



WALI KOTA MADIUN
SALINAN

PERATURAN WALI KOTA MADIUN
NOMOR 11 TAHUN 2023
TENTANG
SISTEM MANAJEMEN KEAMANAN INFORMASI

WALI KOTA MADIUN,

- Menimbang** :
- a. bahwa dalam rangka pelaksanaan pelayanan publik berbasis digital di lingkungan Pemerintah Kota Madiun, 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 agar pengelolaan keamanan informasi dapat berjalan lancar, berdaya guna, dan berhasil guna maka perlu dibuat dalam sistem manajemen keamanan informasi;
 - c. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b, perlu menetapkan Peraturan Wali Kota Madiun tentang Sistem Manajemen Keamanan Informasi;

- Mengingat** :
1. Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi sebagaimana telah diubah dengan Undang-Undang Nomor 11 Tahun 2020;
 2. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016;
 3. Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik;
 4. Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik;
 5. Undang-Undang Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-undangan sebagaimana telah diubah beberapa kali terakhir dengan Undang-Undang Nomor 13 Tahun 2022;

6. Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah sebagaimana telah diubah beberapa kali terakhir dengan Peraturan Pemerintah Pengganti Undang-Undang Nomor 2 Tahun 2022;
7. Undang-Undang Nomor 1 Tahun 2022 tentang Hubungan Keuangan antara Pemerintah Pusat dan Pemerintahan Daerah;
8. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik;
9. Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi;
10. 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;
11. Peraturan Daerah Kota Madiun Nomor 15 Tahun 2011 tentang Pelayanan Publik sebagaimana telah diubah dengan Peraturan Daerah Kota Madiun Nomor 5 Tahun 2019;
12. Peraturan Daerah Kota Madiun Nomor 6 Tahun 2017 tentang Pembentukan Produk Hukum Daerah;
13. Peraturan Walikota Madiun Nomor 39 Tahun 2021 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik di Lingkungan Pemerintah Kota Madiun;

MEMUTUSKAN:

Menetapkan : PERATURAN WALI KOTA MADIUN TENTANG SISTEM MANAJEMEN KEAMANAN INFORMASI.

BAB I

KETENTUAN UMUM

Pasal 1

Dalam Peraturan Wali Kota ini yang dimaksud dengan:

1. Daerah adalah Kota Madiun.
2. Pemerintah Daerah adalah Pemerintah Kota Madiun.
3. Wali Kota adalah Wali Kota Madiun.

4. Perangkat Daerah adalah Perangkat Daerah di Lingkungan Pemerintah Kota Madiun.
5. Informasi adalah keterangan, pernyataan, gagasan, dan tanda-tanda yang mengandung nilai, makna, dan pesan, baik data, fakta maupun penjelasannya yang dapat dilihat, didengar, dan dibaca yang disajikan dalam berbagai kemasan dan format sesuai dengan perkembangan teknologi informasi dan komunikasi secara elektronik ataupun non elektronik.
6. Teknologi Informasi adalah suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan/atau menyebarkan informasi.
7. 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.
8. Sistem adalah kumpulan komponen atau elemen-elemen yang saling berhubungan satu sama lain untuk mencapai suatu tujuan tertentu.
9. Keamanan Informasi adalah terjaganya kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*) informasi.
10. 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, memonitoring, mengevaluasi, mengelola, dan meningkatkan keamanan informasi.
11. Aset Informasi adalah unit informasi yang dapat dipahami, dibagi, dilindungi dan dimanfaatkan secara efektif.
12. Aset Pengolahan Informasi adalah suatu perangkat baik elektronik maupun non-elektronik yang dapat digunakan untuk membuat dan menyunting informasi.

13. Penyimpanan Informasi adalah suatu proses menyimpan informasi dengan menggunakan media baik elektronik maupun non-elektronik.
14. Perangkat Keras adalah semua jenis piranti atau komponen komputer yang bagian fisiknya dapat dilihat secara kasat mata dan dirasakan langsung.
15. Perangkat Lunak adalah satu atau sekumpulan program komputer, prosedur, dan/atau dokumentasi yang terkait dalam pengoperasian sistem elektronik.
16. Perangkat Lunak Sistem adalah jenis perangkat lunak yang digunakan untuk menjalankan atau mengoperasikan perangkat keras, diantaranya yaitu sistem operasi, pemroses bahasa, dan *driver*.
17. Pusat Data adalah suatu fasilitas untuk menempatkan sistem komputer dan perangkat-perangkat terkait, seperti sistem komunikasi data dan penyimpanan data.
18. 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.
19. Daftar Inventaris Aset Informasi adalah kumpulan informasi yang memuat bentuk, pemilik, lokasi, retensi, dan hal-hal yang terkait dengan aset informasi.
20. Data adalah catatan atas kumpulan fakta yang mempunyai arti baik secara kualitatif maupun kuantitatif.
21. Direktori adalah hirarki atau *tree structure*.
22. Dokumen Sistem Manajemen Keamanan Informasi yang selanjutnya disebut dokumen SMKI adalah dokumen terkait pelaksanaan sistem manajemen keamanan informasi yang meliputi antara lain dokumen kebijakan, standar, prosedur, dan catatan penerapan sistem manajemen keamanan informasi.
23. Fasilitas adalah sarana untuk melancarkan pelaksanaan fungsi atau mempermudah sesuatu.
24. Fasilitas Utama adalah sarana utama gedung atau bangunan.

