyaratan dan kebutuhan keamanan informasi dari pihak-pihak yang berkepentingan terhadap Keamanan Informasi di lingkungan kerjanya.

6. Setiap Perangkat Daerah melakukan audit internal SMKI secara berkala untuk memastikan pengendalian, proses dan prosedur SMKI dilaksanakan secara efektif sesuai dengan Kebijakan dan Standar SMKI yang telah ditetapkan dan dipelihara dengan baik.
7. Kepala Perangkat Daerah secara berkala melakukan evaluasi terhadap kepatuhan dan keefektifan pelaksanaan SMKI serta melakukan tindak lanjut yang diperlukan untuk secara berkesinambungan meningkatkan kepatuhan dan keefektifan implementasi SMKI di lingkungan kerjanya.
8. Kepala Perangkat Daerah tidak bertanggung jawab atas kerugian atau kerusakan data maupun perangkat lunak milik pihak ketiga yang diakibatkan dari upaya untuk melindungi kerahasiaan, keutuhan, dan ketersediaan aset informasi.

D. STANDAR

1. Sasaran keamanan informasi *(information security objective)* setidaknya mencakup kriteria berikut ini:
   a. terukur;
   b. mencakup derajat pencapaian persyaratan dan kebutuhan keamanan informasi dari pihak-pihak yang berkepentingan terhadap Keamanan Informasi di setiap Perangkat Daerah;dan
   c. mencakup derajat kepatuhan dan keefektifan implementasi SMKI terhadap Kebijakan dan Standar SMKI di setiap Perangkat Daerah yang telah ditetapkan.
2. Standar manajemen risiko keamanan informasi mengikuti ketentuan mengenai Penerapan Manajemen Risiko di setiap Perangkat Daerah.
3. Standar Catatan Penerapan Kebijakan dan Standar SMKI di setiap Perangkat Daerah di Lingkungan Pemerintah Daerah Kota sebagai berikut:
   a. kepala Perangkat Daerah harus memastikan terdokumentasinya catatan penerapan Kebijakan dan Standar SMKI di lingkungan kerjanya, sehingga kepatuhan dan efektivitas penerapan SMKI dapat diukur;dan
   b. catatan penerapan Kebijakan dan Standar SMKI di setiap Perangkat Daerah setidaknya meliputi:
      1) Formulir-formulir sesuai prosedur operasional yang dijalankan;
      2) Catatan gangguan keamanan informasi;
      3) Catatan dari system;
      4) Catatan pengunjung di area terbatas;
      5) Kontrak dan perjanjian layanan;
      6) Perjanjian kerahasiaan *(confidentiality agreements)*;dan
      7) Laporan audit.
4. Dokumen pendukung kebijakan keamanan informasi setidaknya memuat informasi-informasi sebagai berikut:
   a. tujuan dan ruang lingkup dokumen pendukung kebijakan keamanan informasi;
   b. kerangka kerja setiap tujuan/sasaran pengendalian keamanan informasi;
   c. metodologi penilaian risiko *(risk assessment)*;
   d. penjelasan singkat mengenai standar, prosedur dan kepatuhan termasuk persyaratan peraturan yang harus dipenuhi, pengelolaan kelangsungan kegiatan, konsekuensi apabila terjadi pelanggaran;
   e. tanggung jawab dari setiap bagian terkait;dan
   f. dokumen referensi yang digunakan dalam menyusun dokumen pendukung kebijakan keamanan informasi.
5. Standar pengendalian dokumentasi SMKI adalah sebagai berikut:
   a. setiap Kepala Perangkat Daerah harus mengendalikan dokumen SMKI untuk menjaga kemutakhiran dokumen, efektivitas pelaksanaan operasional, menghindarkan dari segala jenis kerusakan, dan mencegah akses oleh pihak yang tidak berwenang;dan

b. setiap Kepala Perangkat Daerah harus menempatkan dokumen SMKI di semua area operasional sehingga mudah diakses oleh pengguna di unit kerja masing-masing sesuai peruntukannya.

6. Audit internal SMKI harus dilaksanakan setidaknya satu kali dalam 1 (satu) tahun.
7. Evaluasi kepatuhan dan implementasi SMKI setidaknya mencakup hal-hal sebagai berikut:
   a. evaluasi terhadap hasil audit internal SMKI;
   b. evaluasi terhadap pencapaian Sasaran Keamanan Informasi *(information security objective)*;
   c. evaluasi terhadap pencapaian persyaratan dan kebutuhan persyaratan dan kebutuhan keamanan informasi dari pihak-pihak yang berkepentingan terhadap Keamanan Informasi di lingkungan Pemerintah Daerah Kota Cirebon;
   d. evaluasi terhadap umpan balik dari pihak-pihak di luar Pemerintah Daerah Kota Cirebon;
   e. evaluasi dari penerapan manajemen risiko SMKI;dan
   f. evaluasi terhadap kemungkinan-kemungkinan untuk peningkatan kinerja SMKI.
8. Peningkatan berkelanjutan.
   a. peningkatan kinerja manajemen layanan teknologi informasi secara berkelanjutan dikoordinasikan melalui:
      1) Pengembangan proses manajemen keamanan informasi agar dapat menyesuaikan dengan *best practices* yang didefinisikan dalam ISO 27001;
      2) Pengkajian tingkat keamanan informasi secara berkala untuk melihat kesesuaiannya dengan kondisi terkini;
      3) Sarana peningkatan/perbaikan dari pengguna keamanan informasi yang didokumentasikan dalam *Security Improvement Program* (SIP);
      4) Pengkajian SIP secara berkala untuk memastikan tindak lanjut dari pelaksanaan peningkatan keamanan informasi yang telah direncanakan;
      5) Perumusan rencana peningkatan terhadap keamanan informasi berdasarkan hasil evaluasi manajemen yang telah dilakukan;dan
      6) Pencapaian dan pemeliharaan sertifikasi manajemen keamanan informasi berdasarkan standar ISO 27001.
   b. kriteria peningkatan kinerja manajemen layanan teknologi informasi antara lain berdasarkan:
      1. Pengembangan proses bisnis;
      2. Hasil ketidaksesuaian dari gangguan/insiden, proses perubahan dan lain;
      3. Hasil audit internal dan/atau eksternal;
      4. Hasil tinjauan manajemen;dan
      5. Hasil ketidaksesuaian dari inspeksi atau temuan dari *stakeholders* lain.

BAB II
PENGENDALIAN ORGANISASI KEAMANAN INFORMASI

A. TUJUAN

Bab ini bertujuan memberikan pedoman dalam membentuk organisasi fungsional keamanan informasi yang bertanggung jawab untuk mengelola keamanan informasi dan perangkat pengolah informasi di lingkungan kerja setiap Perangkat Daerah termasuk hubungan dengan pihak luar.

B. RUANG LINGKUP

Kebijakan dan standar organisasi keamanan informasi meliputi:

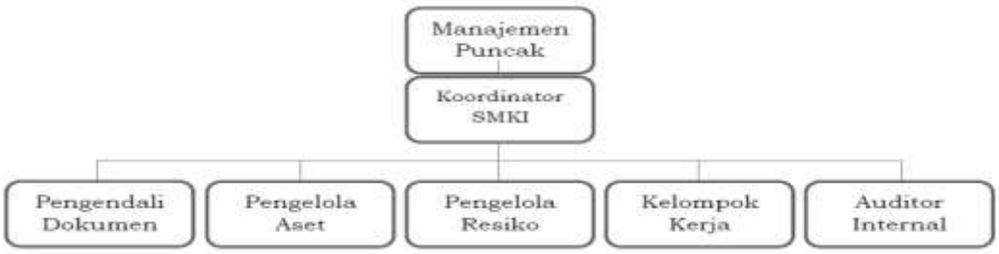
1. Struktur Tim Keamanan Informasi di setiap Perangkat Daerah.
2. Perjanjian kerahasiaan;
3. Pemisahan tugas;
4. Hubungan dengan pihak berwenang, komunitas keamanan informasi, dan pihak ketiga;
5. Keamanan informasi pada pengelolaan proyek;dan
6. Pengendalian terhadap *mobile device* dan *teleworking*.

C. KEBIJAKAN

1. Struktur Tim Keamanan lnformasi setiap Perangkat Daerah, berikut tanggung jawab dan wewenangnya diuraikan dalam standar organisasi keamanan informasi.
2. Tanggung jawab dan wewenang Tim Keamanan Informasi di setiap perangkat daerah dapat dipetakan dalam jabatan struktural dan/atau diperankan oleh Pejabat struktural dan/atau Pejabat fungsional.
3. Perjanjian Kerahasiaan.
   Setiap Kepala Perangkat Daerah mengidentifikasi dan mengkaji secara berkala persyaratan untuk menjaga kerahasiaan aset informasi yang dituangkan dalam dokumen perjanjian kerahasiaan.
4. Pemisahan tugas.
   Setiap Kepala Perangkat Daerah harus melakukan pemisahan tugas untuk proses yang melibatkan informasi yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA untuk menghindari adanya Pegawai yang memiliki pengendalian eksklusif terhadap seluruh aset informasi dan perangkat pengolahnya.
5. Hubungan dengan Pihak Berwenang.
   Setiap Kepala Perangkat Daerah mengidentifikasi dan menjalin kerjasama dengan pihak-pihak berwenang di luar Perangkat Daerah yang terkait dengan keamanan informasi.
6. Hubungan dengan Komunitas Keamanan Informasi.
   Setiap Kepala Perangkat Daerah menjalin kerjasama dengan komunitas keamanan informasi di luar Kepala Perangkat Daerah melalui pelatihan, seminar, atau forum lain yang relevan dengan keamanan informasi.
7. Keamanan informasi pada pengelolaan proyek.
   Pengendalian terhadap keamanan informasi harus diterapkan dalam pengelolaan proyek dan harus diaplikasikan pada seluruh fase dalam metodologi pengelolaan proyek.
8. Pengendalian terhadap *mobile device* dan *teleworking*.
   a. Setiap Kepala Perangkat Daerah membangun kepedulian pengguna perangkat *mobile device* dan *teleworking* akan risiko-risiko keamanan yang terus meningkat terhadap informasi yang tersimpan dalam perangkat *mobile device*;dan
   b. Pengguna perangkat *mobile device* dan *teleworking* harus mengikuti prosedur yang terkait penggunaan perangkat *mobile device* dan *teleworking* untuk menjaga keamanan perangkat dan informasi di dalamnya.

D. STANDAR

1. Tim Keamanan Informasi.
   a. Struktur Tim Keamanan Informasi Perangkat Daerah;



   b. Tanggung jawab Tim Keamanan Informasi setiap Perangkat Daerah.
      1) Manajemen Puncak.
         a) menetapkan Kebijakan;
         b) menetapkan kebijakan, sistem, dan prosedur keamanan informasi yang berlaku untuk setiap Perangkat Daerah;
         c) menetapkan pembagian tugas dan tanggung jawab untuk pengambilan keputusan terkait manajemen risiko keamanan informasi;dan
         d) memastikan tersedianya sumber daya dalam pelaksanaan SMKI.
      2) Koordinator SMKI.
         a) mendukung aspek program pengelolaan keamanan informasi dan mengkomunikasikan kepada seluruh pegawai;
         b) melakukan koordinasi antar Sub Bagian tentang pelaksanaan pengelolaan keamanan informasi;
         c) melakukan evaluasi terhadap hasil penetapan mitigasi risiko.
         d) memantau pelaksanaan perbaikan SMKI;
         e) memberikan laporan kepada Kepala Perangkat Daerah sehubungan dengan pelaksanaan implementasi pengelolaan keamanan informasi;
         f) memantau dan memastikan implementasi pengelolaan keamanan informasi sesuai dengan standar yang ditetapkan;
         g) bertindak selaku Koordinator SMKI dalam implementasi pengelolaan keamanan informasi;
         h) melaksanakan program information *security awareness* terkait SMKI;dan
         i) menetapkan jadwal audit internal/eksternal dan penunjukan Auditor Internal.
      3) Pengendali Dokumen.
         a) memelihara *'Master List'* dokumen SMKI berupa Kebijakan Keamanan Informasi, Standar Sistem Manajemen Keamanan Informasi, Standar Penilaian Risiko SMKI, Prosedur, Formulir yang digunakan serta Standar lain yang digunakan;
         b) memastikan seluruh dokumen ISO 27001 didistribusikan ke personil yang berwenang;
         c) melakukan administrasi terhadap seluruh dokumen, pengesahan, registrasi, penarikan, dan pemusnahan dokumen;dan
         d) melakukan inventarisasi untuk setiap kegiatan Audit Internal/Eksternal, Hasil Laporan Temuan Audit Internal/Eksternal, dan Risalah Rapat Tinjauan Manajemen.
      4) Pengelola Aset.
         a) mengelola data inventaris aset pemroses dan penyimpan informasi yang digunakan dalam pelaksanaan pekerjaan di setiap Perangkat Daerah;dan
         b) mendokumentasikan setiap penambahan, permohonan, perpindahan, peminjaman, pengembalian, perbaikan, dan penghapusan terkait aset pemroses informasi.

5) Kelompok Kerja.
   a) melakukan *monitoring* pelaksanaan SMKI di masing-masing Sub Bagian;
   b) memastikan bahwa semua prosedur, instruksi kerja dan formulir dapat digunakan dan diterapkan di Sub Bagian terkait untuk mengurangi terjadinya kesalahan dalam penerapan sistem manajemen;
   c) memantau pengukuran sasaran implementasi SMKI pada masing-masing Sub Bagian;dan
   d) melakukan tindak lanjut hasil temuan audit internal.
6) Pengelola Risiko.
   a) melaksanakan *Risk Assessment* terkait dengan SMKI;
   b) melakukan pemantauan terhadap risiko keamanan informasi yang baru di organisasi, baik dari pihak internal maupun eksternal;dan
   c) melakukan pengkinian terhadap daftar risiko (*risk register*).
7) Auditor Internal.
   a) melaksanakan audit internal dengan Sub Bagian terkait sesuai jadwal yang ditetapkan;
   b) mengkoordinasikan hasil temuan audit, pelaksanaan *closing meeting* dan tindak lanjut hasil audit internal;dan
   c) melaporkan pelaksanaan audit internal kepada Koordinator SMKI.

