SALINAN

BUPATI SUMEDANG
PROVINSI JAWA BARAT

PERATURAN BUPATI SUMEDANG

NOMOR 87 TAHUN 2022

TENTANG

SISTEM MANAJEMEN KEAMANAN INFORMASI

DENGAN RAHMAT TUHAN YANG MAHA ESA

BUPATI SUMEDANG,

Menimbang : a. bahwa dalam rangka melindungi kerahasiaan, keutuhan dan ketersediaan aset informasi di lingkungan Pemerintah Daerah Kabupaten Sumedang dari berbagai ancaman keamanan informasi baik dalam maupun luar, perlu melakukan pengelolaan keamanan informasi;

b. bahwa untuk memberikan pedoman dalam pengelolaan sistem manajemen keamanan informasi secara terpadu untuk memastikan terjaganya kerahasiaan (*confidentiality*), keutuhan (*integrity)* dan ketersediaan (availability), perlu dibentuk Peraturan Bupati;

c. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b, perlu menetapkan Peraturan Bupati tentang 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 Propinsi Djawa Barat (Lembaran Negara Republik Indonesia Tahun 1968 Nomor 31, Tambahan Lembaran Negara Republik Indonesia Nomor 2851);

2. Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi (Lembaran Negara Republik Indonesia Tahun 1999 Nomor 154, Tambahan Lembaran Negara Republik Indonesia Nomor 3881) sebagaimana telah diubah 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);

3. Undang-Undang ...

3. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843) sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251, Tambahan Lembaran Negara Republik Indonesia Nomor 5952);
4. Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 61, Tambahan Lembaran Negara Republik Indonesia Nomor 4846);
5. Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik (Lembaran Negara Republik Indonesia Tahun 2009 Nomor 112, Tambahan Lembaran Negara Republik Indonesia Nomor 5038);
6. Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 244, Tambahan Lembaran Negara Republik Indonesia Nomor 5587) sebagaimana telah diubah beberapa kali, terakhir dengan Undang-Undang Nomor 11 Tahun 2020 tentang Cipta Kerja (Lembaran Negara Republik Indonesia Tahun 2020 Nomor 245, Tambahan Lembaran Negara Republik Indonesia Nomor 6573);
7. Undang-Undang Nomor 30 Tahun 2014 tentang Administrasi Pemerintahan (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 294, Tambahan Lembaran Negara Republik Indonesia Nomor 5601) sebagaimana telah diubah 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);
8. 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);
9. Peraturan Pemerintah Nomor 71 Tahun 2019 Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185, Tambahan Lembaran Negara Republik Indonesia Nomor 6400);
10. Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi (Berita Negara Republik Indonesia Tahun 2016 Nomor 1308);

11. Peraturan Daerah Kabupaten Sumedang Nomor 11 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Kabupaten Kabupaten Sumedang (Lembaran Daerah Kabupaten Sumedang Tahun 2016 Nomor 11) sebagaimana telah diubah dengan Peraturan Daerah Kabupaten Sumedang Nomor 17 Tahun 2021 tentang Perubahan atas Peraturan Daerah Nomor 11 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Kabupaten Sumedang (Lembaran Daerah Kabupaten Sumedang Tahun 2021 Nomor 17, Tambahan Lembaran Daerah Kabupaten Sumedang Nomor 28);
12. Peraturan Bupati Sumedang Nomor 89 Tahun 2020 tentang Pemanfaatan Sertifikat Elektronik (Berita Daerah Kabupaten Sumedang Tahun 2020 Nomor 89);
13. Peraturan Bupati Sumedang Nomor 47 Tahun 2021 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik (Berita Daerah Kabupaten Sumedang Tahun 2021 Nomor 47);
14. Peraturan Bupati Sumedang Nomor 50 Tahun 2021 tentang Manajemen Sistem Pemerintahan Berbasis Elektonik dan Audit Teknologi Informasi dan Komunikasi (Berita Daerah Kabupaten Sumedang Tahun 2021 Nomor 50);

MEMUTUSKAN:

Menetapkan : PERATURAN BUPATI TENTANG SISTEM MANAJEMEN KEAMANAN INFORMASI.