25. 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.
26. Informasi adalah hasil pemrosesan, manipulasi dan pengorganisasian data yang dapat disajikan sebagai pengetahuan.
27. Jejak Audit adalah urutan kronologis catatan audit yang berkaitan dengan pelaksanaan suatu kegiatan.
28. Kata Sandi adalah serangkaian kode yang dibuat Pengguna, bersifat rahasia dan pribadi digunakan bersamaan dengan akun pengguna.
29. Koneksi Eksternal adalah suatu akses jaringan komunikasi dari luar organisasi ke dalam organisasi.
30. 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.
31. 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.
32. Pemilik Aset Informasi adalah unit kerja yang memiliki kewenangan terhadap aset informasi.
33. 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.
34. 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.

Pasal 2

- (1) Peraturan Wali Kota ini dimaksudkan sebagai pedoman pengelolaan SMKI secara terpadu untuk memastikan agar aspek kerahasiaan, keutuhan dan ketersediaan informasi tetap terjaga.
- (2) Pengelolaan SMKI sebagaimana dimaksud pada ayat (1) meliputi infrastruktur jaringan komputer, perangkat lunak, dan sumber daya manusia.

BAB II

PENGAMANAN INFORMASI

Pasal 3

Pengamanan informasi yang diatur dalam Peraturan Wali Kota ini meliputi:

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

Pasal 4

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

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

Pasal 5

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

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

Pasal 6

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

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

BAB III

SUMBER DAYA

Pasal 7

- (1) Pimpinan Perangkat Daerah menyediakan sumber daya yang dibutuhkan untuk membentuk dan mengimplementasikan serta meningkatkan penerapan SMKI secara berkesinambungan.
- (2) Ketentuan lebih lanjut mengenai SMKI sebagaimana dimaksud pada ayat (1) sebagaimana tercantum dalam Lampiran Peraturan Wali Kota ini.

BAB IV

STANDAR DAN PROSEDUR PENGENDALIAN

Pasal 8

- (1) Setiap Perangkat Daerah harus menyusun standar dan prosedur pengendalian kegiatan Teknologi Informasi yang memenuhi persyaratan Keamanan Informasi.
- (2) Persyaratan Keamanan Informasi sebagaimana dimaksud pada ayat (1) digunakan untuk mengimplementasikan tindakan dalam mengelola risiko yang meliputi:
 - a. organisasi Keamanan Informasi;
 - b. keamanan sumber daya manusia;
 - c. pengelolaan aset;
 - d. pengendalian akses;
 - e. kriptografi;
 - f. keamanan fisik dan lingkungan;
 - g. keamanan operasional;
 - h. keamanan komunikasi;

- i. keamanan dalam proses akuisisi, pengembangan dan pemeliharaan sistem informasi;
- j. hubungan kerja dengan pemasok (*supplier*);
- k. penanganan insiden keamanan informasi;
- l. kelangsungan usaha; dan
- m. kepatuhan.

Pasal 9

- (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 wajib mengidentifikasi dan memantau aktivitas operasional Teknologi Informasi untuk memastikan efektivitas, efisiensi, dan keamanan dari aktivitas tersebut antara lain dengan:
 - a. menerapkan perimeter fisik dan lingkungan di area kerja Pusat Data;
 - 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 10

- (1) Setiap Perangkat Daerah 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 11

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

Pasal 12

- (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 13

- (1) Apabila terjadi kebocoran Informasi yang mempunyai dampak luas pada Perangkat Daerah terkait, Pemerintah Daerah dapat menunjuk auditor independen untuk melakukan investigasi yang diperlukan.
- (2) Perangkat Daerah penyelenggara Teknologi Informasi wajib menyediakan akses kepada auditor independen sebagaimana dimaksud pada ayat (1) untuk melakukan pemeriksaan seluruh aspek terkait penyelenggaraan Teknologi Informasi.