2. Perjanjian Kerahasiaan.
   Perjanjian kerahasiaan harus memuat unsur-unsur sebagai berikut:
   a. Definisi dari informasi yang akan dilindungi;
   b. Durasi yang diharapkan dari sebuah perjanjian kerahasiaan;
   c. Tanggung jawab yang diharapkan dari sebuah perjanjian kerahasiaan;
   d. Penanda-tangan untuk menghindari pengungkapan informasi secara tidak sah;
   e. Perlindungan kepemilikan informasi, rahasia organisasi, dan kekayaan intelektual;
   f. Izin menggunakan informasi rahasia, dan hak-hak penanda-tangan untuk menggunakan informasi;
   g. Hak untuk melakukan audit dan memantau kegiatan yang melibatkan informasi rahasia;
   h. Proses untuk pemberitahuan dan pelaporan dari penyingkapan yang dilakukan secara tidak sah atau pelanggaran terhadap kerahasiaan informasi;
   i. Tindakan yang diperlukan pada saat sebuah perjanjian kerahasiaan diakhiri;
   j. Syarat-syarat untuk informasi yang akan dikembalikan atau dimusnahkan pada saat penghentian perjanjian;dan
   k. Tindakan yang akan diambil apabila terjadi pelanggaran terhadap perjanjian ini.

BAB III
KEAMANAN SUMBER DAYA MANUSIA

A. TUJUAN

Keamanan sumber daya manusia bertujuan memastikan bahwa seluruh pegawai dan pihak ketiga di setiap Perangkat Daerah memahami tanggung jawabnya masing-masing, sadar atas ancaman keamanan informasi, serta mengetahui proses terkait keamanan informasi sebelum, selama, dan setelah bertugas.

B. RUANG LINGKUP

Kebijakan dan standar keamanan sumber daya manusia ini mencakup peran dan tanggung jawab seluruh pegawai dan pihak ketiga di setiap Perangkat Daerah yang harus dipahami dan dilaksanakan. Peran dan tanggung jawab pegawai juga mengacu pada peraturan perundang-undangan lainnya yang berlaku.

C. KEBIJAKAN

1. Seluruh pegawai bertanggung jawab untuk menjaga keamanan informasi di setiap Perangkat Daerah sesuai dengan tugas dan fungsinya.
2. Pihak ketiga harus menyetujui dan menandatangani syarat dan perjanjian untuk menjaga keamanan informasi di setiap Perangkat Daerah.
3. Peran dan tanggung jawab pegawai dan pihak ketiga terhadap keamanan informasi didefinisikan, didokumentasikan, dan dikomunikasikan kepada yang bersangkutan.
4. Kepala Perangkat Daerah akan melakukan pemeriksaan data pribadi yang diberikan oleh pegawai dan pihak ketiga sesuai dengan peraturan perundang-undangan yang berlaku.
5. Seluruh Aparatur Sipil Negara harus mendapatkan pendidikan, pelatihan, dan sosialisasi keamanan informasi secara berkala sesuai tingkat tanggung jawabnya.
6. Pihak ketiga, jika diperlukan, mendapatkan sosialisasi untuk meningkatkan kepedulian terhadap keamanan informasi. Seluruh pegawai dan pihak ketiga yang melanggar Kebijakan dan Standar SMKI di lingkungan Pemerintah Daerah Kota Cirebon akan dikenai sanksi atau tindakan disiplin sesuai ketentuan yang berlaku. Kepatuhan pegawai terhadap Kebijakan dan Standar SMKI di setiap Perangkat Daerah harus dievaluasi secara berkala oleh atasan masing-masing dan menjadi bagian dari penilaian kinerja pegawai. Kepala Perangkat Daerah harus menghentikan hak penggunaan aset informasi bagi pegawai yang sedang menjalani pemeriksaan yang terkait dengan dugaan adanya pelanggaran Kebijakan dan Standar SMKI di setiap Perangkat Daerah dan/atau yang sedang menjalani proses hukum.
7. Kepala Perangkat Daerah harus mencabut hak akses terhadap aset informasi yang dimiliki pegawai dan pihak ketiga apabila yang bersangkutan tidak lagi bekerja di Perangkat Daerah tersebut.
8. Kepala Perangkat Daerah harus mencabut hak akses terhadap aset informasi yang dimiliki pegawai dan pihak ketiga apabila yang bersangkutan tidak lagi bekerja di Perangkat Daerah tersebut.

D. STANDAR

Keamanan Sumber Daya Manusia meliputi:

1. Peran dan tanggung jawab pegawai di setiap Perangkat Daerah terhadap keamanan informasi harus menjadi bagian dari penjabaran tugas dan fungsi, khususnya bagi yang memiliki akses terhadap aset informasi.
2. Pimpinan dari pegawai berkeahlian khusus atau yang berada di posisi kunci *(key person)* harus memastikan ketersediaan pengganti pegawai tersebut dengan kompetensi yang setara apabila pegawai yang bersangkutan mutasi/berhenti.
3. Peran dan tanggung jawab pegawai terhadap keamanan informasi harus menyertakan persyaratan untuk:
   a. melaksanakan dan bertindak sesuai dengan organisasi keamanan informasi;
   b. melindungi aset dari akses yang tidak sah, penyingkapan, modifikasi, kerusakan atau gangguan;
   c. melaksanakan proses keamanan atau kegiatan keamanan informasi sesuai dengan peran dan tanggung jawabnya;dan

d. melaporkan kejadian, potensi kejadian, atau risiko keamanan informasi sesuai dengan Kebijakan dan Standar SMKI di setiap Perangkat Daerah.

4. Pemeriksaan latar belakang terhadap calon pegawai dan pihak ketiga, setiap Perangkat Daerah harus memperhitungkan privasi, perlindungan data pribadi dan/atau pekerjaan berdasarkan undang-undang, meliputi:
   a. ketersediaan referensi, dari referensi hubungan kerja, dan referensi pribadi;
   b. pemeriksaan kelengkapan dan ketepatan dari riwayat hidup pemohon;
   c. konfirmasi kualifikasi akademik dan profesional yang diklaim;
   d. pemeriksaan independen identitas (paspor atau dokumen yang sejenis);dan
   e. pemeriksaan lebih rinci, seperti pemeriksaan dari catatan kriminal.

BAB IV
PENGELOLAAN ASET

A. TUJUAN

Pengelolaan aset informasi bertujuan memberikan pedoman dalam mengelola aset informasi di setiap Perangkat Daerah untuk melindungi dan menjamin keamanan aset informasi.

B. RUANG LINGKUP

Kebijakan dan standar pengelolaan aset informasi ini meliputi:

1. Tanggung jawab terhadap aset informasi;
2. Pengklasifikasian aset informasi;
3. Penanganan aset informasi;
4. Penanganan media *removable*;
5. Pengamanan penggunaan kembali, penghapusan atau pemusnahan perangkat; dan
6. Pertukaran media informasi secara Fisik.

C. KEBIJAKAN

1. Tanggung Jawab terhadap Aset Informasi.
   a. kepala Perangkat Daerah mengidentifikasi aset informasi dan mendokumentasikannya dalam daftar inventaris aset informasi. Daftar inventaris aset informasi dipelihara dan dikelola perubahannya oleh Penanggung Jawab Pengendalian Dokumen;
   b. kepala Perangkat Daerah menetapkan pemilik aset informasi;
   c. kepala Perangkat Daerah menetapkan aset informasi yang terkait dengan perangkat pengolah informasi;
   d. pemilik Aset Informasi menetapkan aturan penggunaan aset informasi;
   e. seluruh pegawai yang berhenti bekerja atau mutasi harus mengembalikan seluruh aset informasi yang dipergunakan selama bekerja sesuai dengan ketentuan yang berlaku;dan
   f. pihak ketiga yang habis masa kontrak kerjanya harus mengembalikan seluruh aset informasi yang dipergunakan selama bekerja di Perangkat Daerah yang bersangkutan.
2. Klasifikasi Aset Informasi.
   a. aset informasi diklasifikasikan sesuai tingkat kerahasiaan, nilai, tingkat kritikalitas, serta aspek hukumnya;
   b. ketentuan rinci klasifikasi aset informasi diuraikan dalam standar pengelolaan aset informasi;dan
   c. pemberian label klasifikasi aset informasi harus dilakukan secara konsisten terhadap seluruh aset informasi.
3. Penanganan Aset Informasi.

   Kepala Perangkat Daerah perlu menyusun dan menetapkan peraturan atau prosedur terkait penanganan aset informasi sesuai dengan klasifikasi informasi yang telah ditetapkan.

4. Penanganan Media *Removable.*
   Kepala Perangkat Daerah perlu menyusun dan menetapkan peraturan atau prosedur terkait penanganan media *removable* sesuai dengan klasifikasi informasi yang telah ditetapkan.
5. Pengamanan penggunaan kembali atau penghapusan atau pemusnahan perangkat.
   a. perangkat pengolah informasi penyimpan data yang sudah tidak digunakan lagi harus disanitasi sebelum digunakan kembali atau dihapuskan atau dimusnahkan;dan
   b. penanganan perangkat pengolah informasi penyimpan data di setiap Perangkat Daerah sesuai dengan standar penanganan media penyimpan data yang yang berlaku di Perangkat Daerah yang bersangkutan.
6. Pertukaran Media Informasi secara Fisik.
   Kepala Perangkat Daerah perlu menyusun dan menetapkan peraturan terkait pertukaran informasi yang tidak menggunakan perangkat komunikasi elektronik misalnya melalui jasa pengantar media informasi melalui transportasi untuk melindungi informasi di dalam media terhadap akses yang tidak sah, penyalahgunaan, dan kerusakan ketika pengiriman.

D. STANDAR
   Pengelolaan Aset Informasi meliputi:
1. Pemilik Aset Informasi menetapkan dan mengkaji secara berkala klasifikasi aset informasi dan jenis perlindungan keamanannya;
2. Pemilik Aset Informasi menetapkan pihak yang berwenang untuk mengakses aset informasi;
3. Dalam pengelolaan aset informasi di setiap Perangkat Daerah, aset informasi diklasifikasikan seperti pada tabel berikut:

KLASIFIKASI ASET	KETERANGAN
Sangat Rahasia (*Strictly Confidential*)	Informasi yang apabila didistribusikan secara tidak sah atau jatuh ke tangan yang tidak berhak akan menyebabkan kerugian negara.
Rahasia (*Confidential*)	Informasi yang apabila secara tidak sah atau jatuh ke tangan yang tidak berhak akan mengganggu citra dan reputasi yang menurut peraturan perundang-undangan dinyatakan rahasia.
Terbatas (Internal)	Informasi yang apabila didistribusikan secara tidak sah atau jatuh ke tangan yag tidak berhak akan mengganggu citra dan reputasi.
Informasi Publik	Informasi yang dihasilkan, disimpan, dikelola, dikirim dan/atau diterima oleh suatu badan publik yang berkaitan dengan penyelenggara dan penyelenggaraan negara dan/atau penyelenggara dan penyelenggaraan badan publik lainya yang sesuai dengan Undang-Undang serta informasi lain yang berkaitan dengan kepentingan publik.

BAB V
PENGENDALIAN AKSES

A. TUJUAN

Pengendalian akses bertujuan untuk memastikan otorisasi akses pengguna dan mencegah akses pihak yang tidak berwenang terhadap aset informasi khususnya perangkat pengolah informasi.

B. RUANG LINGKUP

Kebijakan dan standar pengendalian akses ini meliputi:

1. Persyaratan untuk pengendalian akses;
2. Pengelolaan akses pengguna;
3. Tanggung jawab pengguna;
4. Pengendalian akses jaringan;
5. Pengendalian akses ke sistem operasi;dan
6. Pengendalian akses ke aplikasi dan sistem informasi.

