SALINAN

BUPATI SUBANG

PROVINSI JAWA BARAT

PERATURAN BUPATI SUBANG

NOMOR 372 TAHUN 2022

TENTANG

KEBIJAKAN UMUM SISTEM MANAJEMEN KEAMANAN INFORMASI

DENGAN RAHMAT TUHAN YANG MAHA ESA,

BUPATI SUBANG,

Menimbang : a. bahwa untuk melindungi kerahasiaan, keutuhan dan ketersediaan aset informasi Pemerintah Daerah Kabupaten Subang dari berbagai bentuk gangguan serta ancaman keamanan informasi, perlu dilakukan pengelolaan keamanan informasi yang sesuai dengan SNI ISO/IEC 27001;

b. bahwa berdasarkan ketentuan 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 untuk mewujudkan pengelolaan keamanan informasi Pemerintah Daerah perlu dibuat Sistem Manajemen Keamanan Informasi;

c. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b, maka perlu menetapkan Peraturan Bupati Subang tentang Kebijakan Umum Sistem Manajemen Keamanan Informasi;

Mengingat : 1. Undang-Undang Nomor 14 Tahun 1950 tentang Pembentukan Daerah-Daerah Kabupaten Dalam Lingkungan Propinsi Djawa Barat (Berita Negara Republik Indonesia Tahun 1950), sebagaimana telah diubah dengan Undang-Undang Nomor 4 Tahun 1968 tentang Pembentukan Kabupaten Purwakarta dan Kabupaten Subang, dengan Mengubah Undang-Undang Nomor 14 Tahun 1950 tentang Pembentukan Daerah-Daerah Kabupaten Dalam Lingkungan Provinsi Jawa Barat (Lembaran Negara Republik Indonesia Tahun 1968 Nomor 31, Tambahan Lembaran Negara Republik Indonesia Nomor 2851);

2. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843), sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251, Tambahan Lembaran Negara Republik Indonesia Nomor 5952);
3. Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 61, Tambahan Lembaran Negara Republik Indonesia Nomor 4846);
4. Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 244, Tambahan Lembaran Negara Republik Indonesia Nomor 5887), sebagaimana telah diubah beberapa kali terakhir dengan Undang-Undang Nomor 11 Tahun 2020 tentang Cipta Kerja (Lembaran Negara Republik Indonesia Tahun 2020 Nomor 245, Tambahan Lembaran Negara Republik Indonesia Nomor 6573);
5. Peraturan Pemerintah Nomor 61 Tahun 2010 tentang Pelaksanaan Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (Lembaran Negara Republik Indonesia Tahun 2010 Nomor 99, Tambahan Lembaran Negara Republik Indonesia Nomor 5149);
6. Peraturan Pemerintah Nomor 18 Tahun 2016 tentang Perangkat Daerah (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 114, Tambahan Lembaran Negara Republik Indonesia Nomor 5887), sebagaimana telah diubah dengan Peraturan Pemerintah Nomor 72 Tahun 2019 tentang Perubahan Atas Peraturan Pemerintah Nomor 18 Tahun 2016 tentang Perangkat Daerah (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 187, Tambahan Lembaran Negara Republik Indonesia Nomor 6402);
7. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185, Tambahan Lembaran Negara Republik Indonesia Nomor 6400);
8. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);

9. Peraturan ...

9. Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian untuk Pengamanan Informasi di Pemerintah Daerah (Berita Negara Republik Indonesia Tahun 2019 Nomor 1054);
10. Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2020 tentang Sistem Pengamanan Dalam Penyelenggaraan Sistem Elektronik (Berita Negara Republik Indonesia Tahun 2020 Nomor 1375);
11. Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2021 Nomor 541);
12. Peraturan Daerah Kabupaten Subang Nomor 7 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Kabupaten Subang (Lembaran Daerah Kabupaten Subang Tahun 2016 Nomor 7), sebagaimana telah diubah beberapa kali terakhir dengan Peraturan Daerah Kabupaten Subang Nomor 1 Tahun 2021 tentang Perubahan Ketiga Atas Peraturan Daerah Kabupaten Subang Nomor 7 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Kabupaten Subang (Lembaran Daerah Kabupaten Subang Tahun 2021 Nomor 1);
13. Peraturan Bupati Subang Nomor 120 Tahun 2019 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik (Berita Daerah Kabupaten Subang Tahun 2019 Nomor 120);
14. Peraturan Bupati Subang Nomor 101 Tahun 2021 tentang Susunan Organisasi Perangkat Daerah Dinas (Berita Daerah Kabupaten Subang tahun 2021 Nomor 101);
15. Peraturan Bupati Subang Nomor 11 Tahun 2022 tentang Tugas Pokok, Fungsi, dan Tata Kerja Dinas Komunikasi dan Informatika Kabupaten Subang (Berita Daerah Kabupaten Subang Tahun 2022 Nomor 11);

MEMUTUSKAN :

Menetapkan : PERATURAN BUPATI SUBANG TENTANG KEBIJAKAN UMUM SISTEM MANAJEMEN KEAMANAN INFORMASI.

BAB I ...

BAB I

KETENTUAN UMUM

Pasal 1

Dalam Peraturan Bupati ini yang dimaksud dengan :

1. Daerah Kabupaten adalah Daerah Kabupaten Subang.
2. Pemerintah Daerah adalah kepala daerah sebagai unsur penyelenggara Pemerintahan Daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan daerah otonom.
3. Bupati adalah Bupati Subang.
4. Wakil Bupati adalah Wakil Bupati Subang.
5. Perangkat Daerah adalah unsur pembantu kepala daerah dan Dewan Perwakilan Rakyat Daerah dalam penyelenggaraan Urusan Pemerintahan yang menjadi kewenangan Daerah.
6. Dinas adalah Dinas Komunikasi dan Informatika yang melaksanakan urusan pemerintahan di bidang komunikasi dan informatika, statistik, dan persandian.
7. Aparatur Sipil Negara yang selanjutnya disingkat ASN adalah Aparatur Sipil Negara di lingkungan Pemerintah Daerah Kabupaten Subang.
8. Informasi adalah keterangan, pernyataan, gagasan, dan tanda-tanda yang mengandung nilai, makna, dan pesan, baik kata, fakta, maupun penjelasan yang dapat dilihat, didengar, dan dibaca yang disajikan dalam berbagai kemasan dan format sesuai dengan perkembangan teknologi dan komunikasi secara elektronik maupun nonelektronik.
9. Teknologi Informasi adalah suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan/atau menyebarkan informasi.
10. Keamanan Informasi adalah terjaganya kerahasiaan, keaslian, keutuhan, ketersediaan, dan kenirsangkalan informasi.
11. Sistem Manajemen Keamanan Informasi yang selanjutnya disingkat SMKI adalah bagian dari sistem manajemen secara keseluruhan, berdasarkan pendekatan risiko bisnis untuk menetapkan, menerapkan, mengoperasikan, memantau, mengkaji, meningkatkan, dan memelihara keamanan informasi.
12. Aset Informasi adalah unit informasi yang dapat dipahami, dibagi, dilindungi dan dimanfaatkan secara efektif.

13. Aset ...

13. Aset Pengolahan Informasi adalah suatu perangkat baik elektronik maupun nonelektronik yang dapat digunakan untuk membuat dan menyunting informasi.
14. Penyimpanan Informasi adalah suatu proses menyimpan informasi dengan menggunakan media, baik elektronik maupun nonelektronik.
15. Perangkat keras adalah semua jenis piranti atau komponen komputer yang bagian fisiknya dapat dilihat secara kasat mata dan dirasakan langsung.
16. Komputer adalah alat untuk memproses data elektronik, mengetik, optik, atau sistem yang melaksanakan fungsi logika, aritmatika, dan menyimpan.
17. Perangkat lunak adalah satu atau sekumpulan program komputer, prosedur, dan/atau dokumentasi yang terkait dalam pengoperasian sistem elektronik.
18. Perangkat lunak sistem adalah jenis perangkat lunak yang digunakan untuk menjalankan atau mengoperasikan perangkat perangkat keras, diantaranya yaitu sistem operasi, pemroses bahasa, dan driver.
19. Perangkat lunak aplikasi adalah jenis perangkat lunak yang dirancang untuk mencapai kebutuhan pengguna tertentu, diantaranya yaitu pengolah kata, *spreadsheet*, dan *web browser*.
20. Data Center atau Pusat Data adalah suatu fasilitas untuk menempatkan sistem komputer dan perangkat-perangkat terkait, seperti sistem komunikasi data dan penyimpanan data.

BAB II

MAKSUD DAN TUJUAN

Pasal 2

(1) Maksud ditetapkannya Peraturan Bupati ini adalah untuk terciptanya sistem pengendalian keamaman yang terpadu dan menjamin keberlangsungan Sistem Manajemen Keamanan Informasi Pemerintahan Berbasis Elektronik dengan meminimalkan dampak risiko Keamanan Informasi.

(2) Tujuan ditetapkannya Peraturan Bupati ini adalah untuk :

a. memberikan landasan hukum dalam penerapan Sistem Manajemen Keamanan Informasi Pemerintahan Berbasis Elektronik di lingkungan Pemerintah Daerah.

b. memberikan ...

b. memberikan pedoman dalam hal pengelolaan Sistem Manajemen Keamanan Informasi secara terpadu untuk memastikan terjaganya kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*).

BAB III

PENGAMANAN INFORMASI

Pasal 3

Pengamanan informasi yang diatur dalam Peraturan Bupati ini meliputi:

a. aset informasi;

b. aset pengelolaan 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 di atas kertas, papan tulis, spanduk, atau di dalam buku dan dokumen; dan

b. elektronik, meliputi informasi tercetak, tertulis dan tersimpan dalam bentuk elektronik seperti *database*, pada *file* di dalam komputer, ditampilkan pada *website*, layar komputer dan dikirimkan melalui jaringan telekomunikasi.

Pasal 5

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

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

b. peralatan elektronik yang bekerja secara elektronik penuh.

Pasal 6

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

a. elektronik, meliputi antara lain server dan media penyimpanan; dan

b. nonelektronik ...

b. nonelektronik, meliputi antara lain lemari, rak, laci, *filling cabinet*, dan perlengkapan kantor lainnya.

BAB IV

SUMBER DAYA

Pasal 7

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

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

BAB V

STANDAR DAN PROSEDUR PENGENDALIAN DAN PENANGGUNG JAWAB

Pasal 8

(1) Setiap Perangkat Daerah wajib menyusun standar dan prosedur pengendalian kegiatan Teknologi Informasi yang memenuhi prasyarat Keamanan Informasi.

(2) Prasyarat Keamanan Informasi sebagaimana dimaksud pada ayat (1) digunakan untuk mengimplementasikan tindakan dalam mengelola risiko yang meliputi aspek sebagai berikut:

a. keamanan sumber daya manusia;

b. pengelolaan aset;

c. pengendalian akses;

d. kriptografi;

e. keamanan fisik dan lingkungan;

f. keamanan operasional;

g. keamanan komunikasi;

h. keamanan dalam proses akuisisi, pengembangan dan pemeliharaan sistem Informasi;

i. hubungan kerja dengan pemasok (supplier);

j. penanganan insiden Keamanan Informasi;

k. kelangsungan usaha; dan

l. kepatuhan.

Pasal 9 ...

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 penyelenggara Teknologi Informasi wajib mengidentifikasi dan memantau aktivitas operasional Teknologi Informasi untuk memastikan efektivitas, efesiensi, dan keamanan dari aktivitas tersebut antara lain dengan:

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

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

c. menerapkan pengendalian terhadap Informasi yang diproses;

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

e. melakukan pemantauan kegiatan operasional Teknologi Informasi termasuk *audit trail*/riwayat; dan

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

BAB VI

MANAJEMEN RISIKO

Pasal 10

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

(2) Proses manajemen risiko sebagaimana dimaksud pada ayat (1) meliputi:

a. identifikasi;

b. pengukuran;

c. pemantauan; dan

d. pengendalian atas risiko terkait penggunaan Teknologi Informasi.

(3) Manajemen ...

(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 disetiap penggunaan operasional Teknologi Informasi pada sistem yang digunakan.

BAB VII

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 Data Center baik dikelola oleh internal maupun oleh pihak penyedia jasa.

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

Pasal 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 dibawah tanggung jawabnya meliputi:

a. kegiatan pemantauan secara terus menerus; dan

b. pelaksanaan fungsi pemeriksaan internal yang efektif dan menyeluruh.

(3) Perangkat ...

(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 Dinas dan didokumentasikan.

Pasal 13

(1) Apabila terjadi kebocoran Informasi yang mempunyai dampak luas pada Perangkat Daerah terkait, maka Pemerintah Daerah dapat menunjuk auditor independen untuk melakukan investigasi yang diperlukan.

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

BAB VIII ...

BAB VIII

KETENTUAN PENUTUP

Pasal 14

Peraturan Bupati ini mulai berlaku pada tanggal diundangkan.

Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Bupati ini dengan penempatannya dalam Berita Daerah Kabupaten Subang.

Ditetapkan di Subang
pada tanggal 25 Oktober 2022

BUPATI SUBANG,

ttd.

RUHIMAT

Diundangkan di Subang
pada tanggal 25 Oktober 2022

SEKRETARIS DAERAH KABUPATEN SUBANG,

ttd.

ASEP NURONI

BERITA DAERAH KABUPATEN SUBANG TAHUN 2022 NOMOR 372

Salinan sesuai dengan aslinya
KEPALA BAGIAN HUKUM,

YOYON KARYONO, SH., M.H.
Pembina Tk. I (IV/b)
NIP. 19680416 200212 1 003

LAMPIRAN
PERATURAN BUPATI SUBANG
NOMOR : 372
TANGGAL : 25 Oktober 2022
TENTANG KEBIJAKAN UMUM SISTEM MANAJEMEN KEAMANAN INFORMASI.