BAB VII

PEMBINAAN, PENGAWASAN DAN EVALUASI

Pasal 14

- (1) Pembinaan dilakukan oleh Wali Kota Madiun.
- (2) Dinas Komunikasi Dan Informatika bertugas melakukan pengawasan dan evaluasi terhadap pelaksanaan kegiatan SMKI di lingkungan Pemerintah Daerah.
- (3) Pelaksanaan pengawasan dan evaluasi sebagaimana dimaksud pada ayat (2) dilaksanakan paling sedikit 1 (satu) kali dalam satu tahun.
- (4) Hasil pengawasan dan evaluasi kegiatan SMKI dilaporkan kepada Wali Kota Madiun.

BAB VIII
PENDANAAN
Pasal 15

Pendanaan pelaksanaan kegiatan SMKI dibebankan pada Anggaran Pendapatan dan Belanja Daerah dan sumber lain yang sah dan tidak mengikat.

BAB IX
KETENTUAN PENUTUP
Pasal 16

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 Madiun.

Ditetapkan di Madiun
pada tanggal 1 Maret 2023

WALI KOTA MADIUN,

ttd

Drs. H. MAIDI, SH, MM, M.Pd.

Diundangkan di Madiun
pada tanggal 1 Maret 2023

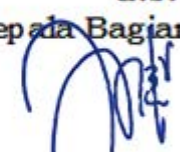
SEKRETARIS DAERAH,

ttd

Ir. SOEKO DWI HANDIARTO, M.T.
Pembina Utama Madya
NIP. 19670416 199303 1 015

BERITA DAERAH KOTA MADIUN
TAHUN 2023 NOMOR 11/G

Salinan sesuai dengan aslinya
a.n. WALIKOTA MADIUN
Sekretaris Daerah
u.b.
Kepada Bagian Hukum


BUDI WIBOWO, SH
Pembina Tingkat I
NIP. 19750117 199602 1 001

BAB I

PENDAHULUAN

A. LATAR BELAKANG

Informasi adalah aset yang sangat penting bagi Instansi Pemerintah Daerah, baik informasi yang terkait dengan data, keuangan, laporan maupun informasi lainnya. Kebocoran, kerusakan, ketidakakuratan, ketidaktersediaan atau gangguan lain terhadap informasi tersebut dapat menimbulkan dampak yang merugikan baik secara finansial maupun non finansial bagi layanan Pemerintah Daerah. Dampak yang dimaksud tidak hanya terbatas ruang lingkup layanan pemerintah, namun juga kepada masyarakat umum, lembaga lain dan bahkan terhadap sistem pemerintahan berbasis elektronik di lingkup Pemerintah Kota Madiun.

Mengingat pentingnya informasi, maka informasi harus dilindungi atau diamankan oleh seluruh pegawai Pemerintah Daerah. Pengamanan informasi sangat bergantung pada pengamanan terhadap semua aspek dan komponen TIK terkait, seperti Perangkat Lunak, Perangkat Keras, jaringan, peralatan pendukung (misalnya sumber daya listrik, AC) dan sumber daya manusia (termasuk kualifikasi dan keterampilan).

Pemerintah Daerah beroperasi pada lingkungan bisnis dimana terdapat ketergantungan yang tinggi pada Sistem Informasi dan jaringan komputer yang saling berhubungan. Dalam lingkungan seperti ini, terdapat berbagai risiko yang mengancam terjaganya kerahasiaan, integritas dan ketersediaan informasi. Beberapa ancaman yang berpotensi seperti di bawah ini:

- kebocoran data;
- sabotase;
- vandalisme;
- *virus, malware* dan *phishing*;
- *hacking*;
- *spoofing*;
- *ransomware* dan sebagainya.

Dewasa ini, ancaman-ancaman tersebut semakin meningkat seiring dengan berkembangnya layanan dan produk elektronik serta layanan *online*. Peningkatan layanan Pemerintah Daerah yang cepat juga meningkatkan kerentanan terhadap informasi milik Instansi Pemerintah Daerah. Oleh karena itu aset-aset informasi yang penting milik Pemerintah Daerah dipastikan sudah terlindungi dengan baik.

Kebijakan dan standar SMKI digunakan sebagai acuan dalam rangka melindungi Aset Informasi Pemerintah Daerah dari berbagai bentuk ancaman baik dari dalam maupun dari luar, yang dilakukan secara sengaja maupun tidak sengaja. Pengamanan dan perlindungan ini diberikan untuk menjamin (3) tiga komponen utama yang menjadi dasar keamanan informasi, yaitu aspek kerahasiaan (*Confidentiality*), keutuhan (*Integrity*), dan ketersediaan (*Availability*) atau CIA pada Aset Informasi agar selalu terjaga dan terpelihara dengan baik.