C. KEBIJAKAN

1. Persyaratan untuk Pengendalian Akses.
   Setiap Perangkat Daerah harus menyusun, mendokumentasikan, dan mengkaji ketentuan akses ke aset informasi berdasarkan kebutuhan organisasi dan persyaratan keamanan.
2. Pengelolaan Akses Pengguna.
   a. pendaftaran pengguna;
      Setiap Perangkat Daerah harus menyusun prosedur pengelolaan hak akses pengguna sesuai dengan peruntukannya.
   b. pengelolaan hak akses khusus;
      Setiap Perangkat Daerah harus membatasi dan mengendalikan penggunaan hak akses khusus.
   c. pengelolaan kata sandi pengguna;
      1) Kepala Perangkat Daerah harus mengatur pengelolaan kata sandi pengguna;dan
      2) Pengelolaan kata sandi pengguna sesuai dengan standar yang berlaku di lingkungan Perangkat Daerah yang bersangkutan.
   d. kajian hak akses pengguna.
      Kepala Perangkat Daerah harus memantau dan mengevaluasi hak akses pengguna dan penggunaannya secara berkala untuk memastikan kesesuaian status pemakaiannya.
3. Tanggung Jawab Pengguna.
   a. pengguna harus mematuhi aturan pembuatan dan penggunaan kata sandi. Tanggung jawab pengguna terhadap kata sandi sesuai dengan standar tanggung jawab pengguna yang berlaku di setiap Perangkat Daerah;
   b. pengguna harus memastikan perangkat pengolah informasi yang digunakan mendapatkan perlindungan terutama pada saat ditinggalkan; dan
   c. pengguna harus melindungi informasi agar tidak diakses oleh pihak yang tidak berwenang.
4. Pengendalian Akses Jaringan.
   a. penggunaan layanan jaringan;
      1) Setiap Kepala Perangkat Daerah harus mengatur akses pengguna dalam mengakses jaringan yang digunakan pada Perangkat Daerah yang bersangkutan sesuai dengan peruntukannya; dan
      2) Setiap Kepala Perangkat Daerah harus mengatur akses pengguna dalam mengakses internet. Akses pengguna dalam mengakses internet sesuai dengan standar yang berlaku pada Perangkat Daerah yang bersangkutan.

b. otorisasi pengguna untuk koneksi eksternal;
Setiap Perangkat Daerah harus menerapkan proses otorisasi pengguna untuk setiap akses ke dalam jaringan internal melalui koneksi eksternal *(remote access)*.
c. perlindungan terhadap diagnosa jarak jauh dan konfigurasi *port*;
1) Akses ke perangkat keras dan perangkat lunak untuk diagnosa harus dikendalikan berdasarkan prosedur dan hanya digunakan oleh pegawai yang berwenang untuk melakukan pengujian, pemecahan masalah, dan pengembangan system;dan
2) *Port* pada fasilitas jaringan yang tidak dibutuhkan dalam kegiatan atau fungsi layanan harus dinonaktifkan.
d. pemisahan dalam jaringan;
Setiap Perangkat Daerah harus memisahkan jaringan untuk pengguna, sistem informasi, dan layanan informasi.
e. pengendalian koneksi jaringan;dan
Setiap Perangkat Daerah harus menerapkan mekanisme pengendalian akses pengguna sesuai dengan persyaratan pengendalian akses.
f. pengendalian *routing* jaringan.
Pengendalian *routing* jaringan internal di setiap Perangkat Daerah harus dilakukan sesuai pengendalian akses dan kebutuhan layanan informasi.

5. Pengendalian Akses ke Sistem Operasi
a. prosedur akses yang aman;
Akses ke sistem operasi harus dikontrol dengan menggunakan prosedur akses yang aman.
b. identifikasi dan otorisasi pengguna;
1) setiap pengguna harus memililki akun yang unik dan hanya digunakan sesuai dengan peruntukannya;dan
2) proses otorisasi pengguna harus menggunakan teknik autentikasi yang sesuai untuk memvalidasi identitas dari pengguna.
c. sistem pengelolaan kata sandi;
Sistem pengelolaan kata sandi harus mudah digunakan dan dapat memastikan kualitas kata sandi yang dibuat pengguna.
d. Penggunaan *system utilities*;
Setiap Perangkat Daerah harus membatasi dan mengendalikan penggunaan *system utilities*.
e. *session time-out*;dan
Fasilitas *session time-out* harus diaktifkan untuk menutup dan mengunci layar komputer, aplikasi, dan koneksi jaringan apabila tidak ada aktivitas pengguna setelah periode tertentu.
f. pembatasan waktu koneksi.
Setiap Perangkat Daerah harus membatasi waktu koneksi untuk sistem informasi dan aplikasi yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA.

6. Pengendalian Akses ke Aplikasi dan Sistem Informasi.
a. kepala Perangkat Daerah harus memastikan bahwa akses terhadap aplikasi dan sistem informasi hanya diberikan kepada pengguna sesuai peruntukannya;dan
b. aplikasi dan sistem informasi yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA harus diletakkan pada lokasi terpisah untuk mengurangi kemungkinan diakses oleh pihak yang tidak berwenang.

D. STANDAR
1. Persyaratan untuk Pengendalian Akses.
Persyaratan untuk pengendalian akses mencakup:
a. penentuan kebutuhan keamanan dari pengolah aset informasi;dan
b. pemisahan peran pengendalian akses, seperti administrasi akses dan otorisasi akses.

2. Pengelolaan Akses Pengguna.
   Prosedur pengelolaan akses pengguna harus mencakup:
   a. penggunaan akun yang unik untuk mengaktifkan pengguna agar terhubung dengan sistem informasi atau layanan, dan pengguna dapat bertanggung jawab dalam penggunaan sistem informasi atau layanan tersebut. Penggunaan akun khusus hanya diperbolehkan sebatas yang diperlukan untuk kegiatan atau alasan operasional, dan harus disetujui Pejabat yang berwenang serta didokumentasikan;
   b. pemeriksaan bahwa pengguna memiliki otorisasi dari pemilik sistem untuk menggunakan sistem informasi atau layanan, dan jika diperlukan harus mendapat persetujuan yang terpisah dari Pejabat yang berwenang;
   c. pemeriksaan bahwa tingkat akses yang diberikan sesuai dengan tujuan kegiatan dan konsisten dengan Kebijakan dan Standar SMKI di Lingkungan Perangkat Daerah yang bersangkutan;
   d. pemberian pernyataan tertulis kepada pengguna tentang hak aksesnya dan meminta pengguna menandatangani pernyataan ketentuan akses tersebut;
   e. pemastian penyedia layanan tidak memberikan akses kepada pengguna sebelum prosedur otorisasi telah selesai;
   f. pemeliharaan catatan pengguna layanan yang terdaftar dalam menggunakan layanan;
   g. penghapusan atau penonaktifan akses pengguna yang telah berubah tugas dan/atau fungsinya, setelah penugasan berakhir atau mutasi;
   h. pemeriksaan, penghapusan, serta penonaktifan akun dilakukan secara berkala;dan
   i. pemastian bahwa akun tidak digunakan oleh pengguna lain.
3. Pengelolaan Hak Akses Khusus *(privilege management)*
   Pengelolaan hak akses khusus harus mempertimbangkan:
   a. hak akses khusus setiap sistem dari pabrikan perlu diidentifikasi untuk dialokasikan atau diberikan kepada pengguna yang terkait dengan produk, seperti sistem operasi, sistem pengelolaan basis data, dan aplikasi;
   b. hak akses khusus hanya diberikan kepada pengguna sesuai dengan peruntukkannya berdasarkan kebutuhan dan kegiatan tertentu;
   c. pengelolaan proses otorisasi dan catatan dari seluruh hak akses khusus yang dialokasikan atau diberikan kepada pengguna. Hak akses khusus tidak boleh diberikan sebelum proses otorisasi selesai;
   d. pengembangan dan penggunaan sistem rutin (misal *job scheduling*) harus diutamakan untuk menghindari kebutuhan dalam memberikan hak akses khusus secara terus menerus kepada pengguna;dan
   e. hak akses khusus harus diberikan secara terpisah dari akun yang digunakan untuk kegiatan umum, seperti akun *system administrator, database administrator,* dan *network administrator.*
4. Kajian Hak Akses Pengguna.
   Kajian hak akses pengguna harus mempertimbangkan:
   a. hak akses pengguna harus dikaji paling sedikit 6 (enam) bulan sekali atau setelah terjadi perubahan pada sistem, atau struktur organisasi;
   b. hak akses khusus harus dikaji paling sedikit 6 (enam) bulan sekali dalam jangka waktu lebih sering dibanding jangka waktu pengkajian hak akses pengguna, atau apabila terjadi perubahan pada sistem, atau struktur organisasi; dan
   c. pemeriksaan hak akses khusus harus dilakukan secara berkala, untuk memastikan pemberian hak akses khusus telah diotorisasi.
5. Pengendalian Akses Jaringan.
   a. menerapkan prosedur otorisasi untuk pemberian akses ke jaringan dan layanan jaringan;

b. menerapkan teknik autentikasi akses dari koneksi eksternal, seperti teknik kriptografi, token *hardware*, dan *dial-back*;dan
c. melakukan penghentian atau isolasi layanan jaringan pada area jaringan yang mengalami gangguan keamanan informasi.

6. Pemisahan dalam Jaringan.
   Melakukan pemisahan dalam jaringan antara lain:
   a. pemisahan berdasarkan kelompok layanan informasi, pengguna, dan aplikasi;dan
   b. pemberian akses jaringan kepada tamu, hanya dapat diberikan akses terbatas misalnya internet dan/atau surat elektronik tanpa bisa terhubung ke jaringan internal Perangkat Daerah yang bersangkutan.

BAB VI
KRIPTOGRAFI

A. TUJUAN
   Tujuan dari penerapan kriptografi adalah untuk menambah jaminan dalam perlindungan kerahasiaan, keotentikan dan integritas informasi yang disimpan dan ditransmisikan melalui perangkat teknologi informasi dan komunikasi.

B. RUANG LINGKUP
   Kebijakan dan standar penerapan kriptografi ini meliputi:
   1. Penentuan kondisi yang mengharuskan penerapan kriptografi;dan
   2. Persyaratan penerapan kriptografi dan kunci kriptografi.

C. KEBIJAKAN
   1. Setiap Perangkat Daerah mengembangkan dan/atau menerapkan sistem kriptografi untuk perlindungan informasi dan membuat rekomendasi yang tepat bagi penerapannya.
   2. Sistem kriptografi harus digunakan untuk melindungi aset informasi yang memiliki klasifikasi SANGAT RAHASIA, RAHASIA, dan TERBATAS.

D. STANDAR
   Pengembangan dan/atau penerapan sistem kriptografi untuk perlindungan informasi harus mempertimbangkan:
   1. Kondisi dari suatu kegiatan yang menentukan bahwa informasi harus dilindungi, seperti risiko kegiatan, media pengiriman informasi, dan tingkat perlindungan yang dibutuhkan;
   2. Tingkat perlindungan yang dibutuhkan harus diidentifikasi berdasarkan penilaian risiko, dengan mempertimbangkan jenis, kekuatan, dan kualitas dari algoritma enkripsi yang akan digunakan;
   3. Keperluan enkripsi untuk perlindungan informasi SANGAT RAHASIA, RAHASIA dan TERBATAS yang melalui perangkat *mobile computing*, *removable* media, atau jalur komunikasi;
   4. Kemudahan dan teknologi yang diperlukan dalam pengelolaan kunci kriptografi, seperti perlindungan kunci kriptografi, pemulihan informasi terenkripsi dalam hal kehilangan atau kerusakan kunci kriptografi;dan
   5. Dampak penggunaan informasi terenkripsi, seperti pengendalian terkait pemeriksaan suatu konten, kecepatan pemrosesan pada sistem.

BAB VII
KEAMANAN FISIK DAN LINGKUNGAN

A. TUJUAN

Keamanan fisik dan lingkungan bertujuan untuk mencegah akses fisik oleh pihak yang tidak berwenang, dan menghindari terjadinya kerusakan pada perangkat pengolah informasi serta gangguan pada aktivitas organisasi.

B. RUANG LINGKUP

Kebijakan dan standar keamanan fisik dan lingkungan ini meliputi:

1. Pengamanan area;dan
2. Pengamanan perangkat.

C. KEBIJAKAN

1. Pengamanan Area.
   a. seluruh pegawai, pihak ketiga, dan tamu yang memasuki lingkungan Perangkat Daerah harus mematuhi aturan yang berlaku; dan
   b. ketentuan rinci tentang pengamanan area lingkungan kerja di setiap Perangkat Daerah diuraikan dalam Kebijakan Keamanan Informasi pada Perangkat Daerah yang bersangkutan.
2. Pengamanan Perangkat.
   a. penempatan dan perlindungan perangkat;
      Perangkat pengolah informasi dan perangkat pendukung harus ditempatkan di lokasi yang aman dan diposisikan sedemikian rupa untuk mengurangi risiko aset informasi dapat diakses oleh pihak yang tidak berwenang.
   b. penyediaan perangkat pendukung;
      Perangkat pendukung harus dipasang untuk menjamin beroperasinya perangkat pengolah informasi dan secara berkala harus diperiksa dan diuji ulang kinerjanya.
   c. pengamanan kabel;
      1) kabel sumber daya listrik harus dilindungi dari kerusakan;dan
      2) kabel telekomunikasi yang mengalirkan informasi harus dilindungi dari kerusakan dan penyadapan.
   d. pemeliharaan perangkat;
      Perangkat harus dipelihara secara berkala untuk menjamin ketersediaan, keutuhannya, dan fungsinya.
   e. pengamanan perangkat di luar lingkungan Perangkat Daerah;
      Penggunaan perangkat yang dibawa ke luar dari lingkungan setiap Perangkat Daerah harus disetujui oleh Pejabat yang berwenang.
   f. pengamanan penggunaan kembali atau penghapusan atau pemusnahan perangkat;
      1) Perangkat pengolah informasi penyimpan data yang sudah tidak digunakan lagi harus disanitasi sebelum digunakan kembali atau dihapuskan atau dimusnahkan; dan
      2) Penanganan perangkat pengolah informasi penyimpan data di setiap Perangkat Daerah sesuai dengan standar penanganan media penyimpan data yang berlaku.
   g. pengamanan perangkat yang tidak dalam pengawasan;
      Pengguna harus memastikan perangkat Teknologi Informasi yang tidak berada dalam pengawasan memiliki perlidungan yang tepat terhadap akses oleh pihak yang tidak berwenang.
   h. kebersihan meja kerja dan layar.
      Peraturan terkait kebersihan meja kerja serta layar dari informasi penting perlu disusun dan diterapkan.