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Bupati ini yang dimaksud dengan:
1. Daerah Kabupaten adalah Daerah Kabupaten Sumedang.
2. Pemerintah Daerah Kabupaten adalah Bupati sebagai unsur penyelenggara pemerintahan daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan daerah otonom.
3. Bupati adalah Bupati Sumedang.
4. Wakil Bupati adalah Wakil Bupati Sumedang.
5. Sekretaris Daerah adalah Sekretaris Daerah Kabupaten Sumedang
6. Perangkat Daerah Kabupaten adalah unsur pembantu Bupati dan Dewan Perwakilan Rakyat Daerah dalam menyelenggarakan urusan pemerintahan yang menjadi kewenangan daerah.
7. Dinas Komunikasi dan Informatika, Persandian dan Statistik adalah Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang.

8. Informasi adalah keterangan, pernyataan, gagasan, dan tanda-tanda yang mengandung nilai, makna, dan pesan, baik data, fakta maupun penjelasannya yang dapat dilihat, didengar, dan dibaca yang disajikan dalam berbagai kemasan dan format sesuai dengan perkembangan Teknologi Informasi dan komunikasi secara elektronik ataupun non-elektronik
9. Sistem adalah suatu kesatuan yang terdiri komponen atau elemen yang dihubungkan bersama untuk memudahkan aliran Informasi, materi atau energi untuk mencapai suatu tujuan.
10. Teknologi Informasi adalah suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan/atau menyebarkan Informasi.
11. Teknologi Informasi dan komunikasi yang selanjutnya disingkat TIK adalah segala kegiatan yang terkait dengan pemrosesan, manipulasi, pengelolaan, dan pemindahan Informasi antar media.
12. Komputer adalah alat untuk memproses data elektronik, mengetik, optik, atau sistem yang melaksanakan fungsi logika, aritmatika, dan menyimpan.
13. Perangkat Lunak adalah satu atau sekumpulan program komputer, prosedur, dan/atau dokumentasi yang terkait dalam pengoperasian sistem elektronik.
14. Keamanan Informasi adalah suatu kondisi dimana terjaganya aspek kerahasiaan, integritas dan ketersediaan dari Informasi.
15. Sistem Manajemen Keamanan Informasi yang selanjutnya disingkat SMKI adalah sistem manajemen untuk membangun, mengimplementasikan, mengoperasikan, memonitor, meninjau, memelihara dan meningkatkan Keamanan Informasi berdasarkan pendekatan risiko.
16. Aset Informasi adalah unit Informasi yang dapat dipahami, dibagi, dilindungi dan dimanfaatkan secara efektif.
17. Aset Pengolahan adalah suatu perangkat baik elektronik maupun non-elektronik yang dapat digunakan untuk membuat dan menyunting Informasi.
18. Penyimpanan Informasi adalah suatu proses menyimpan Informasi dengan menggunakan media baik elektronik maupun non-elektronik.
19. Data Center/Pusat Data adalah suatu fasilitas untuk menempatkan sistem komputer dan perangkat-perangkat terkait, seperti Sistem komunikasi data dan penyimpanan data.

BAB II
PENGELOLAAN SISTEM MANAJEMEN KEAMANAN INFORMASI

Pasal 2

Pengelolaan SMKI meliputi infrastruktur komputer, jaringan, Sistem Informasi/aplikasi, dan sumber daya manusia.

BAB III
PENGAMANAN INFORMASI

Bagian Kesatu
Umum

Pasal 3

(1) Pengamanan Informasi dilakukan terhadap:
    a. Aset Informasi; dan
    b. Aset Pengolahan Informasi.
(2) Pengamanan Informasi sebagaimana dimaksud pada ayat (1) dilaksanakan dengan cara Penyimpanan Informasi.