Komponen	Deskripsi
<i>Confidentiality</i>	Berkaitan dengan kerahasiaan informasi agar informasi penting milik Pemerintah Daerah tidak terungkap kepada pihak yang tidak berwenang
<i>Integrity</i>	Berkaitan dengan kebenaran, akurasi dan kelengkapan informasi
<i>Availability</i>	Berkaitan dengan aspek ketersediaan informasi, agar informasi yang penting bagi berlangsungnya proses bisnis selalu tersedia setiap saat dibutuhkan

Informasi yang berada dalam berbagai bentuk (tersimpan pada sistem komputer, ditransmisikan melalui jaringan komunikasi, tercetak dalam bentuk *hardcopy* atau diucapkan dalam pembicaraan), harus diamankan dengan cara yang tepat agar ketiga aspek CIA tersebut selalu terjaga.

B. TUJUAN

Kebijakan dan Standar SMKI menyatakan komitmen dan arahan Manajemen untuk melaksanakan prinsip-prinsip keamanan informasi. Kebijakan dan Standar SMKI disusun dengan tujuan agar manajemen dapat:

- a. memastikan terpeliharanya kerahasiaan, integritas dan ketersediaan informasi Pemerintah Daerah, serta seluruh sistem sumber daya informasi;
- b. membangun pengamanan untuk melindungi Aset Informasi milik Pemerintah Daerah dari ancaman pencurian, penyalahgunaan, atau kerusakan;
- c. memastikan terlaksananya prinsip *non-repudiation* atas pihak-pihak yang terlibat dalam proses bisnis Pemerintah Daerah;
- d. menetapkan tanggung jawab dan akuntabilitas penggunaan dalam mengakses informasi milik Pemerintah Daerah;

- e. memastikan terpenuhinya kepatuhan terhadap hukum, undang-undang, dan peraturan eksternal yang berlaku;
- f. memastikan kemampuan Pemerintah Daerah untuk melanjutkan aktivitasnya dalam hal terjadi insiden Keamanan Informasi yang signifikan atau ancaman terhadap Sistem Informasi Pemerintah Daerah;
- g. mendorong manajemen dan seluruh pegawai Pemerintah Daerah untuk memiliki tingkat kesadaran (*awareness*), pengetahuan dan keterampilan yang memadai agar dapat memenuhi kewajiban mereka dalam menjaga keamanan Aset Informasi;
- h. memiliki sumber daya yang memadai untuk melaksanakan program Keamanan Informasi yang efektif; dan
- i. memastikan konsistensi dalam menerapkan Keamanan Informasi.

C. RUANG LINGKUP

Kebijakan dan standar SMKI ini berlaku untuk seluruh pegawai Pemerintah Daerah dan pegawai pihak ketiga (pegawai dari pihak *vendor*, konsultan atau tenaga kerja kontrak) untuk pengelolaan pengamanan seluruh Aset Informasi Pemerintah Daerah dan dilaksanakan oleh pegawai Pemerintah Daerah dan seluruh pihak yang terikat kontrak kerja sama dengan Pemerintah Daerah meliputi:

- a. Organisasi dan lokasi: meliputi seluruh unit kerja Pemerintah Daerah serta pihak eksternal lainnya yang menyediakan dan atau mendukung layanan Teknologi Informasi Pemerintah Daerah.
- b. Informasi: mencakup semua jenis informasi yang dihasilkan atau diterima Pemerintah Daerah, tersimpan dalam media elektronik yang dikelola dengan Teknologi Informasi, dan informasi lainnya yang berhubungan dengan Sistem Informasi yang digunakan oleh Pemerintah Daerah, termasuk namun tidak terbatas pada dokumen mengenai topologi jaringan, data pegawai, surat-surat internal, laporan-laporan internal dan lain-lain.
- c. Bisnis Proses: mencakup bisnis proses Keamanan TI, Perencanaan TI, Penanganan Keluhan TI, Pengembangan Aplikasi Inti, Pengembangan Aplikasi Pendukung, Pengembangan Data Manajemen, *Quality Assurance*, Manajemen Basis Data, Layanan TI, DC, Jaringan dan Infrastruktur.