D. STANDAR

1. Perangkat harus dipelihara sesuai dengan petunjuk manualnya. Untuk pemeliharaan yang dilakukan oleh pihak ketiga, harus diadakan Perjanjian Tingkat Layanan *(Service Level Agreement/SLA)* yang mendefinisikan tingkat pemeliharaan yang disediakan dan tingkat kinerja yang harus dipenuhi pihak ketiga.
2. Pemeliharaan terhadap perangkat keras atau perangkat lunak dilakukan hanya oleh pegawai yang berwenang.
3. Dalam hal pemeliharaan perangkat tidak dapat dilakukan di tempat, maka pemindahan perangkat harus mendapatkan persetujuan Pejabat yang berwenang. Terhadap data yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA yang disimpan dalam perangkat tersebut harus dipindahkan terlebih dahulu.
4. Otorisasi penggunaan perangkat harus dilakukan secara tertulis dan data-data yang terkait dengan aset informasi yang digunakan, seperti nama pemakai aset, lokasi, dan tujuan penggunaan aset, harus dicatat dan disimpan.
5. Pengamanan Area.
   a. setiap Perangkat Daerah menyimpan perangkat pengolah informasi di ruangan khusus yang dilindungi dengan pengamanan fisik yang memadai antara lain pintu elektronik, sistem pemadam kebakaran, alarm bahaya dan perangkat pemutus aliran listrik;
   b. akses ke ruang *server*, pusat data, dan area kerja yang berisikan aset informasi yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA harus dibatasi dan hanya diberikan kepada pegawai yang berwenang;
   c. pihak ketiga yang memasuki ruang *server*, pusat data, dan area kerja yang berisikan aset informasi yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA harus didampingi pegawai dan sudah diketahui oleh Kepala Perangkat Daerah sepanjang waktu kunjungan. Waktu masuk dan keluar serta maksud kedatangan harus dicatat dalam buku catatan kunjungan;
   d. Kantor, ruangan, dan perangkat yang berisikan aset informasi yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA harus dilindungi secara memadai;
   e. pegawai dan pihak ketiga tidak diizinkan merokok, makan, minum di ruang *server* dan pusat data;dan
   f. area keluar masuk barang dan area publik harus selalu dijaga, diawasi dan dikendalikan, dan jika memungkinkan disterilkan dari perangkat pengolah informasi untuk menghindari akses oleh pihak yang tidak berwenang.
6. Pengamanan Kantor, Ruangan dan Fasilitas.
   Pengamanan kantor, ruangan dan fasilitas mencakup:
   a. pengamanan kantor, ruangan, dan fasilitas harus sesuai dengan peraturan dan standar keamanan dan keselamatan kerja yang berlaku;
   b. fasilitas utama harus ditempatkan khusus untuk menghindari akses publik;dan
   c. pembatasan pemberian identitas atau tanda-tanda keberadaan aktivitas pengolahan informasi.
7. Perlindungan terhadap Ancaman Eksternal dan Lingkungan.
   Perlindungan terhadap ancaman eksternal dan lingkungan harus mempertimbangkan:
   a. bahan-bahan berbahaya atau mudah terbakar harus disimpan pada jarak yang aman dari area terbatas;
   b. perlengkapan umum seperti alat tulis tidak boleh disimpan di dalam area terbatas;
   c. perangkat *fallback* dan media *backup* harus diletakkan pada jarak yang aman untuk menghindari kerusakan dari bencana yang mempengaruhi fasilitas utama;dan

d. perangkat pemadam kebakaran harus disediakan dan diletakkan di tempat yang tepat.

8. Penempatan dan Perlindungan Perangkat.
   Penempatan dan perlindungan perangkat harus mencakup:
   a. perangkat harus diletakkan pada lokasi yang meminimalkan akses yang tidak perlu ke dalam area kerja;
   b. perangkat pengolah informasi yang menangani informasi sensitif harus diposisikan dan dibatasi arah sudut pandangnya untuk mengurangi risiko informasi dilihat oleh pihak yang tidak berwenang selama digunakan, dan perangkat penyimpanan diamankan untuk menghindari akses oleh pihak yang tidak berwenang;
   c. perangkat yang memerlukan perlindungan khusus seperti perangkat cetak khusus, perangkat jaringan di luar ruang *server* harus terisolasi untuk mengurangi tingkat perlindungan atau perlakuan standar yang perlu dilakukan;
   d. langkah-langkah pengendalian dilakukan untuk meminimalkan risiko potensi ancaman fisik, seperti pencurian, api, bahan peledak, asap, air termasuk kegagalan penyediaan air, debu, getaran, efek kimia, gangguan pasokan listrik, gangguan komunikasi, radiasi elektromagnetis, dan perusakan;
   e. kondisi lingkungan, seperti suhu dan kelembaban harus dimonitor untuk mencegah perubahan kondisi yang dapat mempengaruhi pengoperasian perangkat pengolah informasi;
   f. perlindungan petir harus diterapkan untuk semua bangunan dan filter perlindungan petir harus dipasang untuk semua jalur komunikasi dan listrik;dan
   g. perangkat pengolah informasi sensitif harus dilindungi untuk meminimalkan risiko kebocoran informasi.

9. Pengamanan Kabel.
   Perlindungan keamanan kabel mencakup :
   a. pemasangan kabel sumber daya Listrik dan kabel telekomunikasi ke perangkat pengolah informasi selama memungkinkan harus terletak di bawah tanah, atau menerapkan alternatif perlindungan lain yang memadai;
   b. pemasangan kabel jaringan harus dilindungi dari penyusupan yang tidak sah atau kerusakan, misalnya dengan menggunakan *conduit* (saluran) atau menghindari rute melalui area publik;
   c. pemisahan antara kabel sumber daya listrik dengan kabel telekomunikasi untuk mencegah interferensi;
   d. penandaan atau penamaan kabel dan perangkat harus diterapkan secara jelas untuk memudahkan penanganan kesalahan;
   e. penggunaan dokumentasi daftar panel *patch* diperlukan untuk mengurangi kesalahan;dan
   f. pengendalian untuk sistem informasi yang sensitif harus mempertimbangkan:
      1) Menggunaan *conduit*;
      2) Penggunaan ruangan terkunci pada tempat inspeksi dan titik pemutusan kabel;
      3) Penggunaan rute alternatif dan/atau media transmisi yang menyediakan keamanan yang sesuai;
      4) Penggunaan kabel *fiber optic*;
      5) Penggunaan lapisan elektromagnet untuk melindungi kabel;
      6) Inisiasi penghapusan teknikal *(technical sweeps)* dan pemeriksaan secara fisik untuk peralatan yang tidak diotorisasi saat akan disambungkan ke kabel;dan
      7) Penerapan akses kontrol ke panel *patch* dan ruangan kabel.

BAB VIII
KEAMANAN OPERASIONAL

A. TUJUAN

Pengelolaan keamanan operasional bertujuan untuk memastikan keamanan dalam pengoperasian fasilitas pemrosesan informasi yang berada di setiap lingkungan Perangkat Daerah.

B. RUANG LINGKUP

Kebijakan dan standar pengelolaan operasional ini meliputi:

1. Prosedur operasional dan tanggung jawab;
2. Perencanaan dan penerimaan system;
3. Perlindungan terhadap *Malicious Code*;
4. Information *Backup*;
5. Penanganan media penyimpan data;
6. *Logging* dan *Monitoring*;
7. *Pengendalian* operasional perangkat lunak;
8. *Pengelolaan* Kerentanan Teknis;dan
9. Audit *Operasional*.

C. KEBIJAKAN

1. Prosedur Operasional dan Tanggung Jawab.
   a. dokumentasi prosedur operasional;
      Setiap Perangkat Daerah harus mendokumentasikan, memelihara, dan menyediakan seluruh prosedur operasional yang terkait dengan penggunaan perangkat pengolah informasi bagi pengguna sesuai dengan peruntukannya.
   b. pengelolaan perubahan perangkat Teknologi Informasi;
      Setiap Perangkat Daerah harus mengendalikan perubahan terhadap perangkat pengolah informasi. Pengelolaan perubahan layanan Teknologi Informasi di setiap Perangkat Daerah akan ditetapkan dalam ketentuan tersendiri.
   c. pemisahan tugas;
      Kepala Perangkat Daerah harus melakukan pemisahan tugas untuk proses yang melibatkan informasi yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA untuk menghindari adanya pegawai yang memiliki pengendalian eksklusif terhadap seluruh aset informasi dan perangkat pengolahnya.
   d. pengelolaan kapasitas;
      Kepala Perangkat Daerah harus memantau dan mengelola penggunaan sumber daya Teknologi Informasi serta menyusun proyeksi penggunaan sumber daya Teknologi Informasi di masa-masa mendatang, untuk menjamin ketersediaan layanan Teknologi Informasi dalam hal pemrosesan dan penyimpanan informasi.
   e. pemisahan perangkat pengembangan, pengujian dan operasional.
      Kepala Perangkat Daerah harus melakukan pemisahan perangkat pengembangan, pengujian, dan operasional untuk mengurangi risiko perubahan atau akses oleh pihak yang tidak berwenang terhadap sistem operasional.
2. Perencanaan dan Penerimaan Sistem.
   Kegiatan perencanaan dan penerimaan sistem meliputi:
   a. pengelolaan kapasitas dalam rangka perencanaan sistem;
      1) Kepala Perangkat Daerah harus memantau penggunaan perangkat pengolah informasi dan membuat perkiraan pertumbuhan kebutuhan ke depan untuk memastikan ketersediaan kapasitas;dan
      2) Pengelolaan kapasitas di setiap Perangkat Daerah akan ditetapkan dalam ketentuan tersendiri.

b. Penerimaan Sistem.
   1) Kepala Perangkat Daerah harus menetapkan kriteria penerimaan *(acceptance criteria)* untuk sistem informasi baru, pemutakhiran *(upgrade)* dan versi baru serta melakukan pengujian sebelum penerimaan;dan
   2) Penerimaan sistem di setiap Perangkat Daerah akan ditetapkan dalam ketentuan tersendiri.

3. Perlindungan Terhadap *Malicious Code.*
   a. setiap Perangkat Daerah harus menerapkan sistem yang dapat melakukan pendeteksian, pencegahan, dan pemulihan sebagai bentuk perlindungan terhadap ancaman program yang membahayakan *(Malicious Code)*;dan
   b. Perlindungan terhadap ancaman program yang membahayakan *(Malicious Code)* di setiap Perangkat Daerah akan ditetapkan dalam ketentuan tersendiri.
4. *Information Backup*.
   a. setiap Perangkat Daerah harus melakukan *backup* informasi dan perangkat lunak yang berada di *data center* secara berkala;dan
   b. proses *backup* data di setiap Perangkat Daerah harus dilakukan sesuai dengan standar *backup data* yang berlaku.
5. Penanganan Media Penyimpan Data.
   a. setiap Perangkat Daerah harus mempunyai prosedur yang mengatur penanganan media penyimpan data untuk melindungi aset informasi; dan
   b. penanganan media penyimpanan data di setiap Perangkat Daerah sesuai dengan standar penanganan media penyimpan data yang berlaku.
6. *Logging* dan *Monitoring.*
   a. event *logging*;
      Setiap Perangkat Daerah harus mengaktifkan dan secara rutin me*review event logging* yang mencatat aktivitas pengguna, pengecualian, dan kejadian keamanan informasi.
   b. memantau penggunaan sistem;
      Setiap Perangkat Daerah harus memantau penggunaan sistem dan mengkaji secara berkala hasil kegiatan *monitoring.*
   c. perlindungan terhadap informasi *log*;
      Setiap Perangkat Daerah harus memastikan perlindungan terhadap fasilitas *logging* dan informasi *log* agar terhindar dari kerusakan dan akses oleh pihak yang tidak berwenang.
   d. pencatatan *log system administrator* dan *system operator*;
      Setiap Perangkat Daerah harus memastikan agar kegiatan pencatatan *log system administrator* dan *system operator* tercatatkan di dalam *log*.
   e. pencatatan kesalahan *(fault logging)*;dan
      Setiap Perangkat Daerah harus menerapkan pencatatan kesalahan (*fault logging*) untuk dianalisis dan diambil tindakan penanganan yang tepat.
   f. sinkronisasi waktu.
      Setiap Perangkat Daerah harus memastikan semua perangkat pengolah informasi yang tersambung dengan jaringan telah disinkronisasi dengan sumber waktu yang akurat dan disepakati.
7. Pengendalian operasional perangkat lunak.
   Setiap Perangkat Daerah harus mempunyai prosedur untuk pengendalian perangkat lunak pada sistem operasional.
8. Pengelolaan Kerentanan Teknis.
   a. setiap Perangkat Daerah harus mengumpulkan informasi kerentanan teknis secara berkala dari seluruh sistem informasi yang digunakan maupun komponen pendukung sistem informasi;dan

b. setiap Perangkat Daerah harus melakukan evaluasi dan penilaian risiko terhadap kerentanan teknis yang ditemukan dalam sistem informasi serta menetapkan pengendalian yang tepat terhadap risiko terkait.

9. Audit *Operasional.*
   Audit yang mencakup verifikasi terhadap perangkat pemrosesan informasi harus direncanakan dan disepakati dengan pihak terkait sehingga gangguan terhadap proses bisnis dapat diminimalisasi.