KEBIJAKAN UMUM
SISTEM MANAJEMEN KEAMANAN INFORMASI

Versi 1.0

PEMERINTAH DAERAH KABUPATEN SUBANG
2022

BAB I
PENDAHULUAN

A. Tujuan

Kebijakan Umum Sistem Manajemen Keamanan Informasi disusun sebagai pedoman atau panduan umum untuk seluruh Perangkat Daerah di lingkungan Pemerintah Daerah Kabupaten Subang dalam hal mengelola kebijakan dan standar sistem manajemen keamanan informasi secara terpadu, sehingga Aset Informasi yang dimiliki setiap Perangkat Daerah dapat terlindungi dari aspek kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*).

B. Ruang Lingkup

Adapun ruang lingkup yang dimaksud, yaitu:

1. Ruang lingkup kebijakan ini adalah seluruh Aset Informasi dan aset pemrosesan Informasi yang berada dibawah pengelolaan Data Center Pemerintah Daerah, beserta Perangkat Daerah pemilik aset terkait.
2. Kebijakan dan standar ini berlaku untuk pengelolaan pengamanan seluruh aset informasi di setiap Perangkat Daerah di lingkungan Pemerintah Daerah Kabupaten Subang dan dilaksanakan oleh seluruh unit kerja, seluruh pegawai, baik sebagai pengguna maupun pengelola Teknologi Informasi dan Komunikasi, dan pihak ketiga di lingkungan Pemerintah Daerah Kabupaten Subang.
3. Aset Informasi adalah aset dalam bentuk:
   3.1 fisik, meliputi Informasi yang tercetak, tertulis dan tersimpan dalam bentuk fisik seperti di atas kertas, papan tulis, spanduk, atau di dalam buku dan dokumen; dan
   3.2 elektronik, meliputi Informasi tercetak, tertulis dan tersimpan dalam bentuk elektronik seperti *database*, pada file di dalam komputer, ditampilkan pada website, layar komputer dan dikirimkan melalui jaringan telekomunikasi.

C. Kebijakan

1. Perangkat Daerah berkomitmen untuk mengembangkan, mengimplementasikan, memelihara dan meningkatkan SMKI secara berkesinambungan untuk menjamin Keamanan Informasi Perangkat Daerah dari risiko Keamanan Informasi, baik dari pihak internal maupun eksternal.
2. Seluruh Informasi dalam bentuk fisik maupun elektronik, yang dikomunikasikan langsung atau melalui teknologi komunikasi harus dilindungi dari kemungkinan kerusakan, kesalahan penggunaan baik secara sengaja atau tidak, dicegah dari akses oleh pengguna yang tidak berwenang dan dari ancaman terhadap kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*).
3. Perangkat Daerah bertanggung jawab untuk mengidentifikasikan persyaratan dan kebutuhan keamanan informasi dari pihak-pihak yang berkepentingan terhadap Keamanan Informasi di lingkungan kerjanya.

4. Perangkat Daerah berkomitmen untuk mendukung pemenuhan prasyarat internal maupun eksternal Keamanan Informasi Perangkat Daerah yang relevan.
5. Perangkat Daerah berkomitmen untuk mematuhi seluruh peraturan perundang-undangan, regulasi dan kewajiban kontrak yang relevan.
6. Perangkat Daerah berkomitmen untuk memastikan ketersediaan dari sumber daya yang dibutuhkan oleh SMKI di Perangkat Daerah untuk menjamin terciptanya SMKI yang efektif dan efisien.
7. Kontrol Keamanan Informasi beserta sasaran masing-masing kontrol ditetapkan oleh Kepala Perangkat Daerah secara tahunan, didasarkan atas hasil identifikasi dan analisis risiko yang sesuai dengan ruang lingkup kebijakan SMKI, serta prioritisasi dengan mempertimbangkan ketersediaan dan kemampuan sumber daya.
8. Kebijakan Keamanan Informasi harus dikomunikasikan ke seluruh pegawai dan pihak ketiga terkait melalui media komunikasi yang ada agar dipahami dengan mudah dan dipatuhi.
9. Perangkat Daerah berkomitmen meningkatkan kepedulian (*awareness*), pengetahuan dan keterampilan tentang Keamanan Informasi bagi pegawai, serta mitra pihak ketiga lain sejauh diperlukan.
10. Seluruh kelemahan keamanan informasi yang berpotensi atau telah mengakibatkan gangguan penggunaan TIK atau gangguan Keamanan Informasi harus segera dilaporkan kepada penanggung jawab TIK terkait.
11. 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.
12. 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.
13. Kepala Perangkat Daerah secara berkala melakukan evaluasi terhadap kepatuhan dan keefektifan pelaksanaan SMKI serta melakukan tindak lanjut yang diperlukan untuk secara berkesinambungan meningkatkan kepatuhan dan keefektifan implementasi SMKI di lingkungan kerjanya.
14. Seluruh pimpinan di setiap Perangkat Daerah bertanggung jawab menjamin kebijakan ini diterapkan di bawah pengawasannya.
15. Seluruh pegawai bertanggung jawab untuk menjaga dan melindungi keamanan Aset Informasi serta mematuhi kebijakan dan prosedur Keamanan Informasi yang telah ditetapkan.
16. Setiap pelanggaran terhadap kebijakan ini dapat dikenai sanksi administratif sesuai ketentuan peraturan perundang-undangan.
17. Setiap pengecualian terhadap kebijakan ini dan standar dan prosedur pengendalian kegiatan Teknologi Informasi harus mendapat persetujuan dari Kepala Dinas.

18. Dokumen ini harus ditinjau paling sedikit 1 (satu) kali dalam 1(satu) tahun atau apabila terdapat perubahan signifikan dalam proses bisnis Perangkat Daerah untuk menjamin kesesuaian dan kecukupan dengan kondisi terkini.
19. Setiap perubahan terhadap dokumen ini harus didokumentasikan dan disetujui melalui proses manajemen perubahan.

BAB II
PEDOMAN PELAKSANAAN
SISTEM MANAJEMEN KEAMANAN INFORMASI

A. Tujuan

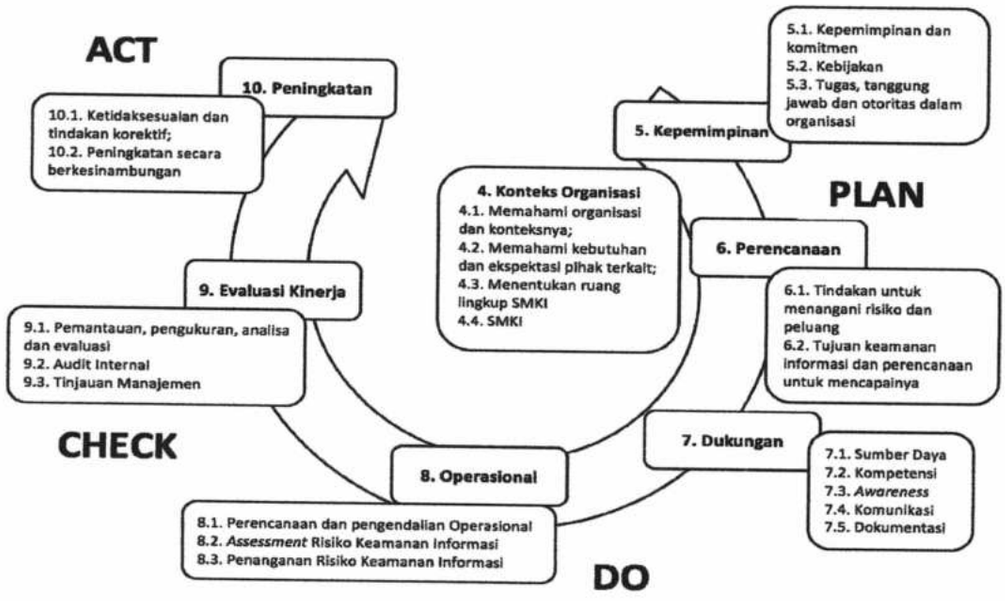
Tata kelola SMKI disusun dalam rangka untuk memastikan efektivitas dan efisiensi dari SMKI. Kerangka kerja ini akan menjabarkan proses-proses dan aktivitas-aktivitas yang harus dijalankan oleh Perangkat Daerah dalam rangka menetapkan, mengimplementasikan, memelihara SMKI dan meningkatkan secara berkesinambungan.

B. Ruang Lingkup

Pedoman pelaksanaan SMKI yang diatur dalam Peraturan Bupati ini merupakan acuan bagi seluruh Perangkat Daerah di lingkungan Pemerintah Daerah Kabupaten.

C. Kebijakan

1. Perangkat Daerah harus merencanakan suatu sistem manajemen Keamanan Informasi dengan mengadopsi siklus proses pada standard SNI ISO/IEC 27001:2013. Deskripsi umum tentang siklus proses berdasarkan arahan standar SNI ISO/IEC 27001:2013 dapat dilihat dari Gambar 2.1 sebagai berikut:



Gambar 2.1
Penggunaan siklus proses PDCA dalam proses SMKI

2. Proses perencanaan dalam pengembangan SMKI meliputi:
   2.1 Perangkat Daerah harus menentukan konteks dan ruang lingkup SMKI Perangkat Daerah dengan cara:

2.1.1 menentukan dan secara berkala meninjau faktor serta permasalahan internal dan eksternal yang dihadapi oleh Perangkat Daerah yang:

2.1.1.1 relevan dengan tujuan dari Perangkat Daerah dan SMKI; dan

2.1.1.2 mempengaruhi kemampuan Perangkat Daerah untuk mencapai tujuan SMKI yang diharapkan oleh Perangkat Daerah.

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

2.1.3 menentukan dan secara berkala meninjau kebutuhan dan ekspektasi terkait Keamanan Informasi dari pihak yang terkait tersebut;

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

2.1.5 menentukan dan secara berkala meninjau ruang lingkup dari SMKI di Perangkat Daerah.

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

2.2.1 memastikan bahwa SMKI mencapai tujuan yang diharapkan;

2.2.2 mencegah atau mengurangi dampak yang tidak diinginkan; dan

2.2.3 mencapai peningkatan yang berkesinambungan.

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

2.3.1 faktor dan permasalahan internal maupun eksternal yang dihadapi Perangkat Daerah; dan

2.3.2 ekspektasi Keamanan Informasi dari pihak terkait Perangkat Daerah.

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

3.1 menangani risiko dan peluang;

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

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

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

5. Seluruh manajemen risiko di Perangkat Daerah harus dilakukan paling tidak 1 (satu) kali dalam satu tahun atau apabila terdapat usulan atau telah terjadi perubahan yang relevan dan signifikan pada Perangkat Daerah. Seluruh catatan (*record*) terkait dengan seluruh proses manajemen risiko harus dibuat dan dipelihara.
6. Dalam proses pemilihan dari kontrol terhadap pengendalian risiko tersebut dilakukan pada saat aktifitas penanganan risiko yang merupakan bagian dari proses manajemen risiko.
7. Pemilihan dari kontrol tersebut dapat memperhatikan kontrol Keamanan Informasi berdasarkan standar SNI ISO/IEC 27001:2013 atau kontrol lainnya sesuai ketentuan peraturan perundang-undangan.
8. Dalam hal proses pendokumentasian SMKI perlu memperhatikan aspek sebagai berikut:
   8.1 Dokumentasi SMKI di Perangkat Daerah perlu mencakup Informasi terdokumentasi yang disyaratkan oleh SNI ISO/IEC 27001:2013 yang mencakup namun tidak terbatas pada:
      8.1.1 ruang lingkup SMKI;
      8.1.2 kebijakan dan tujuan Keamanan Informasi;
      8.1.3 metodologi *assessment* dan penanganan risiko;
      8.1.4 *Statement of Applicability* (SOA);
      8.1.5 rencana penanganan risiko;
      8.1.6 laporan *assessment* risiko;
      8.1.7 pendefinisian tugas dan tanggung jawab Keamanan Informasi;
      8.1.8 inventarisasi aset;
      8.1.9 aturan terkait penggunaan aset;
      8.1.10 kebijakan pengendalian akses;
      8.1.11 prosedur operasional untuk manajemen Teknologi Informasi;
      8.1.12 prinsip rekayasa Sistem secara aman;
      8.1.13 kebijakan keamanan terkait penyedia jasa;
      8.1.14 prosedur pengelolaan insiden;
      8.1.15 prosedur keberlanjutan bisnis;
      8.1.16 prasyarat hukum, regulasi dan kontraktual;
      8.1.17 catatan terkait pelatihan, kemampuan, pengalaman dan kualifikasi;
      8.1.18 hasil pemantauan dan pengukuran SMKI;
      8.1.19 program audit internal;
      8.1.20 hasil audit internal;
      8.1.21 hasil dari tinjauan manajemen;
      8.1.22 hasil dari tindakan korektif;
      8.1.23 *log* dari aktivitas pengguna, pengecualian dan kejadian keamanan; dan
      8.1.24 Informasi terdokumentasi yang dibutuhkan untuk menjamin efektivitas dari SMKI.

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

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

8.3.1 semua dokumentasi SMKI harus ditinjau paling sedikit satu kali dalam 1 (satu) tahun atau apabila terdapat perubahan dalam SMKI dan/atau Perangkat Daerah untuk menjamin kesesuaian dan kecukupannya dengan kondisi terkini SMKI dan Keamanan Informasi di Perangkat Daerah;

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

8.3.3 setiap perubahan terhadap dokumentasi SMKI sebagai hasil dari peninjauan dokumentasi harus disetujui oleh manajemen yang relevan di Perangkat Daerah;

8.3.4 Terkait proses salinan, distribusi dan retensi dokumentasi, hal- hal berikut berlaku:

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

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

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

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

8.3.4.5 kecuali diputuskan berbeda, seluruh dokumen SMKI memiliki masa retensi selama 10 tahun.