Ruang lingkup kebijakan dan standar SMKI tersebut dijabarkan secara rinci yang meliputi:

1. Pengendalian Umum

2. Pengendalian Organisasi Keamanan Informasi
3. Keamanan Sumber Daya Manusia
4. Pengendalian Pengelolaan Aset Informasi
5. Pengendalian Akses
6. Pengendalian Terhadap Penerapan Kriptografi
7. Pengendalian Pengelolaan Keamanan Fisik dan Lingkungan
8. Pengendalian Pengelolaan Keamanan Operasional
9. Pengendalian Keamanan Komunikasi
10. Pengendalian Keamanan Informasi Dalam Akuisisi, Pengembangan dan Pemeliharaan Sistem Informasi
11. Pengendalian Hubungan Dengan Pihak Ketiga Atau Penyedia Jasa/Barang
12. Pengendalian Pengelolaan Gangguan Keamanan Informasi
13. Pengendalian Aspek Keamanan Informasi Dalam Pengelolaan Kelangsungan Kegiatan
14. Pengendalian Kepatuhan

BAB II

PENGENDALIAN UMUM

A. TUJUAN

Kebijakan dan standar SMKI disusun dengan tujuan memberikan pedoman umum untuk seluruh Perangkat Daerah di lingkungan Pemerintah Daerah dalam hal mengelola kebijakan dan standar SMKI secara terpadu, sehingga Aset Informasi yang dimiliki setiap Perangkat Daerah dapat terlindungi baik 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 dan harus dilaksanakan oleh seluruh unit kerja, seluruh pegawai, baik sebagai Pengguna maupun pengelola TIK, dan pihak ketiga di lingkungan Pemerintah Daerah.
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, 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 meliputi pengetahuan, pengalaman, keahlian, citra dan reputasi.

C. KEBIJAKAN

1. Perangkat Daerah bertanggung jawab untuk mengidentifikasi 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. Pimpinan 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. Pimpinan 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 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;
 - 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 sebagai berikut:
 - a. Pimpinan perangkat daerah harus memastikan terdokumentasinya catatan penerapan kebijakan dan Standar SMKI di lingkungan kerjanya, sehingga kepatuhan dan efektivitas penerapan SMKI dapat diukur.
 - b. Catatan penerapan kebijakan dan standar SMKI di setiap Perangkat Daerah 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;
4. Dokumen pendukung kebijakan keamanan informasi 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;
 - 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 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 tidakberwenang; 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 1 (satu) kali dalam 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;
 - c. evaluasi terhadap pencapaian persyaratan dan kebutuhan persyaratan dan kebutuhan keamanan informasi dari pihak-pihak yang berkepentingan terhadap Keamanan Informasi di lingkungan Dinas Komunikasi dan Informatika di Daerah;
 - d. evaluasi terhadap umpan balik dari pihak-pihak di luar Dinas Komunikasi dan Informatika di Daerah;
 - 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*;
 - 4) pengkajian *Security Improvement Program* 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-lain;
 - 3) hasil audit internal dan/atau eksternal;
 - 4) hasil tinjauan manajemen;

- 5) hasil ketidaksesuaian dari inspeksi atau temuan dari *stakeholders* lain.

BAB III

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
 - a. struktur Tim Keamanan Informasi setiap perangkat daerah berikut tanggung jawab dan wewenangnya diuraikan dalam standar organisasi keamanan informasi.
 - b. 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.
2. Perjanjian Kerahasiaan

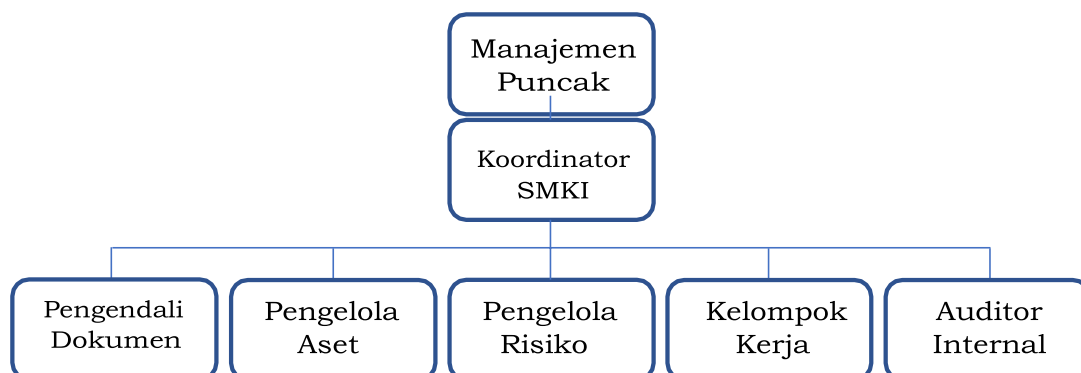
Setiap Pimpinan Perangkat Daerah mengidentifikasi dan mengkaji secara berkala persyaratan untuk menjaga kerahasiaan Aset Informasi yang dituangkan dalam dokumen Perjanjian Kerahasiaan.
3. Pemisahan tugas

Setiap Pimpinan 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.