Bagian Kedua
Aset 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.

Bagian Ketiga
Aset Pengolahan Informasi

Pasal 5

Aset Pengolahan 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.

Bagian Keempat
Penyimpanan Informasi

Pasal 6

Penyimpanan Informasi sebagaimana dimaksud dalam Pasal 3 ayat (2) menggunakan media:
a. elektronik, meliputi:
    1. server; dan
    2. media penyimpanan;
b. non-elektronik, meliputi:
    1. lemari;
    2. rak;
    3. laci;
    4. filling kabinet, dan
    5. perlengkapan kantor lainnya.

BAB IV
SUMBER DAYA

Pasal 7

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

(1) Setiap Perangkat Daerah Kabupaten 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 Kabupaten 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 ...

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 Kabupaten maupun pengguna.

BAB VI
MANAJEMEN RISIKO

Pasal 10

(1) Setiap Perangkat Daerah Kabupaten penyelenggara Teknologi Informasi wajib melakukan proses manajemen risiko dalam menerapkan SMKI.
(2) Proses manajemen risiko sebagaimana dimaksud pada ayat (1) meliputi:
a. identifikasi;
b. pengukuran;
c. pemantauan; dan
d. pengendalian atas risiko terkait penggunaan Teknologi Informasi.
(3) Manajemen risiko sebagaimana dimaksud pada ayat (2) meliputi:
a. pengembangan Sistem;
b. operasional Teknologi Informasi;
c. jaringan komunikasi;
d. penggunaan perangkat komputer;
e. pengendalian terhadap Informasi; dan
f. penggunaan pihak ketiga sebagai penyedia jasa Teknologi Informasi.
(4) Penerapan manajemen risiko harus dilakukan secara terintegrasi disetiap penggunaan operasional Teknologi Informasi pada sistem yang digunakan.
(5) Ketentuan mengenai manajemen risiko sebagaimana dimaksud pada ayat (2) tercantum dalam Lampiran II yang merupakan bagian tidak terpisahkan dari Peraturan Bupati ini.

BAB VII
MEKANISME PENYELENGGARAAN

Pasal 11

(1) Setiap Perangkat Daerah Kabupaten 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 Kabupaten harus menerapkan prinsip pengendalian terhadap aktivitas Teknologi Informasi melalui proses evaluasi dan monitoring secara berkala.
(2) Setiap Perangkat Daerah Kabupaten 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 Daerah Kabupaten 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 Komunikasi dan Informatika, Persandian dan Statistik dan didokumentasikan.

Pasal 13

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

Ditetapkan di Sumedang
pada tanggal 22 Februari 2022

BUPATI SUMEDANG,

ttd

DONY AHMAD MUNIR

Diundangkan di Sumedang
pada tanggal 22 Februari 2022

SEKRETARIS DAERAH
KABUPATEN SUMEDANG,

ttd

HERMAN SURYATMAN

BERITA DAERAH KABUPATEN SUMEDANG TAHUN 2022 NOMOR 87

Salinan sesuai dengan aslinya
KEPALA BAGIAN HUKUM SETDA
KABUPATEN SUMEDANG,

DODI YOHANDI, S.H., M.Kn.
NIP. 19650129 199803 1 001

LAMPIRAN
PERATURAN BUPATI SUMEDANG
NOMOR 87 TAHUN 2022
TENTANG
SISTEM MANAJEMEN KEAMANAN INFORMASI

BAB I
PENDAHULUAN

A. Tujuan

SMKI ini disusun sebagai arahan dan pedoman dalam pengelolaan SMKI secara terpadu serta untuk pengamanan Aset Informasi guna memastikan terjaganya 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 Kabupaten, beserta Perangkat Daerah Kabupaten pemilik aset terkait.
2. Aset Informasi adalah aset dalam bentuk:
   a. fisik, meliputi Informasi yang tercetak, tertulis dan tersimpan dalam bentuk fisik seperti di atas kertas, papan tulis, spanduk, atau didalam 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.