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

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

9.2 sumber daya yang dibutuhkan oleh SMKI mencakup sumber daya dengan kompetensi dan pemahaman yang memadai, dokumentasi, proses dan solusi teknis, baik berupa Perangkat Keras maupun Perangkat Lunak;

9.3 perencanaan sumber daya SMKI dapat dilakukan bersamaan dengan proses perencanaan dan penyusunan anggaran tahunan Perangkat Daerah; dan

9.4 pelatihan dan program peningkatan kesadaran terkait dengan SMKI dan Keamanan Informasi Perangkat Daerah akan dilakukan secara berkala bagi seluruh pengguna Sistem Informasi Perangkat Daerah. Program pelatihan dan peningkatan kesadaran tersebut akan dirancang sesuai dengan fungsi dan tanggung jawab pengguna.

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

10.1 efektivitas alur pertukaran Informasi dalam Perangkat Daerah SMKI dan/atau dari dan ke pihak eksternal;

10.2 tidak ada kebocoran Informasi sensitif milik Perangkat Daerah;

10.3 alur komunikasi SMKI mencakup:

10.3.1 komunikasi tatap muka;

10.3.2 surat dan memo internal;

10.3.3 email;

10.3.4 website Perangkat Daerah;

10.3.5 pengumuman Perangkat Daerah; dan

10.3.6 material cetak.

10.4 personil Perangkat Daerah yang tidak ditunjuk untuk memberikan materi Informasi tidak diperbolehkan untuk memberikan Informasi apapun;

10.5 informasi terkait dengan SMKI dan/atau Keamanan Informasi yang berasal dari sumber eksternal harus dikirimkan kepada Dinas untuk peninjauan dan pendistribusian kepada pihak yang relevan dalam SMKI. Hal ini mencakup:

10.5.1 penerbitan peraturan perundang-undangan yang baru maupun perubahan terhadap peraturan lama;

10.5.2 usulan perubahan terhadap prasyarat Keamanan Informasi; dan

10.5.3 teknologi, ancaman dan kelemahan baru terkait Keamanan Informasi.

11. Proses perencanaan dan pengendalian operasional SMKI harus dikoordinasikan dan dikomunikasikan. Proses perencanaan operasional SMKI harus dilakukan secara tahunan serta didokumentasikan dan dikomunikasikan kepada pihak yang terkait dengan SMKI. Proses pengendalian operasional SMKI adalah proses yang dilakukan untuk memastikan pelaksanaan operasional SMKI Perangkat Daerah telah sesuai dengan perencanaan yang telah dibuat. Proses pengendalian ini dapat mencakup aktivitas rapat peninjauan dan harus dilakukan paling sedikit 1 (satu) kali dalam tiga bulan serta melibatkan personil yang terlibat di SMKI Perangkat Daerah.
12. Metode untuk mencegah, mendeteksi dan menindaklanjuti pelanggaran terhadap hukum terkait HAKI perlu disusun dan diimplementasikan. Hal ini dapat mencakup aktivitas pemantauan, pengukuran, peninjauan dan/atau audit.
13. Pemantauan, pengukuran, analisis dan evaluasi dari implementasi dan operasional SMKI Perangkat Daerah adalah aktivitas periodik yang dilakukan untuk mengevaluasi kinerja Keamanan Informasi dan efektivitas SMKI Perangkat Daerah. Proses pemantauan, pengukuran, analisis, dan evaluasi mencakup:
    13.1 Metrik pemantauan dan pengukuran harus dipilih secara seksama untuk memastikan bahwa aktivitas pengukuran akan memberikan pemahaman mendalam mengenai kinerja SMKI dan kontrol pengendalian Keamanan Informasi Perangkat Daerah;
    13.2 Proses pengukuran tersebut mencakup proses-proses berikut:
        13.2.1 penentuan dari metrik pengukuran;
        13.2.2 pengukuran dari metrik yang telah ditentukan;
        13.2.3 analisis dan evaluasi dari hasil pengukuran.
    13.3 Dalam menentukan metrik pengukuran, harus mempertimbangkan aspek:
        13.3.1 sasaran SMKI yang diberikan pada kebijakan SMKI Perangkat Daerah;
        13.3.2 kontrol Keamanan Informasi yang diimplementasikan;
        13.3.3 metode dalam mengumpulkan data dan mengkalkulasi metrik;
        13.3.4 target pencapaian dari metrik;
        13.3.5 jadwal untuk melakukan pengukuran; dan
        13.3.6 personil yang bertanggung jawab untuk proses pengukuran.
    13.4 metrik pengukuran yang telah ditentukan harus memungkinkan evaluasi dari pencapaian sasaran SMKI;
    13.5 metrik yang telah ditetapkan harus dipantau dengan mengumpulkan data yang relevan dengan metrik;
    13.6 proses pengukuran harus dilakukan minimal 1 (satu) kali dalam satu tahun terutama untuk mengukur pencapaian dari sasaran SMKI;

13.7 hasil dari pengukuran harus dianalisis dan dievaluasi untuk menentukan pencapaian dari target pengukuran tersebut;

13.8 Hasil dari pengukuran harus dilaporkan kepada Kepala Perangkat Daerah;

13.9 Hasil dari proses pemantauan dan pengukuran efektivitas SMKI harus dianalisis dan dievaluasi untuk menentukan apakah implementasi dan operasi SMKI Perangkat Daerah:

13.9.1 sesuai dengan kebijakan, tujuan, standar dan prosedur SMKI Perangkat Daerah ;

13.9.2 memadai untuk menghadapi kebutuhan dan tantangan bisnis serta teknologi terkini; dan

13.9.3 sesuai dengan rencana SMKI yang sudah dibuat.

14. Peninjauan Keamanan Informasi secara independen harus secara rutin dilakukan.

14.1 peninjauan tersebut harus mencakup:

14.1.1 kontrol dan area Keamanan Informasi, seperti keamanan fisik, jaringan atau akses *logical*;

14.1.2 kebijakan, proses dan prosedur yang relevan dengan SMKI;

14.1.3 kepatuhan implementasi SMKI dan Keamanan Informasi dengan kebijakan, proses dan prosedur Keamanan Informasi Perangkat Daerah serta prasyarat hukum, peraturan perundangan-undangan serta kewajiban kontraktual terkait dengan SMKI;

14.1.4 Peninjauan teknis terhadap fasilitas pengolahan Informasi dan sarana pendukungnya.

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

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

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

15.1 Audit internal SMKI di Perangkat Daerah harus dilaksanakan minimal satu kali dalam satu tahun dan harus mencakup seluruh ruang lingkup SMKI;

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

15.3 Auditor yang dipilih untuk proses audit harus ditunjuk secara formal oleh Kepala Perangkat Daerah;

15.4 Program audit harus mencakup jadwal, metode, kriteria dan ruang lingkup, tanggung jawab serta prasyarat pelaporan dari audit;

15.5 Proses audit harus dilakukan sesuai dengan program audit yang telah ditetapkan secara formal;

15.6 Temuan audit harus diklasifikasikan berdasarkan kritikalitas dan cakupan dari temuan tersebut menjadi:

15.6.1 mayor, ketidaksesuaian ini mengindikasikan tidak berjalannya sama sekali sebuah proses SMKI atau kontrol Keamanan Informasi, atau apabila sebuah temuan dapat menyebabkan dampak buruk terhadap proses atau Sistem kritikal Perangkat Daerah;

15.6.2 minor, ketidaksesuaian ini mengindikasikan sebuah kealpaan/masalah kecil yang tidak mengindikasikan bahwa sebuah proses SMKI atau kontrol Keamanan Informasi tidak berjalannya sama sekali, atau apabila sebuah temuan tidak akan menyebabkan dampak buruk terhadap proses atau Sistem kritikal Perangkat Daerah; dan

15.6.3 peluang untuk perbaikan, kategori temuan ini bukan merupakan sebuah ketidaksesuaian namun mengindikasikan bahwa sebuah area dapat diperbaiki untuk meningkatkan kinerja dari proses atau Sistem.

15.7 Setiap ketidaksesuaian dan/atau peluang untuk perbaikan yang ditemukan dalam proses audit harus dicatat secara formal oleh auditor dan diterima oleh auditee;

15.8 Setiap ketidaksesuaian harus dikoreksi dan ditingkatkan oleh auditee dalam jangka waktu yang disepakati dengan cara merencanakan dan melaksanakan koreksi dan tindakan korektif;

15.9 Laporan audit harus dilaporkan kepada Kepala Perangkat Daerah dan dikomunikasikan kepada Dinas;

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

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

16. Ketidaksesuaian SMKI didefinisikan sebagai kondisi dimana adanya prasyarat SMKI yang tidak terpenuhi. Setiap ketidaksesuaian atau tidak terpenuhinya prasyarat SMKI harus diidentifikasi dan dilaporkan:

16.1 identifikasi dan laporan dari setiap ketidaksesuaian dapat didapatkan melalui:

16.1.1 proses pengelolaan insiden Keamanan Informasi;

16.1.2 peninjauan internal SMKI;

16.1.3 proses audit internal SMKI;

16.1.4 proses pemantauan dan pengukuran SMKI;

16.1.5 peninjauan dan/atau proses audit eksternal terhadap SMKI atau Keamanan Informasi; dan

16.1.6 laporan dan masukan dari *stakeholder* yang terkait.

16.2 setiap ketidaksesuaian yang terjadi, harus ditangani secara tepat dengan cara:

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

16.2.2 bmenangani setiap akibat dari ketidaksesuaian yang mungkin terjadi.

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

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

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

16.5.1 peninjauan terhadap ketidaksesuaian yang terjadi;

16.5.2 menentukan penyebab dari ketidaksesuaian;

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

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

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

17. kesesuaian, kecukupan dan efektivitas dari SMKI Perangkat Daerah harus secara berkesinambungan ditingkatkan.

18. inisiatif peningkatan harus secara formal diidentifikasi, direncanakan, diimplementasikan dan ditinjau.

19. identifikasi dari peningkatan harus dilakukan berdasarkan log, laporan dan hasil dari:

19.1 proses pengelolaan insiden Keamanan Informasi;

19.2 peninjauan internal SMKI;

19.3 proses audit internal SMKI;

19.4 proses pemantauan dan pengukuran SMKI;

19.5 peninjauan dan/atau proses audit eksternal terhadap SMKI atau Keamanan Informasi; dan

19.6 laporan dan masukan dari *stakeholder* yang terkait.

20. perencanaan dan dari inisiatif peningkatan harus ditinjau untuk memastikan bahwa inisiatif tersebut dapat mencapai tujuannya.

21. dokumentasi yang relevan dengan proses peningkatan secara berkesinambungan harus dibuat dan dipelihara.

BAB III
PENGENDALIAN ORGANISASI KEAMANAN INFORMASI

A. Tujuan

Tujuan dari pengendalian organisasi keamanan informasi adalah 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;
6. Pengendalian terhadap *mobile device* dan *teleworking*.

C. Kebijakan

1. Struktur Tim Keamanan lnformasi setiap perangkat daerah berikut tanggung jawab dan wewenangnya diuraikan sebagai berikut:
   1.1 Struktur Tim Keamanan Informasi Perangkat Daerah

Gambar 3.1
Struktur Tim Keamanan Informasi Perangkat Daerah

1.2 Tanggung jawab Tim Keamanan Informasi setiap Perangkat Daerah

1.2.1 Manajemen Puncak

1.2.1.1 memberikan arahan dan tujuan umum dari SMKI Perangkat Daerah, dalam bentuk kebijakan Sistem Manajemen Keamanan Informasi (SMKI);

1.2.1.2 memastikan bahwa tujuan dan rencana dari SMKI Perangkat Daerah telah ditetapkan;

1.2.1.3 menetapkan struktur organisasi beserta alokasi tugas dan tanggung jawab dalam SMKI Perangkat Daerah;

1.2.1.4 mengkomunikasikan kepada personil dalam Perangkat Daerah terkait pentingnya pemenuhan aturan terkait keamanan informasi Perangkat Daerah sesuai ketentuan peraturan perundang-undangan serta perlunya peningkatan SMKI Perangkat Daerah secara berkesinambungan;

1.2.1.5 menyediakan sumber daya yang memadai untuk menetapkan, mengimplementasi, mengoperasikan, memantau, meninjau, memelihara dan meningkatkan SMKI Perangkat Daerah;

1.2.1.6 menetapkan kriteria penerimaan risiko dan tingkat risiko yang dapat diterima;

1.2.1.7 menyetujui tingkat risiko residual keamanan informasi;

1.2.1.8 memastikan pelaksanaan audit internal SMKI; dan

1.2.1.9 menghadiri dan memimpin rapat tinjauan manajemen SMKI.

1.2.2 Koordinator SMKI

1.2.2.1 menyusun, mengkoordinasikan serta memantau pelaksanaan program kerja SMKI;

1.2.2.2 mengkoordinasikan pelaksanaan proses manajemen risiko SMKI Perangkat Daerah;

1.2.2.3 mengkoordinasikan pelaksanaan aktifitas SMKI serta pengamanan informasi di Perangkat Daerah;

1.2.2.4 mengkoordinasikan proses peninjauan secara berkala terhadap implementasi SMKI di Perangkat Daerah;

1.2.2.5 mengkoordinasikan proses pengukuran efektivitas SMKI dan kontrol keamanan informasi di Perangkat Daerah;

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

1.2.2.7 memberikan laporan secara berkala terkait kondisi SMKI dan keamanan informasi Perangkat Daerah kepada manajemen puncak SMKI.