4. Hubungan dengan Pihak Berwenang
 - a. Setiap Pimpinan Perangkat Daerah mengidentifikasi dan menjalin kerja sama dengan pihak-pihak berwenang di luar perangkat daerah yang terkait dengan Keamanan Informasi.
 - b. Setiap Pimpinan Perangkat Daerah menjalin kerja sama dengan komunitas Keamanan Informasi di luar Pimpinan Perangkat Daerah melalui pelatihan, seminar, atau forum lain yang relevan dengan Keamanan Informasi.
 - c. Hubungan dengan pihak ketiga.
5. Keamanan Informasi pada pengelolaan proyek
Pengendalian terhadap Keamanan Informasi harus diterapkan dalam pengelolaan proyek dan harus diaplikasikan pada seluruh fase dalam metodologi pengelolaan proyek.
6. Pengendalian terhadap *mobile device* dan *teleworking*
 - a. setiap Pimpinan 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 mengomunikasikan kepada seluruh pegawai;
- b. melakukan koordinasi antar Subbagian tentang pelaksanaan pengelolaan keamanan informasi.
- c. melakukan evaluasi terhadap hasil penetapan mitigasi risiko;
- d. memantau pelaksanaan perbaikan SMKI;
- e. memberikan laporan kepada Pimpinan 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 SMKI, 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, 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 SMKI
- a. melakukan monitoring pelaksanaan SMKI di masing-masing subbagian;
 - b. memastikan bahwa semua prosedur, instruksi kerja dan formulir dapat digunakan dan diterapkan di subbagian terkait untuk mengurangi terjadinya kesalahan dalam penerapan sistem manajemen;
 - c. memantau pengukuran sasaran implementasi SMKI pada masing-masing subbagian; 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 SMKI
- a. melaksanakan audit internal dengan subbagian terkait sesuai jadwal yang ditetapkan;
 - b. mengoordinasikan 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. penandatanganan untuk menghindari pengungkapan informasi secara tidak sah;
- e. perlindungan kepemilikan informasi, rahasia organisasi, dan kekayaan intelektual;
- f. izin menggunakan informasi rahasia, dan hak-hak penandatanganan 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 IV

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 ketentuan 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. Pimpinan Perangkat Daerah akan melakukan pemeriksaan data pribadi yang diberikan oleh pegawai dan pihak ketiga sesuai dengan ketentuan peraturan perundang-undangan.
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.
7. Seluruh pegawai dan pihak ketiga yang melanggar Kebijakan dan Standar SMKI di Lingkungan Dinas Komunikasi dan Informatika akan dikenai sanksi atau tindakan disiplin sesuai ketentuan peraturan perundang-undangan.

8. 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.
9. Pimpinan 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.
10. Pimpinan 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 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 V

PENGENDALIAN PENGELOLAAN ASET INFORMASI

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. Pimpinan 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. Pimpinan Perangkat Daerah menetapkan Pemilik Aset Informasi;
 - c. Pimpinan 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; 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
Pimpinan Perangkat Daerah perlu menyusun dan menetapkan peraturan atau prosedur terkait penanganan Aset Informasi sesuai dengan klasifikasi informasi yang telah ditetapkan.
 4. Penanganan *Media Removable*
Pimpinan 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 berlaku di Perangkat Daerah yang bersangkutan.
 6. Pertukaran Media Informasi secara Fisik
Pimpinan 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

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 (<i>Strictly Confidential</i>)	Informasi yang apabila didistribusikan secara tidak sah atau jatuh ke tangan yang tidak berhak akan menyebabkan kerugian negara.
Rahasia (<i>onfidential</i>)	Informasi yang apabila secara tidak sah atau jatuh ke tangan yang tidak berhak akan mengganggu citra dan reputasi yang menurut ketentuan peraturan perundang-undangan dinyatakan rahasia.
Terbatas (<i>Internal</i>)	Informasi yang apabila didistribusikan secara tidak sah atau jatuh ke tangan yang tidak berhak akan mengganggu citra dan reputasi.
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 lainnya yang sesuai dengan undang-undang serta informasi lain yang berkaitan dengan kepentingan publik.

BAB VI

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) Pimpinan 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
Pimpinan 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.
 - c. Pengguna harus melindungi informasi agar tidak diakses oleh pihak yang tidak berwenang.
4. Pengendalian Akses Jaringan
 - a. penggunaan layanan jaringan
 - 1) setiap Pimpinan Perangkat Daerah harus mengatur akses Pengguna dalam mengakses jaringan yang digunakan pada Perangkat Daerah yang bersangkutan sesuai dengan peruntukannya; dan
 - 2) setiap Pimpinan 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.
 - 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 sistem; 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
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 memiliki 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*
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. Pimpinan Perangkat Daerah harus memastikan bahwa akses terhadap aplikasi dan sistem informasi hanya diberikan kepada pengguna sesuai peruntukannya.
 - 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 hanyadiperbolehkan 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 secara berkala dan untuk Pengguna yang memiliki lebih dari 1 (satu) akun; dan
- i. pemastian bahwa Akun tidak digunakan oleh Pengguna lain.