D. STANDAR

1. Dokumentasi Prosedur Operasional.
   Prosedur operasional harus meliputi:
   a. tata cara pengolahan dan penanganan informasi;
   b. tata cara menangani kesalahan-kesalahan atau kondisi khusus yang terjadi, beserta pihak yang harus dihubungi bila mengalami kesulitan teknis;
   c. cara memfungsikan kembali perangkat dan cara mengembalikan perangkat ke keadaan awal *(recovery)* saat terjadi kegagalan *system*;
   d. tata cara *backup* dan *restore*;dan
   e. tata cara pengelolaan jejak audit *(audit trails)* pengguna dan catatan kejadian atau kegiatan sistem.
2. Pemisahan Perangkat Pengembangan, Pengujian dan Operasional.
   Pemisahan perangkat pengembangan dan operasional harus mempertimbangkan:
   a. pengembangan dan operasional perangkat lunak harus dioperasikan di sistem atau prosesor komputer dan domain atau direktori yang berbeda;
   b. instruksi Kerja *(working instruction)* rilis dari pengembangan perangkat lunak ke operasional harus ditetapkan dan didokumentasikan;
   c. *compiler*, *editor*, dan alat bantu pengembangan lain tidak boleh diakses dari sistem operasional ketika tidak dibutuhkan;
   d. lingkungan sistem pengujian harus diusahakan sama dengan lingkungan sistem operasional;
   e. pengguna harus menggunakan profil pengguna yang berbeda untuk sistem pengujian dan sistem operasional, serta aplikasi harus menampilkan pesan identifikasi dari sistem untuk mengurangi risiko kesalahan;dan
   f. data yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA tidak boleh disalin ke dalam lingkungan pengujian sistem.
3. *Logging* dan *monitoring*.
   Prosedur *logging* dan *monitoring* penggunaan sistem pengolah informasi ditetapkan untuk menjamin agar kegiatan akses yang tidak sah tidak perlu terjadi. Prosedur ini meliputi *monitoring*:
   a. kegagalan akses *(access failures)*;
   b. pola-pola *log-on* yang mengindikasikan penggunaan yang tidak wajar;
   c. alokasi dan penggunaan hak akses *khusus (privileged access capability)*;
   d. penelusuran transaksi dan pengiriman *file* tertentu yang mencurigakan;dan
   e. penggunaan sumber daya sensitif.
4. Pengendalian operasional perangkat lunak.
   Prosedur pengendalian operasional perangkat lunak mencakup beberapa hal berikut:
   a. pengendalian akses terhadap perangkat lunak sebelum dilakukan *deployment*;dan
   b. petunjuk *deployment*, penggunaan lisensi, pengoperasian dan pemeliharaan perangkat lunak.

5. Pengelolaan Kerentanan Teknis
   Pengelolaan kerentanan teknis meliputi:
   a. penunjukan fungsi dan tanggung jawab yang terkait dengan pengelolaan kerentanan teknis termasuk di dalamnya *monitoring* kerentanan, penilaian risiko kerentanan, *patching*, registrasi aset, dan koordinasi dengan pihak terkait;
   b. pengidentifikasian sumber informasi yang dapat digunakan untuk mengidentifikasi dan meningkatkan kepedulian terhadap kerentanan teknis;
   c. penentuan rentang waktu untuk melakukan aksi terhadap munculnya potensi kerentanan teknis. Apabila terjadi kerentanan teknis yang butuh penanganan maka harus diambil tindakan sesuai kontrol yang telah ditetapkan atau melaporkan kejadian tersebut melalui pelaporan kejadian dan kelemahan keamanan informasi;
   d. pengujian dan evaluasi penggunaan *patch* sebelum proses instalasi untuk memastikan *patch* dapat bekerja secara efektif dan tidak menimbulkan risiko yang lain. Apabila *patch* tidak tersedia, harus melakukan hal sebagai berikut:
      1) Mematikan *patch* yang berhubungan dengan kerentanan;
      2) Menambahkan pengendalian akses seperti *firewall*;
      3) Meningkatkan pengawasan untuk mengidentifikasi atau mencegah terjadinya serangan atau kejadian;dan
      4) Meningkatkan kepedulian terhadap kerentanan teknis.
   e. penyimpanan audit *log* yang memuat prosedur dan langkah-langkah yang telah diambil;
   f. *monitoring* dan evaluasi terhadap pengelolaan kerentanan teknis harus dilakukan secara berkala;dan
   g. pengelolaan kerentanan teknis diutamakan terhadap sistem informasi yang memiliki tingkat risiko tinggi.
6. Audit Operasional.
   Prosedur audit yang mencakup kegiatan verifikasi operasional harus disusun yang mencakup hal-hal sebagai berikut:
   a. proses perencanaan audit;
   b. proses untuk melakukan audit;
   c. proses pelaporan dan *monitoring* tindak lanjut audit;dan
   d. persyaratan auditor.

BAB IX
KEAMANAN KOMUNIKASI

A. TUJUAN

Tujuan dari pengendalian keamanan komunikasi adalah untuk memberikan perlindungan terhadap informasi yang ditransmisikan melalui jaringan komunikasi beserta perangkat pendukungnya yang berada di lingkungan Perangkat Daerah.

B. RUANG LINGKUP

Kebijakan pengendalian keamanan komunikasi ini meliputi:
1. Pengelolaan keamanan jaringan;dan
2. Keamanan dalam transfer Informasi.

C. KEBIJAKAN

1. Pengelolaan Keamanan Jaringan.
   a. pengendalian jaringan;
      1) Setiap Perangkat Daerah harus mengelola dan melindungi jaringan dari berbagai bentuk ancaman;dan

2) Ketentuan rinci pengendalian jaringan di setiap Perangkat Daerah diuraikan dalam standar pengelolaan komunikasi dan operasional.

b. keamanan layanan jaringan.
Setiap Perangkat Daerah harus mengidentifikasi fitur keamanan layanan, tingkat layanan, dan kebutuhan pengelolaan serta mencantumkannya dalam kesepakatan penyediaan layanan jaringan termasuk layanan jaringan yang disediakan oleh pihak ketiga.

2. Keamanan dalam Transfer Informasi
a. pertukaran informasi dan perangkat lunak antara Perangkat Daerah dengan pihak ketiga hanya akan dilakukan atas kesepakatan tertulis kedua belah pihak;
b. setiap Perangkat Daerah harus melakukan penilaian risiko yang memadai sebelum melaksanakan pertukaran informasi;
c. setiap Perangkat Daerah harus menerapkan pengendalian keamanan informasi untuk pengiriman informasi melalui surat elektronik atau pengiriman informasi melalui jasa layanan pengiriman dalam rangka menghindari akses pihak yang tidak berwenang;dan
d. ketentuan rinci pertukaran informasi di setiap Perangkat Daerah diuraikan dalam standar pengelolaan komunikasi dan operasional.

D. STANDAR
1. Pengelolaan Keamanan Jaringan.
Pengelolaan keamanan jaringan meliputi:
a. *monitoring* kegiatan pengelolaan jaringan untuk menjamin bahwa perangkat jaringan digunakan secara efektif dan efisien;
b. pengendalian dan pengaturan tentang penyambungan atau perluasan jaringan internal atau eksternal Perangkat Daerah;
c. pengendalian dan pengaturan akses ke sistem jaringan internal atau eksternal Perangkat Daerah;
d. pencatatan informasi pihak ketiga yang diizinkan mengakses ke jaringan Perangkat Daerah dan menerapkan *monitoring* serta pencatatan kegiatan selama menggunakan jaringan;
e. pemutusan layanan tanpa pemberitahuan sebelumnya jika terjadi gangguan keamanan informasi;
f. perlindungan jaringan dari akses yang tidak berwenang meliputi:
1) Penetapan untuk penanggung jawab pengelolaan jaringan dipisahkan dari pengelolaan perangkat pengolah informasi;
2) Penerapan pengendalian khusus untuk melindungi keutuhan informasi yang melewati jaringan umum antara lain dengan penggunaan enkripsi dan tanda tangan elektronik *(digital signature)*;dan
3) Pendokumentasian arsitektur jaringan seluruh komponen perangkat keras jaringan dan perangkat lunak.
g. penerapan fitur keamanan layanan jaringan meliputi:
1) Teknologi keamanan seperti autentikasi, enkripsi, dan pengendalian sambungan jaringan;
2) Parameter teknis yang diperlukan untuk koneksi aman dengan layanan jaringan sesuai dengan keamanan dan aturan koneksi jaringan;dan
3) Prosedur untuk penggunaan layanan jaringan yang membatasi akses ke layanan jaringan atau aplikasi.

2. Keamanan dalam Transfer lnformasi.
a. prosedur pertukaran informasi bila menggunakan perangkat komunikasi elektronik, meliputi:
1) Perlindungan pertukaran informasi dari pencegatan, penyalinan, modifikasi, *miss-routing*, dan perusakan;
2) Pendeteksian dan perlindungan terhadap kode berbahaya yang dapat dikirim melalui penggunaan komunikasi elektronik;

3) Perlindungan informasi elektronik dalam bentuk attachment yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA;dan
4) Pertimbangan risiko terkait penggunaan perangkat komunikasi nirkabel.

b. pertukaran informasi yang tidak menggunakan perangkat komunikasi elektronik, mengacu pada ketentuan yang berlaku;
c. pengendalian pertukaran informasi bila menggunakan perangkat komunikasi elektronik, meliputi:
   1) Pencegahan terhadap penyalahgunaan wewenang pegawai dan pihak ketiga yang dapat membahayakan organisasi;
   2) Penggunaan teknik kriptografi;
   3) Penyelenggaraan penyimpanan dan penghapusan atau pemusnahan untuk semua korespondensi kegiatan, termasuk pesan, yang sesuai dengan ketentuan yang berlaku;
   4) Larangan meninggalkan informasi sensitif pada perangkat pengolah informasi;
   5) Pembatasan penerusan informasi secara otomatis;
   6) Pembangunan kepedulian atas ancaman pencurian informasi, misalnya terhadap:
      a) Pengungkapan informasi sensitif untuk menghindari mencuri dengar (penyadapan) saat melakukan panggilan telepon;
      b) Akses pesan diluar kewenangannya;
      c) Pemrograman mesin faksimili baik sengaja maupun tidak sengaja untuk mengirim pesan ke nomor tertentu;dan
      d) Pengiriman dokumen dan pesan ke tujuan yang salah.
d. pembangunan kepedulian atas pendaftaran data demografis, seperti alamat surat elektronik atau informasi pribadi lainnya untuk menghindari pengumpulan informasi yang tidak sah;dan
e. penyediaan informasi internal Perangkat Daerah bagi masyarakat umum harus disetujui oleh pemilik informasi dan sesuai dengan ketentuan yang berlaku.

BAB X
KEAMANAN DALAM PROSES AKUISISI, PENGEMBANGAN DAN PEMELIHARAAN SISTEM INFORMASI

A. TUJUAN

Keamanan informasi dalam pengadaan, pengembangan, dan pemeliharaan sistem informasi bertujuan untuk memastikan bahwa keamanan informasi merupakan bagian yang terintegrasi dengan sistem informasi, mencegah terjadinya kesalahan, kehilangan, serta modifikasi oleh pihak yang tidak berwenang.

B. RUANG LINGKUP

1. Persyaratan keamanan pada sistem informasi.
2. Keamanan dalam proses pengembangan dan pendukung (*support processes*).
3. Keamanan *system files*.

C. KEBIJAKAN

1. Persyaratan keamanan pada sistem informasi mencakup setidaknya hal-hal berikut ini:
   a. kepala Perangkat Daerah menetapkan dan mendokumentasikan secara jelas persyaratan keamanan informasi yang relevan sebelum pengadaan, pengembangan, atau pemeliharaan system informasi baru;dan

b. pengolahan Informasi pada Aplikasi, meliputi:
   1) Validasi data yang masuk;
      Data yang akan dimasukkan ke aplikasi harus diperiksa terlebih dahulu kebenaran dan kesesuaiannya.
   2) Pengendalian proses internal;dan
      Pada setiap aplikasi harus disertakan proses validasi untuk mendeteksi bahwa informasi yang dihasilkan utuh dan sesuai dengan yang diharapkan.
   3) Validasi data keluaran.
      Data keluaran aplikasi harus divalidasi untuk memastikan data yang dihasilkan adalah benar.

2. Keamanan dalam proses pengembangan dan pendukung *(support processes).*
   a. prosedur pengendalian perubahan sistem operasi;
      Setiap Perangkat Daerah harus mengendalikan perubahan pada sistem operasi dengan penggunaan prosedur pengendalian perubahan.
   b. prosedur pengendalian perubahan pada perangkat lunak;
      Setiap Perangkat Daerah harus mengendalikan perubahan terhadap perangkat lunak, baik perangkat lunak yang dikembangkan sendiri maupun pihak ketiga.
   c. kajian teknis aplikasi setelah perubahan sistem operasi dan/atau perangkat lunak;
      Setiap Perangkat Daerah harus meninjau dan menguji sistem operasi dan/atau perangkat lunak untuk memastikan tidak ada dampak merugikan pada proses operasional atau keamanan informasi di Perangkat Daerah yang bersangkutan apabila terjadi perubahan sistem operasi dan/atau perangkat lunak, terutama pada perangkat lunak yang memproses informasi yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA.
   d. kebocoran informasi;
      Setiap Perangkat Daerah harus mencegah kemungkinan terjadinya kebocoran informasi.
   e. pengembangan perangkat lunak oleh pihak ketiga.
      Kepala Perangkat Daerah harus melakukan supervisi dan memantau pengembangan perangkat lunak oleh pihak ketiga.

3. Keamanan *System File*.
   a. pengendalian operasional perangkat lunak;
      Setiap Perangkat Daerah harus mempunyai prosedur untuk pengendalian perangkat lunak pada sistem operasional.
   b. perlindungan terhadap sistem pengujian data;
      Setiap Perangkat Daerah harus menentukan sistem pengujian data, melindunginya dari kemungkinan kerusakan, kehilangan atau perubahan oleh pihak yang tidak berwenang.
   c. pengendalian akses ke kode program *(source code).*
      Setiap Perangkat Daerah harus mengendalikan akses ke kode program *(source code)* secara ketat dan salinan versi terkini dari perangkat lunak disimpan di tempat yang aman.

D. STANDAR

1. Spesifikasi kebutuhan perangkat pengolah informasi yang dikembangkan baik oleh internal atau pihak ketiga harus didokumentasikan secara formal.
2. Standar Pengolahan Data pada Aplikasi adalah sebagai berikut:
   a. pemeriksaan data masukan harus mempertimbangkan:
      1) Penerapan masukan rangkap *(dual input)* atau mekanisme pengecekan masukan lainnya untuk mendeteksi kesalahan berikut:
         a) Di luar rentang/batas nilai-nilai yang diperbolehkan;
         b) Karakter tidak valid dalam *field* data;

c) Data hilang atau tidak lengkap;
d) Melebihi batas atas dan bawah volume data;dan
e) Data yang tidak diotorisasi dan tidak konsisten.