1.2.3 Auditor Internal SMKI

1.2.3.1 menyusun dan memantau program dan jadwal audit internal SMKI;

1.2.3.2 mengkoordinasikan pelaksanaan proses audit internal SMKI;

1.2.3.3 merangkum dan melaporkan hasil audit internal SMKI kepada manajemen puncak SMKI;

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

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

1.2.4 Pengendali Dokumen dan Kepatuhan

1.2.4.1 mengkoordinasikan dan memantau proses pengelolaan dokumentasi terkait SMKI Perangkat Daerah hal ini mencakup kebijakan dan prosedur terkait SMKI Perangkat Daerah;

1.2.4.2 mengidentifikasi dan mendokumentasikan peraturan perundang-undangan dan kewajiban kontrak yang relevan dengan SMKI dan keamanan informasi Perangkat Daerah;

1.2.4.3 melakukan pemantauan berkala terhadap kepatuhan SMKI Perangkat Daerah dengan prasyarat dari kebijakan dan prosedur SMKI Perangkat Daerah serta peraturan peraturan perundang-undangan dan kewajiban kontrak yang relevan dengan SMKI dan keamanan informasi Perangkat Daerah;

1.2.4.4 menyusun dan mengkoordinasikan pelaksanaan program *security awareness* bagi personil Perangkat Daerah; dan

1.2.4.5 menyusun metrik pengukuran efektivitas SMKI dan kontrol keamanan informasi Perangkat Daerah.

1.2.5 Pengelola Aset dan Risiko

1.2.5.1 mengkoordinasikan dan memantau pengelolaan aset informasi dan aset pengolahan dan penyimpanan informasi Perangkat Daerah, hal ini mencakup proses registrasi, inventarisasi serta pemeliharaan inventarisasi aset tersebut;

1.2.5.2 menyusun dan memelihara dokumen registrasi aset informasi dan aset pengolahan dan penyimpanan informasi Perangkat Daerah;

1.2.5.3 melakukan peninjauan terkait proses penanganan aset informasi dan aset pengolahan dan penyimpanan informasi Perangkat Daerah berdasarkan kebijakan dan prosedur terkait pengelolaan aset SMKI Perangkat Daerah;

1.2.5.4 menyusun dan mengkoordinasikan aktivitas proses pengelolaan manajemen risiko SMKI di Perangkat Daerah, bekerja sama dengan pemilik risiko, berdasarkan kebijakan dan prosedur terkait pengelolaan risiko SMKI Perangkat Daerah;

1.2.5.5 mengkoordinasikan proses registrasi terhadap risiko SMKI di Perangkat Daerah, bekerja sama dengan pemilik risiko;

1.2.5.6 mengkoordinasikan pengkinian secara rutin terhadap registrasi risiko Perangkat Daerah, bekerja sama dengan pemilik risiko; dan

1.2.5.7 menyusun dan memelihara dokumen *risk profile* dan *risk treatment plan* SMKI Perangkat Daerah.

1.2.6 Pengelola Keamanan Fisik dan Sistem Informasi

1.2.6.1 mengkoordinasikan dan memantau proses dan aktifitas pengamanan fisik dan lingkungan dalam Perangkat Daerah;

1.2.6.2 melaksanakan proses pengelolaan dan pemeliharaan fasilitas pengamanan fisik Perangkat Daerah berdasarkan kebijakan dan prosedur terkait keamanan fisik dan lingkungan SMKI Perangkat Daerah;

1.2.6.3 melaksanakan proses pengelolaan dan pemeliharaan hak akses fisik ke fasilitas Perangkat Daerah berdasarkan kebijakan dan prosedur terkait keamanan fisik dan lingkungan SMKI Perangkat Daerah;

1.2.6.4 mengkoordinasikan dan memantau proses dan aktifitas pengelolaan akses *logical*;

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

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

1.2.6.7 mengkoordinasikan dan memantau pengelolaan keamanan operasional sistem informasi Perangkat Daerah berdasarkan kebijakan dan prosedur terkait pengelolaan keamanan operasional sistem informasi Perangkat Daerah; dan

1.2.6.8 merancang, memantau dan memelihara sistem keamanan dari sistem informasi Perangkat Daerah yang mencakup perangkat keras, perangkat lunak maupun keamanan jaringan dalam sistem informasi Perangkat Daerah.

1.2.7 Pengelola Insiden Keamanan Informasi dan *Business Continuity*

1.2.7.1 mengkoordinasikan proses pendokumentasi-an laporan terkait kejadian, kelemahan dan insiden keamanan informasi berdasarkan kebijakan dan prosedur terkait pengelolaan insiden keamanan informasi Perangkat Daerah;

1.2.7.2 mengkoordinasikan dan memantau pengelolaan insiden keamanan informasi berdasarkan kebijakan dan prosedur terkait pengelolaan insiden keamanan informasi Perangkat Daerah;

1.2.7.3 mendokumentasikan proses pengelolaan insiden keamanan informasi di Perangkat Daerah;

1.2.7.4 mengkoordinasikan dan memantau pengelolaan *business continuity management* di Perangkat Daerah berdasarkan kebijakan dan prosedur terkait *business continuity management* Perangkat Daerah;

1.2.7.5 mengkoordinasikan penyusunan, pengujian dan pemeliharaan *business continuity plan* dan *disaster recovery plan* Perangkat Daerah; dan

1.2.7.6 memastikan terjaganya aspek keamanan informasi dalam proses *business continuity management*.

2. Tanggung jawab dan wewenang Tim Keamanan Informasi di setiap perangkat daerah dapat dipetakan dalam jabatan struktural dan/atau diperankan oleh Pejabat struktural dan/atau Pejabat fungsional.
3. Perjanjian Kerahasiaan

   Setiap Kepala Perangkat Daerah mengidentifikasi dan mengkaji secara berkala persyaratan untuk menjaga kerahasiaan aset informasi yang dituangkan dalam dokumen perjanjian kerahasiaan.

   Perjanjian kerahasiaan harus memuat unsur-unsur sebagai berikut:

   3.1 Definisi dari informasi yang akan dilindungi.

   3.2 Durasi yang diharapkan dari sebuah perjanjian kerahasiaan.

   3.3 Tanggung jawab yang diharapkan dari sebuah perjanjian kerahasiaan.

   3.4 Penandatangan untuk menghindari pengungkapan informasi secara tidak sah.

   3.5 Perlindungan kepemilikan informasi, rahasia organisasi, dan kekayaan intelektual.

   3.6 Izin menggunakan informasi rahasia, dan hak-hak penandatangan untuk menggunakan informasi.

   3.7 Hak untuk melakukan audit dan memantau kegiatan yang melibatkan informasi rahasia.

   3.8 Proses untuk pemberitahuan dan pelaporan dari penyingkapan yang dilakukan secara tidak sah atau pelanggaran terhadap kerahasiaan informasi.

   3.9 Tindakan yang diperlukan pada saat sebuah perjanjian kerahasiaan diakhiri.

   3.10 Syarat-syarat untuk informasi yang akan dikembalikan atau dimusnahkan pada saat penghentian perjanjian.

   3.11 Tindakan yang akan diambil apabila terjadi pelanggaran terhadap perjanjian ini.
4. Pemisahan tugas

   Setiap Kepala Perangkat Daerah harus melakukan pemisahan tugas untuk proses yang melibatkan informasi yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA untuk menghindari adanya Pegawai yang memiliki pengendalian eksklusif terhadap seluruh aset informasi dan perangkat pengolahnya.
5. Hubungan dengan Pihak Berwenang

   Setiap Kepala Perangkat Daerah mengidentifikasi dan menjalin kerjasama dengan pihak-pihak berwenang di luar perangkat daerah yang terkait dengan keamanan informasi.

6. Hubungan dengan Komunitas Keamanan Informasi

   Setiap Kepala Perangkat Daerah menjalin kerjasama dengan komunitas keamanan informasi di luar Kepala Perangkat Daerah melalui pelatihan, seminar, atau forum lain yang relevan dengan keamanan informasi.

7. Keamanan informasi pada pengelolaan proyek

   Pengendalian terhadap keamanan informasi harus diterapkan dalam pengelolaan proyek dan harus diaplikasikan pada seluruh fase dalam metodologi pengelolaan proyek.

8. Pengendalian terhadap *mobile device* dan *teleworking*

   8.1 Penggunaan perangkat *mobile*, baik milik pribadi atau milik Perangkat Daerah untuk mengakses dan/atau menyimpan informasi milik Perangkat Daerah harus sangat dibatasi sesuai dengan kebutuhan pekerjaan dengan mempertimbangkan prinsip kehati-hatian saat menggunakan perangkat *mobile* dengan menghindari meninggalkan perangkat tanpa pengawasan.

   8.2 Perangkat *mobile* harus mengaktifkan fitur otentikasi pengguna, seperti penggunaan *user name* dan *password*, sesuai dengan kebijakan terkait pengendalian akses.

   8.3 Informasi sensitif harus dienkripsi atau dilindungi dengan *password* pada saat disimpan di *mobile device*, sesuai dengan klasifikasi informasinya.

   8.4 Informasi sensitif milik Perangkat Daerah yang disimpan pada perangkat *mobile device* harus di-*backup* secara berkala untuk menghindari hilangnya aspek ketersediaan dari informasi.

   8.5 Aktivitas *teleworking* sebagai sarana pegawai untuk bekerja dari lokasi di luar area kerja Perangkat Daerah dengan mengakses jaringan internal secara *remote* melalui jaringan internet diperbolehkan namun sangat dibatasi hanya untuk personil yang diberi izin berdasarkan kebutuhan pekerjaannya.

   8.6 Akses ke jaringan internal Perangkat Daerah dari jaringan internet harus menggunakan koneksi aman dengan menggunakan antara lain teknologi VPN.

   8.7 Kebijakan terkait teknologi *teleworking* sebagai sarana pegawai bekerja pada lokasi di luar Perangkat Daerah dengan mengakses jaringan internal Perangkat Daerah. Teknologi ini diperbolehkan untuk digunakan dalam kondisi sebagai berikut:

      8.7.1 perangkat akses (misalnya komputer, *notebook*) yang digunakan untuk *teleworking* harus terinstalasi *firewall* dan *antivirus*;

      8.7.2 mekanisme akses terhadap sistem atau aplikasi disesuaikan dengan klasifikasi aset informasi:

         8.7.2.1 informasi publik : dapat diakses langsung.

         8.7.2.2 informasi rahasia : harus menggunakan protokol HTTPS atau SSH; dan harus menggunakan VPN, sebelum kemudian mengakses melalui protokol HTTPS atau SSH.

BAB IV
MANAJEMEN RISIKO

A. Tujuan

Tujuan dari manajemen risiko adalah untuk mengelola risiko Keamanan Informasi yang dihadapi oleh Perangkat Daerah dalam rangka untuk mempersiapkan diri terhadap terjadinya risiko beserta dampaknya.

B. Ruang Lingkup

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

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

C. Kebijakan

1. Kriteria penerimaan risiko dan penilaian Keamanan Informasi harus ditetapkan untuk memberikan arahan bagi Perangkat Daerah terhadap penanganan risiko yang harus dilakukan.
2. Perangkat Daerah harus menerapkan konteks terkait rencana perencanaan identifikasi Risiko yang meliputi isu-isu, pihak terkait dan prasyarat Keamanan Informasi internal dan eksternal yang terkait dengan Keamanan Informasi harus diidentifikasi dan ditetapkan sebagai pertimbangan dalam mengidentifikasi risiko Keamanan Informasi. Hal ini setidaknya mencakup:
   2.1 kegiatan utama yang dilakukan oleh Perangkat Daerah;
   2.2 kebijakan internal Perangkat Daerah;
   2.3 proses bisnis Perangkat Daerah;
   2.4 kewajiban hukum, peraturan perundangan-undangan dan kewajiban kontrak yang dimiliki oleh Perangkat Daerah; dan
   2.5 kondisi Teknologi Informasi dan Keamanan Informasi, baik internal maupun eksternal yang relevan dengan Perangkat Daerah.
3. Perangkat Daerah harus melaksanakan penilaian risiko yang berpengaruh terhadap kegagalan sistem dan operasional Teknologi Informasi terkait dengan aspek Keamanan Informasi yang mencakup aktivitas:
   3.1 identifikasi risiko:
      3.1.1 mengidentifikasi ancaman, merupakan aktifitas untuk mengidentifikasi ancaman terhadap risiko Keamanan Informasi;

3.1.2 ancaman didefinisikan sebagai potensi penyebab insiden yang tidak diinginkan yang dapat menyebabkan kerusakan/kerugian bagi Perangkat Daerah dan sistemnya;

3.1.3 sebuah ancaman tidak dapat dikatakan sebuah risiko apabila tanpa kombinasi dengan kelemahan yang dapat dieksploitasi;

3.1.4 mengidentifikasi kelemahan dilakukan setelah pengidentifikasian ancaman dilakukan;

3.1.5 kelemahan didefinisikan sebagai potensi kekurangan pada proses dan kontrol keamanan yang dapat dieksploitasi oleh satu ancaman atau lebih;

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

3.1.7 risiko harus dialokasikan ke pemilik risiko; dan

3.1.8 pemilik risiko bertanggung jawab untuk mengelola risiko yang telah teridentifikasi.