3. Pengelolaan Hak Akses Khusus

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, aplikasi;
- b. Hak Akses Khusus hanya diberikan kepada Pengguna sesuai dengan peruntukannya 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 VII

PENGENDALIAN TERHADAP PENERAPAN KRIPTOGRAFI

A. TUJUAN

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

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; dan
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, 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 VIII

PENGENDALIAN PENGELOLAAN KEAMANAN FISIK DAN LINGKUNGAN

A. TUJUAN

Keamanan fisik dan lingkungan bertujuan untuk mencegah akses fisik oleh pihak yang tidak berwenang, 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;
 - 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 TI yang tidak berada dalam pengawasan memiliki perlindungan 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*) 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.
- 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;
- b. Fasilitas Utama harus ditempatkan khusus untuk menghindari akses publik;
- c. pembatasan pemberian identitas atau tanda-tanda keberadaan aktivitas pengolahan informasi; dan
- d. Direktori dan buku telepon internal yang mengidentifikasi lokasi perangkat pengolah informasi tidak mudah diakses oleh publik.

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) menggunakan *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 IX

PENGENDALIAN PENGELOLAAN 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 sistem;
3. perlindungan terhadap Ancaman Program yang membahayakan;
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
Pimpinan 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
Pimpinan 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
Pimpinan 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) pimpinan 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) pimpinan Perangkat Daerah harus menetapkan kriteria penerimaan 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 Ancaman Program yang membahayakan
- a. setiap Perangkat Daerah harus menerapkan sistem yang dapat melakukan pendeteksian, pencegahan, dan pemulihan sebagai bentuk perlindungan terhadap ancaman program yang membahayakan.
 - b. perlindungan terhadap ancaman program yang membahayakan 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 Pusat Data 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.
6. *Logging* dan *Monitoring*
 - a. *event logging*

Setiap Perangkat Daerah harus mengaktifkan dan secara rutin *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* tercatat di dalam *log*.
 - e. pencatatan kesalahan
Setiap Perangkat Daerah harus menerapkan pencatatan kesalahan 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 mencakup:

- 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 saat terjadi kegagalan sistem;
- d. tata cara *backup* dan *restore*; dan
- e. tata cara pengelolaan Jejak Audit 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 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 pengolahan informasi ditetapkan untuk menjamin agar kegiatan akses yang tidak sah tidak perlu terjadi. Prosedur ini mencakup *monitoring*:

- a. kegagalan akses;
- b. pola-pola *log-on* yang mengindikasikan penggunaan yang tidak wajar;
- c. alokasi dan penggunaan Hak Akses khusus;
- 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 mencakup:

- 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 X

PENGENDALIAN 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 mencakup:

- 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 mencakup.
 - 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 mencakup:
 - 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 Informasi

- a. prosedur pertukaran informasi bila menggunakan perangkat komunikasi elektronik, mencakup:
 - 1) Perlindungan pertukaran informasi dari pencegahan, penyalinan, modifikasi, *miss-routing*, dan kerusakan;
 - 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.
- c. pengendalian pertukaran informasi bila menggunakan perangkat komunikasi elektronik, mencakup:
 - 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;
 - 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.

BAB XI

PENGENDALIAN KEAMANAN INFORMASI DALAM 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; dan
3. keamanan *system files*.

C. KEBIJAKAN

1. Persyaratan keamanan pada Sistem Informasi mencakup setidaknya hal-hal berikut ini:
 - a. pimpinan Perangkat Daerah menetapkan dan mendokumentasikan secara jelas persyaratan Keamanan Informasi yang relevan sebelum pengadaan, pengembangan, atau pemeliharaan Sistem Informasi baru.
 - b. Pengolahan Informasi pada Aplikasi, mencakup:
 - 1) validasi Data yang masuk
Data yang akan dimasukkan ke aplikasi harus diperiksa terlebih dahulu kebenaran dan kesesuaiannya.
 - 2) pengendalian proses internal
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 proses*)
 - 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
Pimpinan 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 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 dan 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 mencakup:
 - 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 sistem;
 - 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 sistem 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 process*)
 - a. prosedur pengendalian perubahan sistem operasi dan perangkat lunak, mencakup:
 - 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 mengganggu kegiatan.
 - b. prosedur kajian teknis aplikasi setelah perubahan sistem operasi dan/atau Perangkat Lunak, mencakup:
 - 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; 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;
- 2) perjanjian *escrow* (jaminan pelaksanaan);
- 3) hak untuk melakukan audit terhadap kualitas dan akurasi pekerjaan;
- 4) persyaratan perjanjian kualitas dan fungsi keamanan aplikasi; dan
- 5) uji coba terhadap aplikasi untuk memastikan tidak terdapat *malicious code* sebelum implementasi.