2) Pengkajian secara berkala terhadap isi *field* kunci *(key field)* atau *file* data untuk mengkonfirmasi keabsahan dan integritas data;
3) Memeriksa dokumen *hard copy* untuk memastikan tidak adanya perubahan data masukan yang tidak melalui otorisasi;
4) Menampilkan pesan yang sesuai dalam menanggapi kesalahan validasi;
5) Prosedur untuk menguji kewajaran dari data masukan;
6) Menguraikan tanggung jawab dari seluruh pegawai yang terkait dalam proses perekaman data;dan
7) Sistem mampu membuat dari mengeluarkan catatan aktivitas terkait proses perekaman data.

b. menyusun daftar pemeriksaan *(check list)* yang sesuai, mendokumentasikan proses pemeriksaan, dan menyimpan hasilnya secara aman. Proses pemeriksaan meliputi:
1) Pengendalian *session* atau *batch*, untuk mencocokkan data setelah perubahan transaksi;
2) Pengendalian *balancing* untuk memeriksa data sebelum dan sesudah transaksi;
3) Validasi data masukan yang dihasilkan system;
4) Keutuhan dan keaslian data yang diunduh/diunggah (*download/upload*);
5) *Hash totals* dari *record* dan *file*;
6) Aplikasi berjalan sesuai dengan rencana dan waktu yang ditentukan;
7) Program dijalankan dalam urutan yang benar dan menghentikan sementara jika terjadi kegagalan sampai masalah diatasi;dan
8) Sistem mampu membuat dan mengeluarkan catatan aktivitas pengelolaan internal.

c. pemeriksaan data keluaran harus mempertimbangkan:
1) Kewajaran dari data keluaran yang dihasilkan;
2) Pengendalian rekonsiliasi data untuk memastikan kebenaran pengolahan data;
3) Menyediakan informasi yang cukup untuk pengguna atau sistem pengolahan informasi untuk menentukan akurasi, kelengkapan, ketepatan, dan klasifikasi informasi;
4) Prosedur untuk menindaklanjuti validasi data keluaran;
5) Menguraikan tanggung jawab dari seluruh pegawai yang terkait proses data keluaran;dan
6) Sistem mampu membuat dan mengeluarkan catatan aktivitas dalam proses validasi data keluaran.

3. Keamanan *System File.*
a. pengembangan prosedur pengendalian perangkat lunak pada sistem operasional harus mempertimbangkan:
1) Proses pemutakhiran perangkat lunak operasional, aplikasi hanya boleh dilakukan oleh *system administrator* terlatih setelah melalui proses otorisasi;
2) Sistem operasional hanya berisi program aplikasi *executable* yang telah diotorisasi, tidak boleh berisi kode program *(source code)* atau *compiler*;
3) Aplikasi dan perangkat lunak sistem operasi hanya dapat diimplementasikan setelah melewati proses pengujian yang ekstensif;
4) Sistem pengendalian konfigurasi harus digunakan untuk mengendalikan seluruh perangkat lunak yang telah diimplementasikan beserta dokumentasi system;
5) Strategi *rollback* harus tersedia sebelum suatu perubahan diimplementasikan;

6) Catatan audit harus dipelihara untuk menjaga kemutakhiran informasi atau data operasional;
7) Versi terdahulu dari suatu aplikasi harus tetap disimpan untuk keperluan kontinjensi;dan
8) Versi lama dari suatu perangkat lunak harus diarsip, bersama dengan informasi terkait dan prosedur, parameter, konfigurasi rinci, dan perangkat lunak pendukung.

b. perlindungan terhadap sistem pengujian data harus mempertimbangkan:
1) Prosedur pengendalian akses, yang berlaku pada sistem aplikasi operasional, harus berlaku juga pada sistem aplikasi pengujian;
2) Proses otorisasi setiap kali informasi atau data operasional digunakan pada sistem pengujian;
3) Penghapusan informasi atau data operasional yang digunakan pada system pengujian segera setelah proses pengujian selesai; dan
4) Pencatatan jejak audit penggunaan informasi atau data operasional.

c. pengendalian akses ke kode program *(source code)* harus mempertimbangkan:
1) Kode program *(source code)* tidak boleh disimpan pada sistem operasional;
2) Pengelolaan kode program *(source code)* dan *library* harus mengikuti prosedur yang telah ditetapkan;
3) Pengelola Teknologi Informasi tidak boleh memiliki akses yang tidak terbatas ke kode program *(source code)* dan *library*;
4) Proses pemutakhiran kode program *(source code)* dan item terkait, serta pemberian kode program *(source code)* kepada programmer hanya dapat dilakukan setelah melalui proses otorisasi;
5) *Listing* program harus disimpan dalam *secure areas*;
6) Catatan audit dari seluruh akses ke kode program *(source code) library* harus dipelihara;dan
7) Pemeliharaan dan penyalinan kode program *(source code) library* harus mengikuti prosedur pengendalian perubahan.

4. Keamanan dalam proses pengembangan dan pendukung *(support processes).*

a. prosedur pengendalian perubahan sistem operasi dan perangkat lunak, meliputi:
1) Memelihara catatan persetujuan sesuai dengan kewenangannya;
2) Memastikan permintaan perubahan diajukan oleh pihak yang berwenang;
3) Melakukan *review* untuk memastikan bahwa tidak ada penurunan kualitas prosedur pengendalian dan integritas akibat permintaan perubahan;
4) Melakukan identifikasi terhadap perangkat lunak, informasi, basis data, dan perangkat keras yang perlu diubah;
5) Mendapatkan persetujuan formal dari pihak yang berwenang sebelum pelaksanaan perubahan;
6) Memastikan pihak yang berwenang menerima perubahan yang diminta sebelum dilakukan implementasi;
7) Memastikan bahwa dokumentasi sistem mutakhir dan dokumen versi sebelumnya diarsip;
8) Memelihara versi perubahan aplikasi;
9) Memelihara jejak audit perubahan aplikasi;
10) Memastikan dokumentasi penggunaan dan prosedur telah diubah sesuai dengan perubahan yang dilaksanakan;dan
11) Memastikan bahwa implementasi perubahan dilakukan pada waktu yang tepat dan tidak menganggu kegiatan.

b. prosedur kajian teknis aplikasi setelah perubahan sistem operasi dan/atau perangkat lunak, meliputi:

1) Melakukan *review* untuk memastikan bahwa tidak ada penurunan kualitas prosedur pengendalian dan integritas akibat permintaan perubahan;
2) Memastikan rencana dan anggaran *annual support* yang mencakup *review* dan sistem *testing* dari perubahan sistem operasi;
3) Memastikan pemberitahuan perubahan sistem informasi dilakukan dalam jangka waktu yang tepat untuk memastikan tes dan *review* telah dilaksanakan sebelum implementasi;dan
4) Memastikan bahwa perubahan telah diselaraskan dengan rencana Kelangsungan kegiatan.

c. kebocoran informasi;
Pengendalian yang dapat diterapkan untuk membatasi risiko kebocoran informasi, antara lain:
1) Melakukan *monitoring* terhadap aktivitas pegawai dan pihak ketiga, sistem sesuai dengan ketentuan yang berlaku;dan
2) Melakukan *monitoring* terhadap aktivitas penggunaan desktop dan perangkat *mobile*.

d. pengembangan perangkat lunak oleh pihak ketiga harus mempertimbangkan:
1) Perjanjian lisensi, kepemilikan *source code*, dan Hak Atas Kekayaan Intelektual (HAKI);
2) Perjanjian *escrow* (Jaminan Pelaksanaan);
3) Hak untuk melakukan audit terhadap kualitas dan akurasi pekerjaan;
4) Persyaratan kontrak mengenai kualitas dan fungsi keamanan aplikasi;dan
5) Uji coba terhadap aplikasi untuk memastikan tidak terdapat *malicious code* sebelum implementasi.

BAB XI
HUBUNGAN KERJA DENGAN PIHAK KETIGA ATAU PENYEDIA JASA ATAU BARANG

A. TUJUAN

Pengelolaan hubungan dengan pihak ketiga atau penyedia jasa/barang bertujuan untuk memastikan terlindungnya aset-aset organisasi di setiap Perangkat Daerah yang dapat diakses oleh pihak ketiga atau penyedia jasa/barang serta mempertahankan tingkat keamanan informasi dan pelayanan yang telah disepakati dengan pihak ketiga atau penyedia jasa/barang.

B. RUANG LINGKUP

Kebijakan dan standar pengelolaan hubungan dengan pihak ketiga atau penyedia jasa/barang ini meliputi:
1. Pengendalian hubungan dengan pihak ketiga atau penyedia jasa/barang;
2. Keamanan informasi dalam kesepakatan dengan penyedia layanan (pihak ketiga atau penyedia jasa/barang);
3. Pengkajian terhadap kinerja penyedia layanan (pihak ketiga atau penyedia jasa/barang);dan
4. Pengelolaan perubahan terhadap layanan yang disediakan oleh pihak ketiga atau penyedia jasa/barang.

C. KEBIJAKAN

1. Kepala Perangkat Daerah harus menerapkan pengendalian keamanan informasi berdasarkan hasil penilaian risiko untuk mencegah atau mengurangi dampak risiko terkait dengan pemberian akses kepada pihak ketiga.

2. Kepala Perangkat Daerah harus memastikan bahwa pengendalian keamanan informasi, definisi layanan, dan tingkat layanan yang tercantum dalam kesepakatan penyediaan layanan telah diterapkan, dioperasikan, dan dipelihara oleh pihak ketiga atau penyedia jasa/barang.
3. Kepala Perangkat Daerah harus memastikan terdapat persyaratan untuk mengatasi risiko keamanan informasi pada kesepakatan dengan pihak ketiga atau penyedia jasa/barang yang berhubungan dengan layanan teknologi informasi dan komunikasi serta rantai pasokan produk.
4. Kepala Perangkat Daerah harus melakukan *monitoring* dan kajian terhadap kinerja penyediaan layanan, laporan, dan catatan yang disediakan oleh pihak ketiga atau penyedia jasa/barang secara berkala.
5. Kepala Perangkat Daerah harus memperhatikan kritikalitas, proses yang terkait, dan hasil penilaian ulang risiko layanan apabila terjadi perubahan pada layanan yang disediakan pihak ketiga atau penyedia jasa/barang.

D. STANDAR

Standar monitoring dan pengkajian layanan dari pihak ketiga, serta laporan dan catatan dari pihak ketiga mencakup proses sebagai berikut:

1. Monitoring tingkat kinerja layanan untuk memastikan kesesuaian kepatuhan dengan perjanjian;
2. Pengkajian laporan layanan pihak ketiga dan pengaturan pertemuan berkala dalam rangka pembahasan perkembangan layanan sebagaimana diatur dalam perjanjian atau kesepakatan;
3. Pemberian informasi tentang gangguan keamanan informasi dan pengkajian informasi ini bersama pihak ketiga sebagaimana diatur dalam perjanjian atau kesepakatan;
4. Pemeriksaan jejak audit pihak ketiga dan pencatatan peristiwa keamanan, masalah operasional, kegagalan, dan gangguan yang terkait dengan layanan yang diberikan;dan
5. Penyelesaian dan pengelolaan masalah yang teridentifikasi.

BAB XII
PENANGANAN INSIDEN KEAMANAN INFORMASI

A. TUJUAN

Pengelolaan gangguan keamanan informasi bertujuan untuk memastikan kejadian dan kelemahan keamanan informasi yang terhubung dengan sistem informasi dikomunikasikan untuk dilakukan perbaikan, serta dilakukan pendekatan yang konsisten dan efektif agar dapat dihindari atau tidak terulang kembali.

B. RUANG LINGKUP

Kebijakan dan standar pengelolaan gangguan keamanan informasi ini meliputi:

1. Pelaporan kejadian dan kelemahan keamanan informasi;dan
2. Pengelolaan gangguan keamanan informasi dan perbaikannya.

C. KEBIJAKAN

1. Pelaporan Kejadian dan Kelemahan Keamanan Informasi.
   a. pegawai dan pihak ketiga harus melaporkan kepada Kepala Perangkat Daerah sesegera mungkin pada saat menemui kelemahan atau terjadi gangguan keamanan informasi dalam sistem atau layanan Teknologi Informasi pada Perangkat Daerah;dan
   b. proses penanganan gangguan di setiap Perangkat Daerah akan ditetapkan dalam ketentuan tersendiri.

2. Pengelolaan Gangguan Keamanan Informasi dan Perbaikannya.
   a. prosedur dan tanggung jawab;
      Setiap Perangkat Daerah harus menyusun prosedur dan menguraikan tanggung jawab pegawai, terkait dalam rangka memastikan gangguan keamanan informasi dapat ditangani secara cepat dan efektif.
   b. peningkatan penanganan gangguan keamanan informasi;
      1) Seluruh gangguan keamanan informasi yang terjadi dan tindakan mengatasinya harus dicatat dalam suatu basis data dan/atau buku catatan pelaporan gangguan keamanan informasi, dan akan menjadi masukan pada proses peningkatan penanganan gangguan keamanan informasi;dan
      2) Seluruh catatan gangguan keamanan informasi akan dievaluasi dan dianalisa untuk perbaikan dan pencegahan agar gangguan keamanan informasi tidak terulang.
   c. pengumpulan bukti pelanggaran.
      Mengumpulkan, menyimpan, dan menyajikan bukti pelanggaran terhadap Kebijakan dan Standar SMKI kepada Tim Keamanan Informasi yang ada di Perangkat Daerah yang bersangkutan.
   d. pengkajian terhadap kejadian keamanan informasi;dan
      Kepala Perangkat Daerah perlu melakukan pengkajian terhadap kejadian keamanan informasi serta memutuskan dari hasil kajian apakah kejadian tersebut tergolong ke dalam gangguan keamanan informasi.
   e. kepala Perangkat Daerah harus memastikan bahwa seluruh gangguan keamanan informasi yang terjadi ditanggapi sesuai dengan prosedur formal penanganan gangguan keamanan informasi yang berlaku.