3.2 analisis risiko:

3.2.1 menilai dampak potensial yang akan terjadi apabila risiko yang teridentifikasi terwujud;

kriteria dampak merupakan parameter untuk menentukan tingkat kerugian terhadap risiko yang terjadi. Contoh kriteria dampak sebagai berikut:

Tabel 4.1 Dampak Risiko SMKI

Tingkat Dampak	Operasional	Peraturan / Hukum	Aset Informasi	Reputasi
1 (Ringan)	Penundaan proses bisnis setengah hari	Tidak ada pelanggaran hukum	Tidak ada kebocoran atau kehilangan Aset Informasi	Jumlah keluhan secara lisan ≤ 3
2 (Sedang)	Penundaan proses bisnis 1 hari	Pelanggaran ringan dengan surat peringatan	Berdampak pada kebocoran atau kehilangan Aset Informasi yang bersifat publik	Jumlah keluhan secara lisan 3 < x ≤ 5
3 (Berat)	Penundaan proses bisnis 3 hari	Pelanggaran sedang yang dikenakan sanksi administratif	Berdampak pada kebocoran atau kehilangan Aset informasi yang bersifat terbatas	Jumlah keluhan secara lisan > 5
4 (Sangat Berat)	Penundaan proses bisnis > 3 hari	Pelanggaran berat dengan sanksi hukum	Berdampak pada kebocoran atau kehilangan Aset Informasi yang bersifat rahasia	Pemberitaan negatif di media massa lokal dan media sosial

3.2.2 menilai kemungkinan realistis terjadinya risiko yang teridentifikasi; dan

3.2.3 kriteria kemungkinan merupakan parameter untuk menentukan tingkat kejadian terhadap Risiko. Contoh kriteria kemungkinan adalah sebagai berikut:

Tabel 4.2 Kemungkinan Risiko SMKI

Nilai	Tingkat	Kriteria Kemungkinan
		Frekuensi terjadinya
1	Rendah	Kejadian < 2 kali dalam 1 tahun
2	Sedang	Kejadian 2 kali s.d 5 kali dalam 1 tahun
3	Tinggi	Kejadian 6 kali s.d 10 kali dalam 1 tahun
4	Ekstrim	Kejadian >10 kali dalam 1 tahun

3.2.4 evaluasi risiko:

3.2.4.1 membandingkan hasil analisis risiko dengan kriteria risiko yang sudah ditetapkan;

3.2.4.2 risiko yang masuk dalam kriteria penerimaan risiko akan diterima;

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

3.2.4.4 setiap penanganan risiko harus diberikan prioritas.

4. hasil evaluasi risiko harus dianalisis terkait risiko tersebut dapat diterima dalam level tertentu berdasarkan kriteria penerimaan risiko yang telah ditetapkan atau memerlukan penanganan risiko lebih lanjut. Tabel risiko adalah matriks antara nilai dari dampak dan kemungkinan yang menghasilkan tingkat risiko. Contoh tabel **risiko** adalah sebagai berikut:

Tabel 4.3 Nilai Risiko SMKI

Matriks Analisis Risiko		Dampak			
		1 (Ringan)	2 (Sedang)	3 (Berat)	4 (Sangat Berat)
Kemungkinan	1 (Rendah)				
	2 (Sedang)				
	3 (Tinggi)				
	4 (Ekstrim)				

Keterangan : Rendah Sedang Tinggi

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

12. Metode komunikasi dan koordinasi risiko harus ditetapkan yang meliputi:
    12.1 proses komunikasi dan koordinasi risiko merupakan proses berkesinambungan untuk mengkomunikasikan dan mengkoordinasikan setiap Informasi, aktifitas dan keputusan terkait dengan risiko Keamanan Informasi dan proses manajemen risiko;
    12.2 setiap Informasi, aktivitas dan keputusan harus dikomunikasikan dan dikoordinasikan dengan pemiliki risiko, personil terkait dan Kepala Perangkat Daerah; dan
    12.3 setiap komunikasi dan koordinasi eksternal terkait risiko Keamanan Informasi dan manajemen risiko harus disetujui oleh Kepala Perangkat Daerah.

BAB V
KEAMANAN SUMBER DAYA MANUSIA

A. Tujuan

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

B. Ruang Lingkup

Kebijakan 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.

C. Kebijakan

1. Seluruh pegawai bertanggung jawab untuk menjaga keamanan informasi di setiap Perangkat Daerah sesuai dengan tugas dan fungsinya.
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. Pihak ketiga harus menyetujui dan menandatangani syarat dan perjanjian untuk menjaga keamanan informasi di setiap Perangkat Daerah.
4. Peran dan tanggung jawab pegawai dan pihak ketiga terhadap keamanan informasi didefinisikan, didokumentasikan, dan dikomunikasikan kepada yang bersangkutan.
5. Peran dan tanggung jawab pegawai terhadap keamanan informasi harus menyertakan persyaratan untuk:
   5.1 Melaksanakan dan bertindak sesuai dengan organisasi keamanan informasi.
   5.2 Melindungi aset dari akses yang tidak sah, penyingkapan, modifikasi, kerusakan atau gangguan.
   5.3 Melaksanakan proses keamanan atau kegiatan keamanan informasi sesuai dengan peran dan tanggung jawabnya.
6. Melaporkan kejadian, potensi kejadian, atau risiko keamanan informasi sesuai dengan Kebijakan dan Standar SMKI di setiap Perangkat Daerah.
7. Kepala Perangkat Daerah akan melakukan pemeriksaan data pribadi yang diberikan oleh pegawai dan pihak ketiga sesuai dengan ketentuan peraturan perundang-undangan.
8. Pemeriksaan latar belakang calon pegawai dan pihak ketiga setiap Perangkat Daerah harus memperhitungkan privasi, perlindungan data pribadi dan/atau pekerjaan berdasarkan undang-undang, meliputi:

8.1 ketersediaan referensi, dari referensi hubungan kerja dan referensi pribadi.

8.2 pemeriksaan kelengkapan dan ketepatan dari riwayat hidup pemohon.

8.3 konfirmasi kualifikasi akademik dan profesional yang diklaim.

8.4 pemeriksaan independen identitas (paspor atau dokumen yang sejenis).

9. Pemeriksaan lebih rinci, seperti pemeriksaan dari catatan kriminal.
10. Seluruh Aparatur Sipil Negara (ASN) harus mendapatkan pendidikan, pelatihan, dan sosialisasi keamanan informasi secara berkala sesuai tingkat tanggung jawabnya.
11. Pihak ketiga, jika diperlukan, mendapatkan sosialisasi untuk meningkatkan kepedulian terhadap keamanan informasi.
12. Seluruh pegawai dan pihak ketiga yang melanggar Kebijakan dan Standar SMKI di Lingkungan Pemerintah Daerah akan dikenai sanksi atau tindakan disiplin sesuai ketentuan yang berlaku.
13. Kepatuhan pegawai terhadap Kebijakan dan Standar SMKI di setiap Perangkat Daerah harus dievaluasi secara berkala oleh atasan masing-masing.
14. Kepala Perangkat Daerah harus menghentikan hak penggunaan aset informasi bagi pegawai yang sedang menjalani pemeriksaan yang terkait dengan dugaan adanya pelanggaran Kebijakan dan Standar SMKI di setiap Perangkat Daerah dan/atau yang sedang menjalani proses hukum.
15. Kepala Perangkat Daerah harus mencabut hak akses terhadap aset informasi yang dimiliki pegawai dan pihak ketiga apabila yang bersangkutan tidak lagi bekerja di Perangkat Daerah tersebut.

BAB VI
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;
6. Pertukaran media informasi secara Fisik.

C. Kebijakan

1. Tanggung Jawab terhadap Aset Informasi
   - 1.1 Kepala Perangkat Daerah mengidentifikasi aset informasi dan mendokumentasikannya dalam daftar inventaris aset informasi. Daftar inventaris aset informasi dipelihara dan dikelola perubahannya oleh Penanggung Jawab Pengendalian Dokumen.
   - 1.2 Kepala Perangkat Daerah menetapkan pemilik aset informasi.
   - 1.3 Kepala Perangkat Daerah menetapkan aset informasi yang terkait dengan perangkat pengolah informasi.
   - 1.4 Pemilik Aset Informasi menetapkan aturan penggunaan aset informasi.
   - 1.5 Seluruh pegawai yang berhenti bekerja atau mutasi harus mengembalikan seluruh aset informasi yang dipergunakan selama bekerja sesuai dengan ketentuan yang berlaku.
   - 1.6 Pihak ketiga yang habis masa kontrak kerjanya harus mengembalikan seluruh aset informasi yang dipergunakan selama bekerja di Perangkat Daerah yang bersangkutan.
2. Aset Informasi yang diinventaris adalah aset dalam bentuk:
   - 2.1 perangkat keras, meliputi perangkat keras yang digunakan untuk mengolah dan menyimpan Informasi dalam bentuk fisik maupun elektronik, yang mencakup namun tidak terbatas pada komputer, *notebook*, server, *harddisk drive*, USB disk;
   - 2.2 Perangkat Lunak, meliputi Perangkat Lunak yang digunakan untuk mengolah Informasi dalam bentuk elektronik, yang mencakup namun tidak terbatas pada sistem operasi, aplikasi, dan database;

2.3 perangkat jaringan, meliputi perangkat keras dan lunak yang digunakan untuk membentuk dan infrastruktur jaringan telekomunikasi, yang mencakup namun tidak terbatas pada *hub*, *switch*, *router*, *firewall*, IDS, IPS, dan *network monitoring tools*;

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

2.5 layanan, meliputi layanan yang digunakan untuk mendukung operasional perangkat pengolahan dan Penyimpanan Informasi yang mencakup namun tidak terbatas pada layanan jaringan komunikasi, layanan *hosting* dan *co-location*, layanan pemeliharaan perangkat dan Sistem, dan layanan pemasangan infrastruktur; dan

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

3. Pemilik aset dapat mendelegasikan tugas pengamanan dan pemeliharaan aset kepada kustodian aset, namun tanggung jawab akhir terhadap aset tetap berada pada pemilik aset.
4. Aset pengolahan dan penyimpanan Informasi harus secara berkala dipelihara dengan memadai.
5. Apabila dalam pemeliharaan aset pengolahan dan penyimpanan Informasi tersebut harus menggunakan jasa pihak ketiga penyedia, maka:
   5.1 kontrak pemeliharaan perlu dibuat dengan pihak ketiga penyedia jasa yang kompeten dan relevan; dan
   5.2 peralatan yang dibawa keluar untuk pemeliharaan harus diperiksa untuk mencegah kebocoran Informasi.
6. Perangkat Daerah harus mendefinisikan klasifikasi Aset Informasi dengan mempertimbangkan sebagai berikut:
   6.1 Aset Informasi diklasifikasikan berdasarkan tingkat sensitivitas Informasi serta tingkat kritikalitas Sistem, yang meliputi:
      6.1.1 klasifikasi Aset Informasi secara berkala; dan
      6.1.2 pengguna yang diijinkan mengakses Aset Informasi.
   6.2 pemberian label klasifikasi Informasi harus dilakukan secara konsisten terhadap seluruh Aset Informasi;
   6.3 klasifikasi Aset Informasi dan seberapa tingkat kerahasiaan Aset Informasi, didefinisikan sesuai ketentuan peraturan perundang- undangan, diuraikan sesuai tabel berikut:

Tabel 6.1 Klasifikasi Aset Informasi

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

7. Setiap pemilik Informasi harus memperhatikan Keamanan Informasi yang tersimpan dalam media penyimpanan Informasi antara lain:
   7.1 dalam hal data yang tersimpan di dalam media bersifat rahasia, perlu diberikan proteksi kata sandi untuk melindungi data;
   7.2 dalam hal tidak lagi dibutuhkan atau digunakan, seluruh data yang tersimpan di dalam media harus sepenuhnya dihapus sehingga tidak lagi dapat dipulihkan;
   7.3 data yang tersimpan di dalam media yang akan dibuang harus mendapatkan perlakuan khusus guna meminimalkan terjadinya kebocoran Informasi kepada pihak yang tidak sah, yaitu:
      7.3.1 data yang tersimpan di dalam media yang memuat Informasi rahasia harus dibuang dengan cara dihancurkan atau dibakar; dan
      7.3.2 data yang tersimpan di dalam media yang memuat Informasi lainnya harus dilakukan penghapusan total dengan cara tertentu yang tidak lagi dapat dipulihkan.
8. Pengamanan penggunaan kembali atau penghapusan atau pemusnahan perangkat
   8.1 perangkat pengolah informasi penyimpan data yang sudah tidak digunakan lagi harus disanitasi sebelum digunakan kembali atau dihapuskan atau dimusnahkan.

8.2 penanganan perangkat pengolah informasi penyimpan data di setiap Perangkat Daerah sesuai dengan standar penanganan media penyimpan data yang yang berlaku di Perangkat Daerah yang bersangkutan.