BAB XII

PENGENDALIAN HUBUNGAN DENGAN PIHAK KETIGA ATAU PENYEDIA JASA/BARANG

A. TUJUAN

Pengelolaan hubungan dengan pihak ketiga atau penyedia jasa/barang bertujuan untuk memastikan terlindunginya 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. Pimpinan 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. Pimpinan 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. Pimpinan Perangkat Daerah harus memastikan terdapat persyaratan untuk mengatasi risiko keamanan informasi pada kesepakatan dengan pihak ketiga atau penyedia jasa/barang yang berhubungan dengan layanan TIK serta rantai pasokan produk.

4. Pimpinan 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. Pimpinan 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 XIII

PENGENDALIAN PENGELOLAAN GANGGUAN 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
Pimpinan Perangkat Daerah perlu melakukan pengkajian terhadap kejadian keamanan informasi serta memutuskan dari hasil kajian apakah kejadian tersebut tergolong ke dalam gangguan keamanan informasi.
- e. Pimpinan Perangkat Daerah harus memastikan bahwa seluruh gangguan keamanan informasi yang terjadi ditanggapi sesuai dengan prosedur formal penanganan gangguan keamanan informasi.

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 di luar 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 mencakup:
 - 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.

- 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;
 - 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 mencakup:
 - 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 perjanjian atau peraturan atau persyaratan dalam hal proses pidana atau perdata.
 - 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 bahwa:

- 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.
- 4) keutuhan sistem dan pengendaliannya dikonfirmasi dengan pihak-pihak terkait sesegera mungkin.

BAB XIV
PENGENDALIAN ASPEK KEAMANAN INFORMASI DALAM PENGELOLAAN
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*);
3. penyusunan dan penerapan rencana kelangsungan kegiatan (*business continuity plan*).
4. pengujian, pemeliharaan, dan pengkajian ulang rencana kelangsungan kegiatan.
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 (*redundancy*) 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 Pimpinan 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 mencakup:
 - 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*), yaitu tindakan mengembalikan kegiatan operasional ke kondisi normal;
 - d. jadwal uji coba, mencakup langkah-langkah dan waktu pelaksanaan uji coba serta proses pemeliharannya;
 - 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.
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 mencakup:
- 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 XV

PENGENDALIAN KEPATUHAN

A. TUJUAN

Pengendalian kepatuhan bertujuan untuk menghindari pelanggaran terhadap ketentuan peraturan perundang-undangan yang terkait Keamanan Informasi.

B. RUANG LINGKUP

Kebijakan dan standar kepatuhan ini meliputi:

1. kepatuhan terhadap ketentuan peraturan perundang-undangan yang terkait Keamanan Informasi;
2. kepatuhan teknis; dan
3. audit Sistem Informasi.

C. KEBIJAKAN

1. Kepatuhan terhadap ketentuan peraturan perundang-undangan yang terkait Keamanan Informasi
 - a. seluruh pegawai dan pihak ketiga harus menaati ketentuan peraturan perundang-undangan yang terkait dengan Keamanan Informasi;
 - b. identifikasi ketentuan peraturan perundang-undangan yang dapat diterapkan setiap Perangkat Daerah harus mengidentifikasi, mendokumentasikan dan memelihara kemutakhiran semua ketentuan peraturan perundang-undangan 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
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 ketentuan peraturan perundang-undangan 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

Pimpinan 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 audit Sistem Informasi
penggunaan alat bantu (baik Perangkat Lunak maupun Perangkat Keras) untuk mengetahui kelemahan keamanan, memindai Kata Sandi, atau untuk melemahkan dan menerobos sistem keamanan informasi tidak diizinkan kecuali atas persetujuan Pimpinan Perangkat Daerah yang bersangkutan; dan

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 mencakup pengujian penetrasi 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 Pimpinan 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;
- 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, Data dan Sistem informasi sensitif harus mempertimbangkan pencatatan waktu pada Jejak Audit;
- h. semua prosedur, persyaratan, dan tanggung jawab harus didokumentasikan; dan
- i. auditor harus independen dari kegiatan yang diaudit.

WALI KOTA MADIUN,

ttd

Drs. H. MAIDI, SH, MM, M.Pd.

Salinan sesuai dengan aslinya
a.n. WALIKOTA MADIUN
Sekretaris Daerah
u.b.
Kepada Bagian Hukum



BUDI WIBOWO, SH
Pembina Tingkat I
NIP. 19750117 199602 1 001