C. Kebijakan

1. Perangkat Daerah Kabupaten berkomitmen untuk mengembangkan, mengimplementasikan, memelihara dan meningkatkan SMKI secara berkesinambungan untuk menjamin Keamanan Informasi Perangkat Daerah Kabupaten 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 Kabupaten berkomitmen untuk mendukung pemenuhan prasyarat internal maupun eksternal Keamanan Informasi Perangkat Daerah Kabupaten yang relevan.
4. Perangkat Daerah Kabupaten berkomitmen untuk mematuhi seluruh peraturan perundang-undangan, regulasi dan kewajiban kontrak yang relevan.
5. Perangkat Daerah Kabupaten berkomitmen untuk memastikan ketersediaan dari sumber daya yang dibutuhkan oleh SMKI di Perangkat Daerah Kabupaten untuk menjamin terciptanya SMKI yang efektif dan efisien.

6. Kontrol …

6. Kontrol Keamanan Informasi beserta sasaran masing-masing kontrol ditetapkan oleh Kepala Dinas Komunikasi, Informatika, Persandian dan Statistik 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.
7. Kebijakan Keamanan Informasi harus dikomunikasikan ke seluruh pegawai dan pihak ketiga terkait melalui media komunikasi yang ada agar dipahami dengan mudah dan dipatuhi.
8. Perangkat Daerah Kabupaten berkomitmen meningkatkan kepedulian (*awareness*), pengetahuan dan keterampilan tentang Keamanan Informasi bagi pegawai, serta mitra pihak ketiga lain sejauh diperlukan.
9. Seluruh Kelemahan Keamanan Informasi yang berpotensi atau telah mengakibatkan gangguan penggunaan TIK atau gangguan Keamanan Informasi harus segera dilaporkan kepada penanggung jawab TIK terkait.
10. Seluruh pimpinan disetiap Perangkat Daerah Kabupaten bertanggung jawab menjamin kebijakan ini diterapkan dibawah pengawasannya.
11. Seluruh pegawai bertanggung jawab untuk menjaga dan melindungi keamanan Aset Informasi serta mematuhi kebijakan dan prosedur Keamanan Informasi yang telah ditetapkan.
12. Setiap pelanggaran terhadap kebijakan ini dapat dikenai sanksi administratif sesuai ketentuan peraturan perundang-undangan.
13. Setiap pengecualian terhadap kebijakan ini dan standar dan prosedur pengendalian kegiatan Teknologi Informasi harus mendapat persetujuan dari Kepala Dinas Komunikasi, Informatika, Persandian dan Statistik Kabupaten Sumedang.
14. Dokumen ini harus ditinjau paling sedikit 1 (satu) kali dalam 1(satu) tahun atau apabila terdapat perubahan signifikan dalam proses bisnis Perangkat Daerah Kabupaten untuk menjamin kesesuaian dan kecukupan dengan kondisi terkini.
15. Setiap perubahan terhadap dokumen ini harus didokumentasikan dan disetujui melalui proses manajemen perubahan.