9. Pelabelan dan penanganan Aset Informasi berdasarkan klasifikasi Aset Informasi dapat dilakukan sebagai berikut :

Tabel 6.2 Pelabelan dan penanganan Aset Informasi

Tipe	Klasifikasi		
	Publik	Internal	Rahasia
Dokumen dan catatan (*record*) dalam bentuk non elektronik	Tidak diperlukan penanganan khusus	Diberi label "Internal"	Diberi label "Rahasia"
Map penyimpan dokumen	Tidak diperlukan penanganan khusus	Tidak diperlukan penanganan khusus	Diberi label "Rahasia"
Amplop pengiriman surat internal (di dalam kantor)	Tidak diperlukan penanganan khusus	Tidak diperlukan penanganan khusus	Amplop diberi label "Rahasia"
Amplop untuk surat eksternal (ke luar kantor)	Tidak diperlukan penanganan khusus	Pada amplop ditandai "Internal"	(1) Menggunakan 2 amplop, dimana amplop pertama dimasukkan kedalam amplop kedua; (2) Pada amplop pertama ditandai "Rahasia", dan pada amplop kedua
Dokumen dan catatan (*record*) dalam bentuk elektronik (*softcopy*)	Tidak diperlukan penanganan khusus	Memberikan label "Internal" pada bagian awal dari nama file atau pada bagian tertentu dari file *properties*.	Memberikan label "Rahasia" pada bagian awal dari nama bagian tertentu dari file *properties*.
Publikasi / Distribusi	Tidak ada pembatasan	(1) Tersedia untuk personil internal perangkat daerah pemilik Informasi; (2) Distribusi kepada pihak eksternal dibatasi berdasakan kebutuhan pekerjaan maupun operasional di lingkungan Pemerintah Daerah; (3) Distribusi kepada pihak eksternal perlu seijin pemilik Informasi; (4) Sensitifitas dan kritikalitas Informasi perlu diberitahukan kepada pihak eksternal.	(1) Distribusi kepada pihak eksternal sangat dibatasi untuk kebutuhan pekerjaan; (2) Apabila memungkinkan, Informasi rahasia tidak disalin oleh pihak eksternal (*eyes only*); (3) Distribusi kepada pihak eksternal perlu seijin pemilik Informasi; (4) Sensitifitas dan kritikalitas Informasi perlu diberitahukan kepada pihak eksternal; (5) Pihak ketiga harus disertai perjanjian kerahasiaan (*non disclosure agreement* - NDA)
Pencetakan Informasi	Tidak ada pembatasan	Dibatasi hanya untuk kebutuhan internal	Pencetakan hanya pada printer organisasi dan diusahakan tidak mencetak menggunakan jasa pencetakan eksternal

Tipe	Klasifikasi		
	Publik	Internal	Rahasia
Surat menyurat internal (di dalam kantor)	Pastikan nama dan alamat tujuan sudah benar	(1) Pastikan nama dan alamat tujuan sudah benar; (2) Mengikuti ketentuan penggunaan amplop untuk surat internal	(1) Pastikan nama dan alamat tujuan sudah benar; (2) Mengikuti ketentuan penggunaan amplop untuk surat internal; (3) MengInformasi kan kepada penerima akan pengiriman Informasi tersebut; (4) Mengkonfirmasi kepada penerima
Surat menyurat eksternal (ke luar kantor)	Pastikan nama dan alamat tujuan sudah benar	(1) Pastikan nama dan alamat dan tujuan sudah benar; (2) Mengikuti ketentuan penggunaan amplop untuk surat eksternal; (3) Menggunakan jasa kurir pengiriman tercatat dengan tanda pengiriman.	(1) Pastikan nama dan alamat tujuan sudah benar; (2) Mengikuti ketentuan penggunaan amplop untuk surat eksternal; (3) Menggunakan jasa kurir pengiriman tercatat dengan tanda pengiriman (4) Menginformasikan kepada penerima akan pengiriman Informasi tersebut; (5) Mengkorfirmasi kepada penerima bahwa Informasi yang dikirim sudah diterima
Pengiriman ke pihak internal melalui email	(1) Pengiriman e- mail harus menggunaka n akun e-mail Perangkat Daerah / Unit Kerja; (2) Tidak diperlukan penanganan khusus.	(1) Pengiriman e- mail harus menggunaka n akun e-mail Perangkat Daerah / Unit Kerja; (2) Pastikan alamat email tujuan sudah benar; (3) Pengiriman Informasi, termasuk *forwarding* / meneruskan email hanya boleh dilakukan oleh pemilik Informasi.	(1) Pengiriman e- mail harus menggunaka n akun e-mail Perangkat Daerah / Unit Kerja; (2) Memberi *Password* pada Informasi yang dikirim melalui email; (3) *password* diinformasikan kepada penerima secara terpisah; (4) Tidak mencantumkan Informasi rahasia di *body text* e-mail; (5) Pengiriman Informasi, termasuk *forwarding* / meneruskan email hanya boleh dilakukan oleh pemilik Informasi.
Pengiriman ke pihak eksternal melalui email	(1) Pengiriman e- mail harus menggunakan akun e-mail Perangkat Daerah / Unit Kerja; (3) Pastikan alamat email tujuan sudah benar	(1) Pengiriman e- mail harus menggunakan akun e-mail Perangkat Daerah / Unit Kerja; (3) Pastikan alamat email tujuan sudah benar	(1) Tidak disarankan menggunakan e-mail untuk mengirim Informasi dengan klasifikasi ini; (2) Pengiriman e- mail harus menggunakan akun e-mail Perangkat Daerah / Unit Kerja; (3) Pastikan alamat email tujuan sudah benar; (4) Memberi *password* pada Informasi yang dikirim melalui email dan *password*

Tipe	Klasifikasi		
	Publik	Internal	Rahasia
			diinformasikan kepada penerima secara terpisah
Penyimpanan Informasi *hardcopy*	Tidak diperlukan penanganan khusus	Tidak diperlukan penanganan khusus	Disimpan secara aman dalam tempat penyimpanan yang terkunci
Penyimpanan Informasi *softcopy*	Tidak diperlukan penanganan khusus	Tidak diperlukan penanganan khusus	(1) Penyimpanan pada komputer atau media penyimpanan harus yang menggunakan *password*; (2) File yang disimpan harus diberi *password*; (3) Media penyimpanan eksternal (*external hard disk*, atau *flashdisk*) harus disimpan pada tempat penyimpanan yang terkunci.
Penyimpanan pada pihak ketiga	Tidak diperlukan penanganan khusus	Harus disertai dengan perjanjian kerahasiaan (*non disclosure agreement* – NDA)	Harus disertai dengan perjanjian kerahasiaan (non disclosure agreement – NDA)
Penghancuran (*disposal*)	(1) Tidak diperlukan penanganan khusus; (2) Masih dapat digunakan kembali sebagai kertas untuk pekerjaan (*scrappaper*)	(1) Memperhatik an masa retensi Informasi yang disetujui oleh pemilik Informasi; (2) Masih dapat digunakan kembali untuk kebutuhan mencetak Informasi dengan klasifikasi yang sama	(1) Memperhatik an masa retensi Informasi yang disetujui oleh pemilik Informasi; (2) Dihancurkan dengan metode pemusnahan dan Informasi tidak dapat diakses kembali (dihancurkan secara fisik atau *secure format*)
Pengamanan pada komputer penyimpan Informasi	Tidak diperlukan penanganan khusus	(1) *Screen saver lock* harus aktif jika meninggalkan komputer / terminal; dan (2) *Sign-off* komputer / terminal jika tidak digunakan atau pulang kerja.	(1) *Screen saver lock* harus aktif jika meninggalkan komputer / terminal; dan (2) *Sign-off* komputer / terminal jika tidak digunakan atau pulang kerja; dan (3) File perlu dienkripsi / *password*
Kehilangan atau kebocoran Informasi	Tidak diperlukan penanganan khusus	Harus dilaporkan kepada pemilik Informasi	Harus dilaporkan kepada pemilik Informasi dan Dinas

10. Informasi yang dianggap kritikal oleh Perangkat Daerah harus di *backup* secara memadai untuk menjamin ketersediaannya.
11. Hal yang perlu dipertimbangkan dalam proses *backup* Informasi meliputi:
    11.1 pemilik Informasi bertanggung jawab untuk menentukan Informasi yang membutuhkan *backup*, frekuensi dan metode *backup* serta waktu retensi untuk setiap *backup* Informasi yang ada;

11.2 pernyataan formal terkait Informasi yang dibutuhkan untuk di-*backup* beserta metode dan frekuensi dari *backup* harus ditentukan bersama dengan personil yang bertugas melaksanakan proses *backup* serta harus dinyatakan secara jelas dalam sebuah rencana *backup* resmi;

11.3 *backup* Informasi harus disimpan sesuai dengan masa retensi dari Informasi utama;

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

11.5 perlindungan terhadap *backup* Informasi harus dilakukan berdasarkan klasifikasi dari Informasi utama.

12. Pemerintah Daerah menyediakan akses internet dan email kepada pegawainya hanya untuk kebutuhan pekerjaan dan operasional Pemerintah Daerah.

13. Ketentuan dalam penggunaan internet dan email adalah sebagai berikut:

13.1 pengguna dilarang menggunakan akses internet dan email Perangkat Daerah untuk kegiatan melanggar hukum dan aktifitas yang dapat membahayakan keamanan jaringan Pemerintah Daerah;

13.2 pengguna dilarang untuk menggunakan akses internet dan email Perangkat Daerah untuk mengakses, mendistribusikan, mengunggah dan/atau mengunduh:

13.2.1 materi pornografi;

13.2.2 materi bajakan seperti, perangkat lunak, file musik dan video/film;

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

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

14. Pengguna disarankan untuk tidak membagi Informasi pribadi melalui situs internet atau media sosial.

15. Pengguna dilarang untuk mendistribusikan Informasi Pemerintah Daerah yang bersifat rahasia tanpa izin dari pemilik Informasi.

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

17. Dinas yang mengelola akun email Perangkat Daerah berhak untuk memblokir akun email Perangkat Daerah pada saat terdapat bukti memadai terkait penyalahgunaan dan/atau pelanggaran keamanan.
18. Pertukaran Media Informasi secara Fisik

    Kepala Perangkat Daerah perlu menyusun dan menetapkan peraturan terkait pertukaran informasi yang tidak menggunakan perangkat komunikasi elektronik misalnya melalui jasa pengantar media informasi melalui transportasi untuk melindungi informasi di dalam media terhadap akses yang tidak sah, penyalahgunaan dan kerusakan ketika pengiriman.

BAB VII
PENGENDALIAN AKSES

A. Tujuan

Tujuan dari pengendalian akses adalah untuk:

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

B. Ruang Lingkup

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

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

C. Kebijakan

1. Persyaratan Pengendalian akses pada suatu sistem meliputi:
   - 1.1 akses ke aset informasi serta aset pengolahan dan penyimpanan informasi dalam lingkungan Pemerintah Daerah harus dikendalikan menggunakan metode pengendalian akses yang memadai;
   - 1.2 pemberian hak akses dikelola secara formal pada seluruh siklusnya, mulai dari proses pengajuan, persetujuan serta pencabutan, serta dilaksanakan oleh para pihak terkait sesuai jenjang kewenangannya;
   - 1.3 pengguna yang mengakses sistem informasi dalam lingkungan Pemerintah Daerah diharuskan untuk mengotentikasi dirinya dengan menggunakan kombinasi *user ID* dan informasi otentikasi pribadi seperti *password* atau PIN;
   - 1.4 pengembangan aturan pemberian akses perlu mempertimbangkan:
     - 1.4.1 klasifikasi dari informasi;
     - 1.4.2 kritikalitas dari aset yang digunakan untuk mendukung operasional bisnis;
     - 1.4.3 prasyarat hukum perundang-undangan, kontraktual serta keamanan yang relevan;
     - 1.4.4 didasarkan atas prinsip *need to know* dan *need to use*, yaitu disesuaikan dengan kebutuhan pekerjaan dan operasional dalam lingkungan Pemerintah Daerah;

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

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

1.7 peninjauan terhadap hak akses pengguna harus didokumentasikan secara formal; dan

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

2. Pengendalian akses jaringan di lingkungan Perangkat Daerah meliputi:

2.1 penggunaan layanan jaringan hanya diperbolehkan secara terbatas, sesuai kebutuhan ketugasan dan kepentingan Perangkat Daerah, layanan lainnya yang tidak diperlukan harus dinon-aktifkan;

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

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

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

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

3.1 pemilik Aset Informasi harus memiliki manajemen identitas pengguna yang mencakup proses pendaftaran dan terminasi pengguna, yang di dalamnya termasuk:

3.1.1 *user ID* harus unik, melekat ke setiap individu tunggal, sehingga setiap tindakan pengguna dapat dipertanggungjawabkan;

3.1.2 tidak diizinkan menggunakan satu *User ID* yang digunakan secara bersama-sama oleh lebih dari satu individu, kecuali untuk tujuan tertentu yang sebelumnya harus mendapatkan persetujuan dari pihak berwenang; dan

3.1.3 memastikan secara berkala bahwa tidak ada *User ID* yang terduplikasi sehingga seluruh *User ID* aktif adalah sesuai dengan pegawai aktif pada Perangkat Daerah.

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

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

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

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

3.6 pemberian Informasi otentikasi suatu pengguna yang bersifat rahasia harus dilakukan melalui proses formal yang mencakup:

3.6.1 informasi otentikasi perdana yang diberikan untuk pertama kalinya adalah bersifat sementara, dimana pengguna wajib menggantinya pada kesempatan pertama mengakses Sistem atau aplikasi;

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

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

3.6.3.1 terjadinya proses kepegawaian, seperti promosi, mutasi, terminasi; dan

3.6.3.2 terjadinya perubahan struktur Perangkat Daerah.

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

3.8 hak akses khusus harus disetujui dan didokumentasikan secara formal.

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

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

3.11 apabila memungkinkan, hak akses khusus harus dialokasikan secara individual dan tidak disebarkan. Hal ini dilakukan untuk menjamin akuntabilitas dari pengguna khusus.

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

3.13 jejak audit (*log*) untuk hak akses khusus pada Sistem Informasi dalam lingkungan Perangkat Daerah harus diaktifkan.

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

4.1 pengguna harus menjaga kerahasiaan dan keamanan *password* pribadi atau kelompok serta Informasi otentikasi rahasia lainnya;

4.2 pengguna harus segera mengganti Informasi otentikasi rahasia jika terindikasi bahwa Informasi tersebut telah diketahui oleh orang lain;

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

4.4 *password* untuk mengakses sistem Informasi dalam lingkungan Perangkat Daerah harus memiliki karakteristik sebagai berikut:

4.4.1 memiliki panjang minimum 8 karakter;

4.4.2 mengandung kombinasi huruf besar, huruf kecil dan nomor;

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

4.4.4 tidak terdiri dari Informasi pribadi seperti ulang tahun pengguna, nama Perangkat Daerah atau nama pengguna;

4.5 *password* untuk mengakses Sistem Informasi dalam lingkungan Pemerintah Daerah harus diganti paling sedikit setiap 3 (tiga) bulan sekali;

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

4.7 prosedur *log in* dari sistem harus menjamin keamanan dari *password* dengan cara:

4.7.1 tidak menampilkan *password* yang dimasukkan; dan

4.7.2 tidak menyediakan pesan bantuan pada saat proses *log in* yang dapat membantu pengguna yang tidak berwenang;

4.8 pengguna wajib menggunakan *password* yang berbeda untuk keperluan ketugasan dan pribadi.