D. STANDAR
1. Pelaporan Kejadian dan Kelemahan Keamanan Informasi.
   a. gangguan keamanan informasi antara lain:
      1) Hilangnya layanan, perangkat, atau fasilitas Teknologi Informasi;
      2) Kerusakan fungsi sistem atau kelebihan beban;
      3) Perubahan sistem diluar kendali;
      4) Kerusakan fungsi perangkat lunak atau perangkat keras;
      5) Pelanggaran akses ke dalam sistem pengolah informasi Teknologi Informasi;
      6) Kelalaian manusia;dan
      7) Ketidaksesuaian dengan ketentuan yang berlaku.
   b. pegawai dan pihak ketiga harus menyadari tanggung jawab mereka untuk melaporkan setiap gangguan keamanan informasi secepat mungkin. Pelaporan gangguan harus meliputi:
      1) Proses umpan balik yang sesuai untuk memastikan bahwa pihak yang melaporkan kejadian keamanan informasi mendapatkan pemberitahuan penanganan masalah;
      2) Formulir laporan gangguan keamanan informasi untuk mendukung tindakan pelaporan dan membantu pelapor mengingat kronologis kejadian keamanan informasi; dan
      3) Perilaku yang benar dalam menghadapi gangguan keamanan informasi, antara lain:
         a) mencatat semua rincian penting gangguan dengan segera, seperti jenis pelanggaran, jenis kerusakan, pesan pada layar, atau anomali sistem;dan
         b) segera melaporkan gangguan ke pihak berwenang sebelum melakukan tindakan penanganan sendiri.
      4) Bukti-bukti pendukung sebagai referensi yang digunakan dalam proses penanganan pelanggaran disiplin bagi pegawai dan pihak ketiga yang melakukan pelanggaran keamanan informasi.

2. Prosedur Pengelolaan Gangguan Keamanan Informasi.
   Prosedur pengelolaan gangguan keamanan informasi harus mempertimbangkan:
   a. prosedur yang harus ditetapkan untuk menangani berbagai jenis gangguan keamanan informasi, antara lain:
      1) Kegagalan sistem informasi dan hilangnya layanan;
      2) Serangan program yang membahayakan *(malicious code)*;
      3) Serangan *denial of service;*
      4) Kesalahan akibat data tidak lengkap atau tidak akurat;
      5) Pelanggaran kerahasiaan dan keutuhan;dan
      6) Penyalahgunaan sistem informasi.
   b. untuk melengkapi rencana kontingensi, prosedur harus meliputi:
      1) Analisis dan identifikasi penyebab gangguan;
      2) Mengarantina atau membatasi gangguan;
      3) Perencanaan dan pelaksanaan tindakan korektif untuk mencegah gangguan berulang;
      4) Komunikasi dengan pihak-pihak yang terkena dampak pemulihan gangguan;dan
      5) Pelaporan tindakan ke pihak berwenang.
   c. jejak audit dan bukti serupa harus dikumpulkan dan diamankan untuk:
      1) Analisis masalah internal;
      2) Digunakan sebagai bukti forensik yang berkaitan dengan potensi pelanggaran kontrak atau peraturan atau persyaratan dalam hal proses pidana atau perdata;dan
      3) Digunakan sebagai bahan tuntutan ganti rugi pada pihak ketiga yang menyediakan perangkat lunak dan layanan.
   d. tindakan untuk memulihkan keamanan dari pelanggaran dan perbaikan kegagalan sistem harus dikendalikan secara hati-hati dan formal, prosedur harus memastikan:
      1) Hanya pegawai yang sudah diidentifikasi dan berwenang yang diizinkan akses langsung ke sistem dan data;
      2) Semua tindakan darurat yang diambil, didokumentasikan secara rinci;
      3) Tindakan darurat dilaporkan kepada pihak berwenang;dan
      4) Keutuhan sistem dan pengendaliannya dikonfirmasikan dengan pihakpihak terkait sesegera mungkin.

BAB XIII
KELANGSUNGAN KEGIATAN

A. TUJUAN

Pengendalian terhadap aspek keamanan informasi dalam pengelolaan kelangsungan kegiatan bertujuan untuk melindungi sistem informasi, memastikan berlangsungnya kegiatan dan layanan pada saat keadaan darurat, serta memastikan pemulihan yang tepat.

B. RUANG LINGKUP

Kebijakan dan standar keamanan informasi dalam pengelolaan kelangsungan kegiatan ini meliputi:

1. Proses Pengelolaan Kelangsungan Kegiatan;
2. Penilaian Risiko dan Analisis Dampak Bisnis *(Business Impact Analysis/BIA)*;
3. Penyusunan dan Penerapan Rencana Kelangsungan Kegiatan *(Business Continuity Plan/BCP)*;
4. Pengujian, Pemeliharaan, dan Pengkajian Ulang Rencana Kelangsungan Kegiatan;dan
5. Menerapkan Kelangsungan Keamanan Informasi.

C. KEBIJAKAN

1. Setiap Perangkat Daerah harus mengelola proses kelangsungan kegiatan pada saat keadaan darurat di lingkungan kerja masing-masing.
2. Setiap Perangkat Daerah harus mengidentifikasi risiko, dan menganalisis dampak yang diakibatkan pada saat terjadi keadaan darurat untuk menjamin kelangsungan kegiatan.
3. Setiap Perangkat Daerah harus menyusun dan menerapkan Rencana Kelangsungan Kegiatan untuk menjaga dan mengembalikan kegiatan operasional dalam jangka waktu yang disepakati dan level yang dibutuhkan.
4. Setiap Perangkat Daerah harus memelihara dan memastikan rencana-rencana yang termuat dalam Rencana Kelangsungan Kegiatan masih sesuai, dan mengidentifikasi prioritas untuk kegiatan uji coba.
5. Setiap Perangkat Daerah harus melakukan uji coba Rencana Kelangsungan Kegiatan secara berkala untuk memastikan Rencana Kelangsungan Kegiatan dapat dilaksanakan secara efektif.
6. Setiap Perangkat Daerah harus menetapkan, mendokumentasikan, menerapkan dan memelihara proses, prosedur dan kontrol untuk memastikan tingkat kelangsungan keamanan informasi yang diperlukan selama terjadi situasi yang merugikan.
7. Fasilitas yang digunakan untuk memproses data atau informasi perlu mengimplementasikan sistem cadangan (*redudancy*) untuk menjamin ketersediaan terhadap data atau informasi organisasi.

D. STANDAR

1. Pengelolaan Kelangsungan Kegiatan pada saat Keadaan Darurat Komponen yang harus diperhatikan dalam mengelola proses kelangsungan kegiatan:
   a. identifikasi risiko dan analisis dampak yang diakibatkan pada saat terjadi keadaan darurat;
   b. identifikasi seluruh aset informasi yang menunjang proses kegiatan kritikal;
   c. identifikasi sumber daya, mencakup biaya, struktur organisasi, teknis pelaksanaan, pegawai dan pihak ketiga;
   d. memastikan keselamatan pegawai, dan perlindungan terhadap perangkat pengolah informasi dan aset organisasi;
   e. penyusunan dan pendokumentasian Rencana Kelangsungan Kegiatan sesuai dengan Rencana Strategi (Renstra) Kepala Perangkat Daerah; dan
   f. pelaksanaan uji coba dan pemeliharaan Rencana Kelangsungan Kegiatan secara berkala.
2. Proses identifikasi risiko mengikuti ketentuan mengenai Penerapan Manajemen Risiko di setiap Perangkat Daerah.
3. Proses analisis dampak kegiatan harus melibatkan pemilik proses bisnis dan dievaluasi secara berkala.
4. Penyusunan Rencana Kelangsungan Kegiatan meliputi:
   a. prosedur saat keadaan darurat, mencakup tindakan yang harus dilakukan serta pengaturan hubungan dengan pihak berwenang;
   b. prosedur *fallback*, mencakup tindakan yang harus diambil untuk memindahkan kegiatan kritikal atau layanan pendukung ke lokasi kerja sementara, dan mengembalikan operasional kegiatan kritikal dalam jangka waktu sesuai dengan standar ketersediaan data yang berlaku di setiap Perangkat Daerah;
   c. prosedur saat kondisi telah normal *(resumption)*, adalah tindakan mengembalikan kegiatan operasional ke kondisi normal;
   d. jadwal uji coba, mencakup langkah-langkah dan waktu pelaksanaan uji coba serta proses pemeliharaannya;

e. pelaksanaan pelatihan dan sosialisasi dalam rangka meningkatkan kepedulian dan pemahaman proses kelangsungan kegiatan dan memastikan proses kelangsungan kegiatan dilaksanakan secara efektif;
f. tanggung jawab dan peran setiap Petugas Pelaksana Pengelolaan Proses Kelangsungan;dan
g. daftar kebutuhan aset informasi kritikal dan sumber daya untuk dapat menjalankan prosedur saat keadaan darurat, *fallback* dan saat kondisi telah normal *(resumption)*.

5. Uji Coba Rencana Kelangsungan Kegiatan harus dilaksanakan untuk memastikan setiap rencana yang disusun dapat dilakukan atau dipenuhi pada saat penerapannya. Kegiatan uji coba Rencana Kelangsungan Kegiatan ini meliputi:
   a. simulasi terutama untuk Petugas Pelaksana Pengelolaan Proses Kelangsungan Kegiatan;
   b. uji coba *recovery* sistem informasi untuk memastikan sistem informasi dapat berfungsi kembali;
   c. uji coba proses *recovery* di lokasi kerja sementara untuk menjalankan proses bisnis secara paralel;
   d. uji coba terhadap perangkat dan layanan yang disediakan oleh pihak ketiga;dan
   e. uji coba keseluruhan mulai dari organisasi, petugas, peralatan, perangkat, dan prosesnya.

BAB XIV
KEPATUHAN

A. TUJUAN

Pengendalian kepatuhan bertujuan untuk menghindari pelanggaran terhadap peraturan perundangan yang terkait keamanan informasi.

B. RUANG LINGKUP

Kebijakan dan standar kepatuhan ini meliputi:
1. Kepatuhan terhadap peraturan perundangan yang terkait keamanan informasi;
2. Kepatuhan teknis;dan
3. Audit sistem informasi.

C. KEBIJAKAN

1. Kepatuhan terhadap peraturan perundangan yang terkait Keamanan lnformasi.
   a. seluruh pegawai dan pihak ketiga harus menaati peraturan perundangan yang terkait dengan keamanan informasi;
   b. identifikasi peraturan perundangan yang dapat diterapkan;
      Setiap Perangkat Daerah harus mengidentifikasi, mendokumentasikan dan memelihara kemutakhiran semua peraturan perundangan yang terkait dengan sistem keamanan informasi.
   c. hak Atas Kekayaan Intelektual;
      Perangkat lunak yang dikelola Perangkat Daerah harus mematuhi ketentuan penggunaan lisensi. Penggandaan perangkat lunak secara tidak sah tidak diizinkan dan merupakan bentuk pelanggaran.
   d. perlindungan terhadap rekaman;dan
      Rekaman milik Perangkat Daerah harus dilindungi dari kehilangan, kerusakan atau penyalahgunaan.
   e. pengamanan data.
      Setiap Perangkat Daerah melindungi kepemilikan dan kerahasiaan data. Data hanya digunakan untuk kepentingan yang dibenarkan oleh peraturan perundangan dan kesepakatan.

2. Kepatuhan Teknis
   Setiap Perangkat Daerah melakukan pemeriksaan kepatuhan teknis secara berkala untuk menjamin efektivitas standar dan prosedur keamanan informasi yang ada di area operasional.
3. Audit Sistem Informasi.
   a. pengendalian audit sistem informasi;
      Kepala Perangkat Daerah bersama dengan Unit Terkait harus membuat perencanaan persyaratan, ruang lingkup, dan kegiatan audit yang melibatkan pemeriksaan sistem operasional untuk mengurangi kemungkinan risiko gangguan yang bisa terjadi terhadap kegiatan pada Perangkat Daerah selama proses audit.
   b. perlindungan terhadap alat bantu *(tools)* audit sistem informasi;dan
      Penggunaan alat bantu (baik perangkat lunak maupun perangkat keras) untuk mengetahui kelemahan keamanan, memindai *(scanning)* kata sandi, atau untuk melemahkan dan menerobos sistem keamanan informasi tidak diizinkan kecuali atas persetujuan Pimpinan Perangkat Daerah yang bersangkutan.
   c. audit sistem informasi di setiap Perangkat Daerah akan ditetapkan dalam ketentuan tersendiri.