5. Pengendalian akses Sistem dan aplikasi yang dikelola oleh Perangkat Daerah meliputi:
   5.1 pemilik Aset Informasi harus memastikan bahwa Sistem dan aplikasi dibawah pengelolaannya memiliki fasilitas manajemen hak akses pengguna, manajemen *password* yang baik, serta mekanisme otentikasi pengguna yang aman;
   5.2 fasilitas manajemen hak akses pengguna harus mampu membatasi akses Informasi sesuai ketugasannya (*role based access control*);
   5.3 fasilitas manajemen *password* harus memastikan dihasilkannya *password* yang berkualitas, yaitu:
      5.3.1 menegakkan akuntabilitas pengguna melalui penggunaan *User ID* tunggal untuk setiap individu;
      5.3.2 memberikan fasilitas penggantian kata sandi mandiri;
      5.3.3 membantu memberikan rekomendasi *password* yang berkualitas;
      5.3.4 mewajibkan pengguna untuk mengganti *password* pada saat pertama kali *log in*;
      5.3.5 mewajibkan pengguna untuk mengganti *password* secara berkala;
      5.3.6 menyimpan riwayat *password* pengguna dan mencegah agar pengguna tidak menggunakan kata sandi yang sebelumnya telah digunakan;
      5.3.7 tidak menampilkan *password* saat sedang dientrikan; dan
      5.3.8 *password* disimpan dalam bentuk terlindungi (dienkripsi), demikian juga pada saat *password* di transmisikan.
      5.3.9 mekanisme otentikasi pengguna perlu dirancang agar meminimalkan peluang terjadinya akses yang tidak sah, yaitu:
         5.3.9.1 password tidak ditransmisikan melalui jaringan secara *plain text*;
         5.3.9.2 memiliki mekanisme penguncian sistem sementara sebagai perlindungan terhadap *brute force attacks*;
         5.3.9.3 adanya pencatatan terhadap seluruh upaya otentikasi yang sukses dan gagal; dan
         5.3.9.4 adanya pembatasan jumlah akses pengguna yang sama secara simultan;

5.4 parameter otentikasi pengguna disesuaikan dengan klasifikasi Aset Informasi sebagai berikut:

Parameter Otentikasi	Rahasia dan Internal	Publik
Jumlah gagal login sebelum penguncian	3	10
Durasi *timeout* sebelum terminasi sesi otomatis	5 menit	15 menit

6. Penggunaan program *utility* khusus dalam operasional sistem di lingkungan Perangkat Daerah harus mempertimbangkan keamanan sebagai berikut yaitu penggunaan program *utility* khusus seperti *registry cleaner* atau *system monitoring* yang dapat mengambil alih kendali sistem/aplikasi atau mendapatkan hak akses khusus pada Sistem/aplikasi harus sangat dibatasi berdasarkan kebutuhan operasional pengguna.
7. Perangkat Daerah yang mengelola aplikasi harus memastikan bahwa *source code* dikelola dan disimpan secara memadai baik yang dikembangkan oleh internal Perangkat Daerah maupun yang dikembangkan oleh penyedia jasa aplikasi.
8. Apabila *source code* dari penyedia jasa aplikasi tidak dapat diserahkan kepada pengelola aplikasi, Perangkat Daerah bersama penyedia jasa aplikasi tersebut harus mempertimbangkan perjanjian /kontrak untuk memastikan kelangsungan operasional sistem aplikasi jika ada pengembangan selanjutnya.
9. Pengendalian terhadap akses ke *source code* aplikasi sebagai berikut:
   9.1 untuk Sistem aplikasi yang dikembangkan secara internal dan/atau dibeli dengan *source code*, pengendalian akses harus diimplementasikan untuk mencegah akses tanpa izin ke *source code* tersebut.
   9.2 pengendalian tersebut mencakup:
      9.2.1 tidak menyimpan *source code* pada sistem operasional;
      9.2.2 menyimpan *source code* pada lokasi fisik yang aman dari ancaman akses tanpa izin maupun ancaman kerusakan karena kondisi lingkungan;
      9.2.3 membatasi akses secara fisik maupun *logical* ke *source code* program hanya kepada pengembang dan personil yang berwenang;
      9.2.4 mengimplementasikan metode *versioning* dan proses manajemen perubahan untuk menjamin integritas dari *source code* aplikasi.

BAB VIII
KRIPTOGRAFI

A. Tujuan

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

B. Ruang Lingkup

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

C. Kebijakan

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

BAB IX
KEAMANAN FISIK DAN LINGKUNGAN

A. Tujuan

Tujuan dari kebijakan keamanan fisik dan lingkungan adalah untuk:

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

B. Ruang Lingkup

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

C. Kebijakan

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

4. Pengendalian akses pengunjung ke dalam area di lingkungan Perangat Daerah harus memperhatikan keamanan fisik yang meliputi:
   4.1 kunjungan ke dalam area tersebut harus disetujui secara formal oleh pengelolaan area tersebut;
   4.2 selama kunjungan di dalam area tersebut, pengunjung harus senantiasa didampingi oleh petugas yang telah mendapatkan otorisasi;
   4.3 kartu identitas pengunjung perlu diverifikasi, disimpan oleh petugas selama kunjungan, dan dikembalikan sesudah selesai kunjungan; dan
   4.4 setiap pengunjung ke dalam area harus tercatat, mencakup jam masuk dan keluar, serta selalu dimonitor kesesuaiannya dengan rekaman CCTV.
5. Perangkat Daerah harus memperhatikan aspek pengamanan terhadap perangkat yang digunakan melalui:
   5.1 seluruh perangkat harus ditempatkan di lokasi yang aman, sedemikian rupa sehingga terlindungi dari terjadinya pencurian, akses oleh pihak yang tidak berwenang, kebakaran, air, debu, dan sebagainya;
   5.2 seluruh perangkat di dalam area harus dipelihara, diinspeksi sesuai spesifikasi perawatan berkala oleh pihak yang berwenang untuk menjamin keberlangsungan efektivitas fungsionalnya;
   5.3 pemeliharaan yang dilakukan oleh pihak ketiga, harus dilaksanakan sesuai dengan kesepakatan tingkat layanan (*service level agreement*/SLA) yang menjabarkan tingkat pemeliharaan dan kinerja yang harus dipenuhi pihak ketiga;
   5.4 bagi pemeliharaan yang tidak dapat dilakukan di lokasi kantor Perangkat Daerah, maka informasi rahasia dan kritikal yang tersimpan dalam peralatan tersebut harus dipindahkan terlebih dahulu;
   5.5 pemeliharaan perangkat yang mengharuskan dibawa dari luar area harus atas persetujuan pejabat berwenang.
   5.6 peralatan pengolahan dan penyimpanan informasi yang tidak digunakan lagi oleh Perangkat Daerah, baik karena rusak, diganti, atau karena sebab lainnya harus dipastikan tidak lagi menyimpan informasi sensitif dan kritikal; dan
   5.7 media penyimpan informasi yang sudah tidak digunakan lagi harus dihancurkan, atau dihapus isinya agar tidak bisa dibaca dan digunakan lagi oleh pihak yang tidak berwenang.
6. Khusus pengamanan area fisik di data center harus mempertimbangkan hal-hal sebagai berikut:
   6.1 seluruh perangkat harus ditempatkan di lokasi yang aman, sedemikian rupa sehingga terlindungi dari terjadinya kebakaran, kebocoran, debu, dan sebagainya;

6.2 seluruh perangkat di dalam *data center* harus dipelihara, diinspeksi sesuai spesifikasi perawatan berkala oleh pihak yang kompeten dan berwenang sesuai dengan rekomendasi dari pembuat perangkat tersebut;

6.3 *data center* harus dilengkapi dengan UPS, generator listrik cadangan, perangkat pemadam kebakaran, dan diusahakan terdapat perlindungan kejut listrik (petir, tegangan tidak stabil);

6.4 *data center* dan *disaster recovery center* dilengkapi dengan sistem sensor deteksi asap, air, suhu dan kelembaban, yang dapat terpantau;

6.5 parameter temperatur dan kelembaban berikut perlu dijaga untuk data center meliputi:

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

6.5.2 kelembaban (*Relative Humidity*/RH) antara 40% (empat puluh per seratus) - 60% enam puluh per seratus).

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

BAB X
KEAMANAN OPERASIONAL SISTEM INFORMASI

A. Tujuan

Tujuan dari kebijakan keamanan operasional sistem informasi adalah untuk:

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

B. Ruang Lingkup

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

C. Kebijakan

1. aktivitas operasional terkait fasilitas pengolahan informasi serta fasilitas komunikasi harus memiliki prosedur yang terdokumentasi dengan baik;
2. prosedur operasional tersebut harus tersedia bagi pengguna yang memerlukannya;
3. seluruh perubahan pada fasilitas pengolahan informasi yang dapat berimplikasi pada keamanan informasi, perlu diperlakukan secara terkendali, mencakup antara lain:
   3.1 menyusun perencanaan mengenai perubahan yang mungkin terjadi serta melakukan pengujian terkait terpenuhinya persyaratan keamanan;
   3.2 melakukan kajian atas implikasi keamanan informasi yang mungkin terjadi;
   3.3 mengajukan persetujuan secara formal atas perubahan yang akan dilakukan; dan
   3.4 mencatat seluruh perubahan yang telah dilakukan.
4. kinerja dan utilisasi atas fasilitas pengolahan informasi harus senantiasa dipantau dengan alat bantu peringatan dini, dioptimalkan pemanfaatannya, serta diproyeksikan kebutuhan kapasitasnya untuk masa yang akan datang.
5. untuk mengurangi risiko perubahan tanpa izin atau penyalahgunaan hak akses, pemisahan fasilitas pengembangan, pengujian, dan operasional harus dilakukan.

6. setiap sistem informasi di lingkungan Perangkat Daerah harus terlindungi dari *malware* secara memadai melalui:
   6.1 instalasi dari perangkat lunak antivirus pada sistem informasi;
   6.2 menutup akses ke website yang dapat menimbulkan ancaman kepada sistem informasi;
   6.3 program peningkatan kesadaran bagi personil organisasi untuk menangani ancaman *malware*; dan
   6.4 setiap insiden terkait dengan *malware* harus dilaporkan kepada administrator sistem dan dikategorikan sebagai insiden keamanan informasi.
7. seluruh aset informasi yang berada di dalam fasilitas pengolahan informasi wajib dilakukan *backup*, dengan persyaratan berikut:
   7.1 *backup* mencakup aplikasi, *database*, dan *system image*;
   7.2 frekuensi *backup* dilakukan secara harian, bulanan, dan tahunan;
   7.3 salinan *backup* harus disimpan secara aman sesuai dengan periode retensi. periode retensi *backup* adalah 1 (satu) tahun, dimana:
      7.3.1 *backup* harian disimpan selama 31 (tiga puluh satu) hari;
      7.3.2 backup bulanan disimpan selama 12 (dua belas) bulan;
   7.4 seluruh hasil *backup* harus dilakukan uji *restore* secara berkala;
   7.5 media *backup* disimpan pada perangkat *storage* yang terpisah dari perangkat pengolahan informasi utama;
   7.6 *backup* merupakan tanggung jawab pengelola *data center*, sedangkan pengujian *restore* merupakan tanggung jawab pemilik aset informasi;
   7.7 parameter *backup* disesuaikan dengan klasifikasi sistem sebagai berikut:

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

   7.8 sistem harus dikonfigurasi untuk melakukan pencatatan (*logging*) atas seluruh aktivitas pengguna, jaringan, sistem, aplikasi, *error* yang terjadi (*exceptions*). Pemilik aset informasi harus menganalisis *log* terkait pola-pola penggunaan yang tidak wajar.

7.9 fasilitas pencatatan *log* dan informasi *log* yang dicatat harus dilindungi dari penghapusan dan akses oleh pihak yang tidak berwenang.

7.10 semua fasilitas pemrosesan informasi yang terhubung ke jaringan internal Perangkat Daerah harus disinkronisasi dengan sumber waktu yang akurat dan telah disepakati.

7.11 proses dan prosedur untuk mengendalikan instalasi perangkat lunak pada sistem operasional harus ditetapkan dan diimplementasikan untuk memastikan terjaganya kerahasiaan, integritas dan ketersediaan informasi.

7.12 instalasi perangkat lunak harus dilakukan oleh administrator sistem yang relevan.

7.13 pemilik aset informasi wajib melakukan upaya-upaya identifikasi atas kelemahan teknis (*vulnerabilities*) dari seluruh aset informasi di bawah pengelolaannya, serta melakukan tindakan pengendalian yang sesuai untuk meminimalkan resiko atas hilangnya aset informasi. Tindakan pengendalian dapat berupa penonaktifan fitur tertentu, perbaikan/*upgrade* sistem, aplikasi, atau *patching*.

7.14 setiap sistem informasi di lingkungan Perangkat Daerah dapat dilakukan proses audit yang mencakup proses verifikasi terhadap sistem informasi dan/atau informasi Perangkat Daerah dengan mempertimbangkan sebagai berikut:

7.14.1 harus direncanakan dan dikelola dengan baik untuk meminimalisasi gangguan terhadap proses bisnis;

7.14.2 setiap proses audit yang membutuhkan akses kepada sistem informasi dan/atau informasi Perangkat Daerah harus disetujui oleh pemilik dari sistem dan/atau informasi tersebut;

7.14.3 hak akses untuk kebutuhan audit harus dibatasi hanya hak akses *read only*; dan

7.14.4 instalasi dari *tools* yang digunakan untuk proses audit hanya dapat dilakukan oleh personil yang berwenang yaitu administrator jaringan dan sistem TI di Perangkat Daerah, dan harus segera dihapus setelah proses audit telah selesai dilakukan.

BAB XI
KEAMANAN KOMUNIKASI

A. Tujuan

Tujuan dari kebijakan keamanan komunikasi adalah untuk:

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

B. Ruang Lingkup

Ruang lingkup dari kebijakan keamanan komunikasi adalah untuk:

1. pengendalian jaringan;
2. keamanan layanan jaringan;
3. pemisahan jaringan; dan
4. pertukaran informasi.

C. Kebijakan

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

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

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

BAB XII
AKUISISI, PENGEMBANGAN DAN PEMELIHARAAN SISTEM

A. Tujuan

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

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

B. Ruang Lingkup

Ruang lingkup dari kebijakan keamanan komunikasi adalah untuk:

1. persyaratan keamanan sistem informasi;
2. keamanan dalam proses pengembangan dan *support*;
3. data pengujian.

C. Kebijakan

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

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

12. Pengujian penerimaan sistem harus dilakukan sesuai dengan kriteria dan jadwal yang ditetapkan.
13. Pengamanan terhadap data hasil pengujian perlu diperhatikan sebagai berikut:
    13.1 data untuk pengujian sistem harus dipilih secara hati-hati untuk menghindari pengungkapan atau perubahan informasi sensitif oleh pihak yang tidak berhak, serta melindung dari kemungkinan kerusakan dan kehilangan informasi;
    13.2 masking data harus dilakukan apabila data operasional yang sensitif digunakan untuk keperluan pengujian;
    13.3 data operasional yang digunakan untuk keperluan pengujian harus dihapus segera setelah proses pengujian telah selesai dilaksanakan.

BAB XIII
HUBUNGAN KERJA DENGAN PEMASOK (*SUPPLIER*)

A. Tujuan

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

B. Ruang Lingkup

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

C. Kebijakan

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

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

6.4 peninjauan dari penyediaan layanan oleh *supplier* harus dilaksanakan paling sedikit satu kali dalam tiga bulan;

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

8. Ketentuan dalam pelaksanaan audit kepada pemasok sebagai berikut:

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

8.2 audit terhadap penyediaan layanan oleh *supplier* harus dilakukan paling sedikit satu kali dalam satu tahun; dan

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

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

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

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

BAB XIV
PENANGANAN INSIDEN KEAMANAN INFORMASI

A. Tujuan

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

B. Ruang Lingkup

Ruang lingkup dari kebijakan penanganan insiden keamanan informasi adalah:

1. tanggung jawab dan prosedur;
2. pelaporan atas kejadian insiden keamanan informasi; dan
3. pelaporan atas kelemahan keamanan informasi.

C. Kebijakan

1. Kejadian keamanan informasi adalah sebuah kejadian pada sistem, layanan ataupun jaringan yang dapat mengindikasikan adanya pelanggaran keamanan informasi atau kegagalan keamanan atau kejadian yang mungkin memiliki keterkaitan dengan keamanan informasi.
2. Kelemahan keamanan informasi adalah sebuah kelemahan yang teridentifikasi pada sistem, layanan atau jaringan yang dapat dieksploitasi oleh pihak yang tidak bertanggung jawab dan dapat menyebabkan pelanggaran terhadap kebijakan keamanan informasi.
3. Insiden keamanan informasi adalah kejadian keamanan informasi yang tidak diinginkan dan tidak diperkirakan dimana kejadian tersebut menimbulkan gangguan terhadap operasional bisnis dan mengancam keamanan informasi.
4. Guna memastikan proses penanganan insiden yang responsif dan efektif, perlu dikembangkan berbagai prosedur yang mencakup:
   4.1 perencanaan dan persiapan penanganan insiden;
   4.2 pemantauan, analisis, dan pelaporan atas insiden;
   4.3 pencatatan atas aktivitas penanganan insiden;
   4.4 penanganan bukti forensik;
   4.5 penilaian dan pengambilan keputusan atas insiden dan kelemahan keamanan informasi; dan
   4.6 pemulihan insiden.
5. Seluruh pegawai dan pihak ketiga wajib melaporkan berbagai kejadian insiden keamanan informasi maupun yang masih bersifat dugaan atas kelemahan keamanan informasi sesegera mungkin, sesuai prosedur pelaporan insiden yang berlaku.
6. Setiap kejadian insiden keamanan informasi harus dianalisis, diklasifikasikan,dan ditentukan skala prioritas penanganannya. Penanganan insiden beserta pemulihannya dilakukan berdasarkan klasifikasi dan prioritas yang telah ditetapkan.

7. Perangkat Daerah harus mengklasifikasikan insiden keamanan informasi untuk memprioritaskan penanganan insiden. Klasifikasi insiden tersebut adalah sebagai berikut:
   7.1 insiden keamanan informasi diklasifikasikan berdasarkan dampaknya menjadi berikut:
      7.1.1 mayor, apabila insiden tersebut menyebabkan terhentinya proses operasional pekerjaan Perangkat Daerah;
      7.1.2 minor, apabila insiden tersebut menyebabkan gangguan yang tidak menghentikan proses operasional pekerjaan Perangkat Daerah.
   7.2 insiden keamanan informasi diklasifikasikan berdasarkan tingkat kepentingannya menjadi berikut:
      7.2.1 *emergency*, apabila insiden tersebut dapat atau telah menghentikan proses operasional Perangkat Daerah dan/atau insiden tersebut mempengaruhi secara langsung pimpinan dalam lingkungan Perangkat Daerah;
      7.2.2 normal, apabila insiden tersebut tidak menghentikan proses operasional Perangkat Daerah dan/atau insiden tersebut mempengaruhi secara langsung pimpinan dalam lingkungan Perangkat Daerah.
8. Setiap insiden keamanan informasi harus ditangani dengan baik untuk mencegah meluasnya insiden, untuk memulihkan layanan atau informasi yang mungkin hilang dan untuk meminimalisasi dampak dari insiden.
9. Setiap tindakan yang diidentifikasi untuk menangani kejadian, kelemahan dan insiden keamanan informasi harus dikonsultasikan kepada Dinas dan/atau personil yang kompeten dan relevan dengan kejadian, kelemahan dan insiden keamanan informasi.
10. Setiap tindakan penanganan kejadian, kelemahan dan insiden keamanan informasi harus didokumentasikan dengan baik.

BAB XV
KELANGSUNGAN USAHA (*BUSINESS CONTINUITY*)

A. Tujuan

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

B. Ruang Lingkup

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

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

C. Kebijakan

1. Perangkat Daerah harus menetapkan, mendokumentasikan, mengimplementasikan dan memelihara proses, prosedur dan kontrol yang diperlukan untuk menjamin keberlanjutan keamanan informasi sesuai prasyarat yang telah ditetapkan pada saat dan setelah terjadinya gangguan besar atau bencana.
2. Perangkat Daerah harus memverifikasi kontrol keberlanjutan keamanan informasi yang telah ditetapkan dan diimplementasikan secara berkala untuk menjamin kesesuaian dan efektivitasnya pada saat dan setelah terjadinya gangguan besar atau bencana.
3. Perangkat Daerah harus menetapkan prasyarat untuk keberlanjutan keamanan informasi dan diintegrasikan dengan prasyarat keberlanjutan bisnis organisasi untuk menjamin keberlanjutan dari keamanan informasi di Perangkat Daerah, pada saat dan setelah terjadinya gangguan besar atau bencana.
4. Prasyarat keamanan informasi dapat diintegrasikan pada siklus proses *business continuity management* (BCM)yang mencakup:
   4.1 memahami kebutuhan organisasi;
   4.2 menentukan strategi BCM;
   4.3 mengembangkan dan mengimplementasikan rencana penanggulangan/keberlanjutan bisnis;
   4.4 pengujian, pemeliharaan dan peninjauan rencana penanggulangan / keberlanjutan bisnis;
5. Aspek redundansi harus ditetapkan untuk fasilitas pengolahan informasi dan sarana pendukungnya untuk memastikan ketersediaan dari proses bisnis dan operasional Perangkat Daerah serta pemberian layanan Perangkat Daerah kepada pengguna layanan.
6. Apabila prasyarat redundansi tidak dapat dipenuhi, maka proses alternatif perlu ditetapkan untuk menjamin ketersediaan dari proses bisnis dan operasional Perangkat Daerah serta pengiriman dari layanan Perangkat Daerah kepada pengguna layanan.

7. Fasilitas pengolahan informasi beserta sarana pendukungnya yang telah memenuhi aspek redundansi harus diuji secara berkala untuk menjamin kesesuaian dari fungsinya.
8. Guna menjamin ketersediaan layanan serta keamanan informasi dalam kondisi darurat (misalnya: bencana alam) pada lokasi utama, perlu adanya redundansi terhadap fasilitas pengolahan informasi yang disebut sebagai fasilitas *backup site*.
9. *Backup site* yang dimaksud dapat berupa lokasi kerja pengganti atau *disaster recovery center* (DRC) bagi alternatif area *data center*.
10. Ketentuan dalam pengelolaan terkait *Backup Site* meliputi:
    10.1 lokasi *backup site* secara geografis memiliki probabilitas kejadian bencana alam yang minimal;
    10.2 *backup site* ditujukan sebagai media penyimpanan *backup* alternatif, serta sebagai fasilitas pengolahan informasi alternatif;
    10.3 terpenuhinya pemulihan layanan operasional sepenuhnya pada fasilitas *backup site* sesuai kerangka parameter *recovery time objective* (RTO);
    10.4 pengelola *backup site* beserta Pemilik Aset Informasi melakukan uji keberlangsungan secara berkala di bawah koordinasi penanggung jawab kelangsungan bisnis, minimal 1 kali dalam setahun, untuk menguji kesiapan seluruh pihak dalam hal:
        10.4.1 memindahkan operasional ke fasilitas *backup site*;
        10.4.2 memulihkan operasional aplikasi beserta data sesuai parameter *recovery point objective* (RPO) yang telah ditetapkan.

BAB XVI
KEPATUHAN

A. Tujuan

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

B. Ruang Lingkup

Ruang lingkup dari kebijakan mengenai kepatuhan:

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

C. Kebijakan

1. Pemerintah Daerah berkomitmen untuk menjaga kepatuhan terhadap setiap prasyarat keamanan informasi yang relevan. Prasyarat keamanan informasi yang dimaksud mencakup prasyarat hukum, regulasi dan kontraktual;
2. Seluruh prasyarat hukum, regulasi dan kontraktual yang terkait dengan keamanan informasi dan berlaku bagi Perangkat Daerah harus diidentifikasikan, didokumentasikan dan dipelihara;
3. Perangkat Daerah harus mematuhi hak atas kekayaan intelektual yang terkait dengan material yang digunakan oleh Perangkat Daerah seperti:
   3.1 penggunaan perangkat lunak dan material yang bersifat *proprietary* harus mematuhi undang-undang terkait hak atas kekayaan intelektual (haki) yang berlaku;
   3.2 bukti dari lisensi atau izin resmi harus didapatkan dan disimpan untuk seluruh materi berlisensi /*copyright* yang di-*install*;
   3.3 lisensi yang bersifat berlangganan/harus diperbaharui dalam jangka waktu tertentu, harus dikelola untuk memastikan penggunaannya secara legal dan berkesinambungan; dan
   3.4 penggunaan lisensi dari materi berlisensi/*copyright* harus dikendalikan dengan baik.
4. Dokumen-dokumen penting Perangkat Daerah harus dilindungi dari kehilangan, pemalsuan, kerusakan, atau penyalahgunaan sesuai dengan peraturan perundangan-undangan, regulasi, dan persyaratan kontrak dan bisnis;
5. Perangkat Daerah harus memastikan privasi dan perlindungan terhadap informasi terkait dengan pribadi (*personally identifiable information*) sesuai dengan prasyarat hukum, perundangan, regulasi dan kontraktual;

6. Kepala Perangkat Daerah harus secara rutin memantau dan meninjau kepatuhan dari personil, proses kerja dan pemrosesan informasi dalam area tanggung jawabnya terhadap kebijakan dan standar keamanan informasi Perangkat Daerah serta prasyarat keamanan informasi yang berlaku;
7. Pada saat terjadi ketidaksesuaian, Kepala Perangkat Daerah bertanggung jawab untuk menangani ketidaksesuaian yang terjadi sesuai dengan kebijakan terkait penanganan ketidaksesuaian dan peningkatan SMKI;
8. Sistem informasi Perangkat Daerah harus ditinjau untuk menganalisis kepatuhan teknis dengan kebijakan dan standard keamanan yang berlaku serta dengan prasyarat keamanan informasi yang relevan dan berlaku, paling tidak satu kali dalam satu tahun;
9. Apabila diperlukan, peninjauan tersebut dapat melibatkan personil yang memiliki kualifikasi di bidang keamanan informasi untuk mendapatkan pemahaman yang mendalam mengenai risiko keamanan informasi yang mungkin muncul dari pengecualian tersebut.

BUPATI SUBANG,

ttd.

RUHIMAT

Salinan sesuai dengan aslinya
KEPALA BAGIAN HUKUM,

YOYON KARYONO, SH., M.H.
Pembina Tk. I (IV/b)
NIP. 19680416 200212 1 003