D. STANDAR
1. Kepatuhan terhadap Hak Kekayaan Intelektual.
   Hal yang perlu diperhatikan dalam melindungi segala materi yang dapat dianggap kekayaan intelektual meliputi:
   a. mendapatkan perangkat lunak hanya melalui sumber yang dikenal dan memiliki reputasi baik, untuk memastikan hak cipta tidak dilanggar;
   b. memelihara daftar aset informasi sesuai persyaratan untuk melindungi hak kekayaan intelektual;
   c. memelihara bukti kepemilikan lisensi, *master disk*, buku manual, dan lain sebagainya;
   d. menerapkan pengendalian untuk memastikan jumlah pengguna tidak melampaui lisensi yang dimiliki;
   e. melakukan pemeriksaan bahwa hanya perangkat lunak dan produk berlisensi yang dipasang;
   f. patuh terhadap syarat dan kondisi untuk perangkat lunak dan informasi yang didapat dari jaringan publik;
   g. dilarang melakukan duplikasi, konversi ke format lain atau mengambil dari rekaman komersial (film atau audio), selain yang diperbolehkan oleh Undang-Undang Hak Cipta;dan
   h. tidak menyalin secara penuh atau sebagian buku, artikel, laporan, atau dokumen lainnya, selain yang diizinkan oleh Undang-Undang Hak Cipta.
2. Kepatuhan terhadap Kebijakan dan Standar.
   Hal yang perlu dilakukan jika terdapat ketidakpatuhan teknis meliputi:
   a. menentukan dan mengevaluasi penyebab ketidakpatuhan;
   b. menentukan tindakan yang perlu dilakukan berdasarkan hasil evaluasi agar ketidakpatuhan tidak terulang kembali;
   c. menentukan dan melaksanakan Tindakan perbaikan yang sesuai; dan
   d. mengkaji tindakan perbaikan yang dilakukan.
3. Kepatuhan Teknis.
   Sistem informasi harus diperiksa secara berkala untuk memastikan pengendalian perangkat keras dan perangkat lunak telah diimplementasikan secara benar. Kepatuhan teknis juga meliputi pengujian penetrasi *(penetration testing)* untuk mendeteksi kerentanan dalam sistem, dan memeriksa pengendalian akses untuk mencegah kerentanan tersebut telah diterapkan.

4. Kepatuhan terkait Audit Sistem Informasi.
   Proses audit sistem informasi harus memperhatikan hal-hal berikut:
   a. persyaratan audit harus disetujui oleh Kepala Perangkat Daerah;
   b. ruang lingkup pemeriksaan atau audit harus disetujui dan dikendalikan oleh pihak berwenang;
   c. pemeriksaan perangkat lunak dan data harus dibatasi untuk akses baca saja *(read-only)*;
   d. selain akses baca saja hanya diizinkan untuk salinan dari *file* sistem yang diisolasi, yang harus dihapus bila audit telah selesai, atau diberikan perlindungan yang tepat jika ada kewajiban untuk menyimpan *file* tersebut di bawah persyaratan dokumentasi audit;
   e. sumber daya untuk melakukan pemeriksaan harus secara jelas diidentifikasi dan tersedia;
   f. persyaratan untuk pengolahan khusus atau tambahan harus diidentifikasi dan disepakati;
   g. semua akses harus dipantau dan dicatat untuk menghasilkan jejak audit, dan untuk data dan sistem informasi sensitif harus mempertimbangkan pencatatan waktu *(timestamp)* pada jejak audit;
   h. semua prosedur, persyaratan, dan tanggung jawab harus didokumentasikan;dan
   i. auditor harus independen dari kegiatan yang diaudit.

ISTILAH YANG DIGUNAKAN

1. Akun adalah identifikasi pengguna yang diberikan oleh unit Pengelola Teknologi Informasi, bersifat unik dan digunakan bersamaan dengan kata sandi ketika akan memasuki sistem Teknologi Informasi.
2. Akun khusus adalah akun yang diberikan oleh unit Pengelola Teknologi Informasi sesuai kebutuhan tetapi tidak terbatas pada pengelolaan Teknologi Informasi (baik berupa aplikasi atau sistem), dan kelompok kerja (baik berupa acara kedinasan, tim, atau unit kerja).
3. Aset fisik adalah jenis aset yang memiliki wujud fisik, misalnya perangkat komputer, perangkat jaringan dan komunikasi, *removable media*, dan perangkat pendukung lainnya.
4. Aset tak berwujud adalah jenis aset yang tidak memiliki wujud fisik, misalnya pengetahuan, pengalaman, keahlian, citra, dan reputasi. Aset ini mempunyai umur lebih dari satu tahun (aset tidak lancar) dan dapat diamortisasi selama periode pemanfaatannya, yang biasanya tidak lebih dari empat puluh tahun.
5. Catatan dalam penggunaannya, data dapat berupa informasi yang menjadi data baru, sebaliknya informasi dapat berfungsi sebagai data untuk menghasilkan informasi baru.
6. Kepala Perangkat Daerah adalah jabatan umum yang diberikan kepada seseorang sebagai kepala teknologi informasi pada suatu organisasi.
7. *Conduit* adalah sebuah tabung atau saluran untuk melindungi kabel yang biasanya terbuat dari baja.
8. Daftar inventaris aset informasi adalah kumpulan informasi yang memuat bentuk, pemilik, lokasi, retensi, dan hal-hal yang terkait dengan aset informasi.
9. Data adalah catatan atas kumpulan fakta yang mempunyai arti baik secara kualitatif maupun kuantitatif.
10. *Denial of service* adalah suatu kondisi dimana sistem tidak dapat memberikan layanan secara normal, yang disebabkan oleh suatu proses yang tidak terkendali baik dari dalam maupun dari luar sistem.
11. Direktori adalah hirarki atau *tree structure*.
12. Dokumen SMKI adalah dokumen terkait pelaksanaan SMKI yang meliputi antara lain dokumen kebijakan, standar, prosedur, dan catatan penerapan SMKI.

13. *Fallback* adalah suatu tindakan pembalikan atau menarik diri dari posisi awal.
14. Fasilitas adalah sarana untuk melancarkan pelaksanaan fungsi atau mempermudah sesuatu.
15. Fasilitas utama adalah sarana utama gedung atau bangunan, seperti: pusat kontrol listrik, CCTV.
16. *Fault logging* adalah pencatatan permasalahan sistem informasi.
17. Hak akses khusus adalah akses terhadap sistem informasi sensitif, termasuk di dalamnya dan tidak terbatas pada sistem operasi, perangkat penyimpanan *(storage devices)*, *file server*, dan aplikasi-aplikasi sensitif, hanya diberikan kepada pengguna yang membutuhkan dan pemakaiannya terbatas dan dikontrol.
18. *Hash totals* adalah nilai pemeriksa kesalahan yang diturunkan dari penambahan satu himpunan bilangan yang diambil dari data (tidak harus berupa data numerik) yang diproses atau dimanipulasi dengan cara tertentu.
19. Informasi adalah hasil pemrosesan, manipulasi dan pengorganisasian data yang dapat disajikan sebagai pengetahuan.
20. Jejak audit *(audit trails)* adalah urutan kronologis catatan audit yang berkaitan dengan pelaksanaan suatu kegiatan.
21. Kata sandi adalah serangkaian kode yang dibuat Pengguna, bersifat rahasia dan pribadi digunakan bersamaan dengan Akun Pengguna.
22. Keamanan informasi adalah perlindungan aset informasi dari berbagai bentuk ancaman untuk memastikan kelangsungan kegiatan, menjamin kerahasiaan, keutuhan, dan ketersediaan aset informasi.
23. Komunitas keamanan informasi adalah kelompok/komunitas yang memiliki pengetahuan/keahlian khusus dalam bidang keamanan informasi atau yang relevan dengan keamanan informasi, seperti: Indonesia *Security Incident Response Team on Internet and Infrastructure* (ID-SIRTII), Unit *Cybercrime* POLRI, ISC2, ISACA.
24. Koneksi eksternal *(remote access)* adalah suatu akses jaringan komunikasi dari luar organisasi ke dalam organisasi.
25. Kriptografi adalah ilmu yang mempelajari cara menyamarkan informasi dan mengubah kembali bentuk tersamar tersebut ke informasi awal untuk meningkatkan keamanan informasi. Dalam kriptografi terdapat dua konsep utama yakni enkripsi dan dekripsi.
26. *Malicious Code* adalah semua macam program yang membahayakan termasuk makro atau *script* yang dapat diesekusi dan dibuat dengan tujuan untuk merusak sistem komputer.
27. Master *disk* adalah media yang digunakan sebagai sumber dalam melakukan instalasi perangkat lunak.
28. *Mobile Device* adalah penggunaan perangkat komputasi yang dapat dipindah *(portable)* misalnya *notebook* dan *personal data assistant* (PDA) untuk melakukan akses, pengolahan data dan penyimpanan.
29. Penanggung jawab pengendalian dokumen adalah pihak yang memiliki kewenangan dan bertanggung jawab dalam proses pengendalian dokumen SMKI.
30. Pengguna adalah pegawai pada Perangkat Daerah atau pihak ketiga serta tidak terbatas pada pengelola Teknologi Informasi dan kelompok kerja yang diberikan hak mengakses sistem Teknologi Informasi di setiap Perangkat Daerah.
31. Pemilik aset informasi adalah unit kerja yang memiliki kewenangan terhadap aset informasi.
32. Penyedia Barang dan Jasa adalah badan usaha atau orang atau perseorangan yang menyediakan barang atau pekerjaan konstruksi/jasa konsultasi/jasa lainnya.

33. Pencatatan waktu *(timestamp)* adalah catatan waktu dalam tanggal dan/atau format waktu tertentu saat suatu aktivitas atau transaksi terjadi. Format ini biasanya disajikan dalam format yang konsisten, yang memungkinkan untuk membandingkan dua aktivitas/transaksi yang berbeda berdasarkan waktu.
34. Perangkat jaringan adalah peralatan jaringan komunikasi data seperti: modem, *hub*, *switch*, *router*, dan lain-lain.
35. Perangkat lunak adalah kumpulan beberapa perintah yang dieksekusi oleh mesin komputer dalam menjalankan pekerjaannya.
36. Perangkat pendukung adalah peralatan pendukung untuk menjamin beroperasinya perangkat keras dan perangkat jaringan serta untuk melindunginya dari kerusakan. Contoh perangkat pendukung adalah *Uninterruptible Power Supply* (UPS), pembangkit tenaga listrik atau generator, antena komunikasi.
37. Perangkat pengolah informasi adalah setiap sistem pengolah informasi, layanan atau infrastruktur. Contoh perangkat pengolah informasi adalah komputer, faksimili, telepon, mesin fotocopy.
38. Perjanjian *escrow* adalah perjanjian dengan pihak ketiga untuk memastikan apabila pihak ketiga tersebut bangkrut (mengalami *failure*) maka Perangkat Daerah yang bersangkutan berhak untuk mendapatkan kode program *(source code)*.
39. Perjanjian kerahasiaan adalah perikatan antara para pihak yang mencantumkan bahan rahasia, pengetahuan, atau informasi yang mana pihak-pihak ingin berbagi satu sama lain untuk tujuan tertentu, tetapi ingin membatasi akses dengan pihak lain.
40. Petugas Pelaksana Pengelolaan Proses Kelangsungan Kegiatan adalah pegawai yang ditunjuk oleh Kepala Perangkat Daerah untuk mengelola proses kelangsungan kegiatan pada saat keadaan darurat.
41. Pihak berwenang adalah pihak yang mempunyai kewenangan terkait suatu hal, seperti: kepolisian, instansi pemadam kebakaran, dan penyedia jasa telekomunikasi atau internet.
42. Pihak ketiga adalah semua unsur di luar pengguna unit Teknologi Informasi yang bukan bagian dari Perangkat Daerah, misal mitra kerja pada Perangkat Daerah (seperti: konsultan, penyedia jasa komunikasi, penyedia jasa/barang dan pemelihara perangkat pengolah informasi), dan kementerian/lembaga lain.
43. Proses pendukung *(support processes)* adalah proses-proses penunjang yang mendukung suatu proses utama yang terkait. Contoh proses pendukung dalam pengembangan *(development)* adalah proses pengujian perangkat lunak, proses perubahan perangkat lunak.
44. Rencana Kontijensi adalah suatu rencana ke depan pada keadaan yang tidak menentu dengan skenario, tujuan, teknik, manajemen, pelaksanaan, serta sistem penanggulangannya telah ditentukan secara bersama untuk mencegah dan mengatasi keadaan darurat.
45. *Rollback* adalah sebuah mekanisme yang digunakan untuk mengembalikan sistem ke kondisi semula sebelum perubahan diimplementasikan. Mekanisme ini biasanya terdapat pada sistem basis data.
46. *Routing* adalah sebuah mekanisme yang digunakan untuk mengarahkan dan menentukan rute atau jalur yang akan dilewati paket dari satu perangkat ke perangkat yang berada di jaringan lain.
47. *Sanitasi* adalah proses penghilangan informasi yang disimpan secara permanen dengan menggunakan medan magnet besar atau perusakan fisik.
48. Sistem informasi adalah serangkaian perangkat keras, perangkat lunak, sumber daya manusia, serta prosedur dan atau aturan yang diorganisasikan secara terpadu untuk mengolah data menjadi informasi yang berguna untuk mencapai suatu tujuan.
49. Sistem Teknologi Informasi adalah sistem operasi, sistem surat elektronik, sistem aplikasi, sistem basis data, sistem jaringan intranet/ internet, dan sebagainya.

50. *Subnet* (kependekan dari *sub network*) adalah pengelompokan secara logis dari perangkat jaringan yang terhubung.
51. Sistem administrator adalah akun khusus untuk mengelola sistem informasi.
52. *System utilities* adalah sebuah sistem perangkat lunak yang melakukan suatu tugas atau fungsi yang sangat spesifik, biasanya disediakan oleh sistem operasi, dan berkaitan dengan pengelolaan sumber daya sistem *(system resources)*, seperti *memory*, *disk*, *printer*, dan sebagainya.
53. *Teleworking* adalah penggunaan teknologi telekomunikasi untuk memungkinkan pegawai bekerja di suatu lokasi yang berada di luar kantor untuk mengakses jaringan internal kantor.

WALI KOTA CIREBON,

ttd,

NASHRUDIN AZIS

Salinan sesuai dengan aslinya,
KEPALA BAGIAN HUKUM,

FERY DJUNAEDI, SH., MH
Pembina Tk. I (IV/b)
NIP. 19711228 199803 1 002