BAB II
PEDOMAN PELAKSANAAN
SISTEM MANAJEMEN KEAMANAN INFORMASI

A. Tujuan

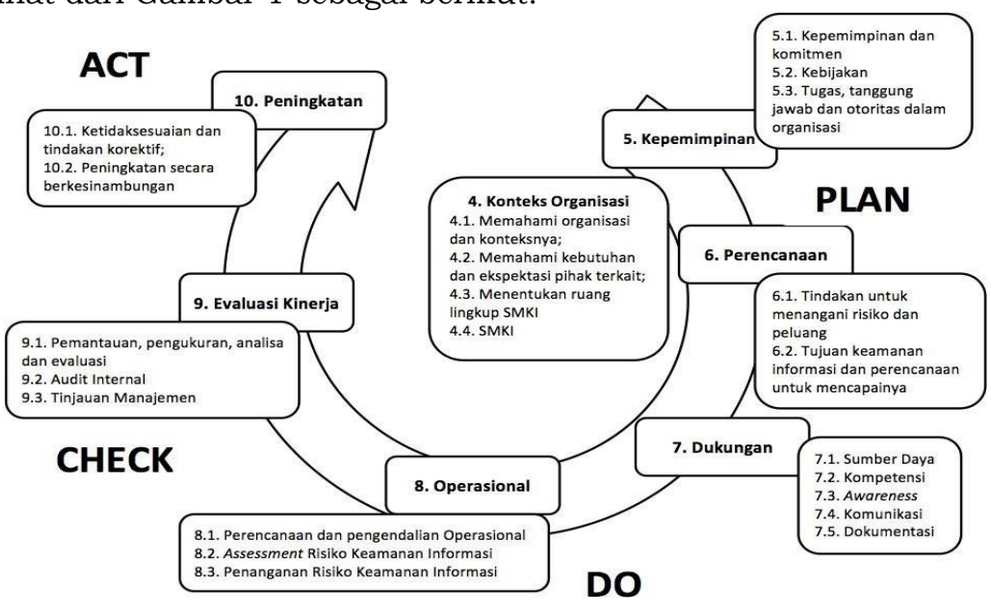
Tata kelola SMKI disusun dalam rangka untuk memastikan efektivitas dan efisiensi dari SMKI. Kerangka kerja ini akan menjabarkan proses-proses dan aktivitas-aktivitas yang harus dijalankan oleh Perangkat Daerah Kabupaten dalam rangka menetapkan, mengimplementasikan, memelihara SMKI dan meningkatkan secara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

B. Ruang Lingkup

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

C. Kebijakan

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



Gambar 1 Penggunaan siklus proses PDCA dalam proses SMKI

2. Proses perencanaan dalam pengembangan SMKI meliputi:
   2.1. Perangkat Daerah Kabupaten harus menentukan konteks dan ruang lingkup SMKI Perangkat Daerah Kabupaten dengan cara:
      a. menentukan dan secara berkala meninjau faktor serta permasalahan internal dan eksternal yang dihadapi oleh Perangkat Daerah Kabupaten yang:
         1) relevan dengan tujuan dari Perangkat Daerah Kabupaten dan SMKI; dan
         2) mempengaruhi kemampuan Perangkat Daerah Kabupaten untuk mencapai tujuan SMKI yang diharapkan oleh Perangkat Daerah Kabupaten.

b. menentukan ...

b. menentukan dan secara berkala meninjau pihak yang terkait dengan Perangkat Daerah Kabupaten dan dapat mempengaruhi SMKI di Perangkat Daerah Kabupaten;
c. menentukan dan secara berkala meninjau kebutuhan dan ekspektasi terkait Keamanan Informasi dari pihak yang terkait tersebut;
d. menentukan dan secara berkala meninjau hubungan dan ketergantungan antar proses dan aktivitas Perangkat Daerah Kabupaten yang dilaksanakan oleh pihak internal maupun pihak eksternal Perangkat Daerah Kabupaten; dan
e. menentukan dan secara berkala meninjau ruang lingkup dari SMKI di Perangkat Daerah Kabupaten.

2.2. Risiko dan peluang yang relevan dengan SMKI harus secara jelas ditentukan dan ditangani untuk:
a. memastikan bahwa SMKI mencapai tujuan yang diharapkan;
b. mencegah atau mengurangi dampak yang tidak diinginkan; dan
c. 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 Kabupaten Kabupaten, yaitu:
a. faktor dan permasalahan internal maupun eksternal yang dihadapi Perangkat Daerah Kabupaten; dan
b. ekspektasi Keamanan Informasi dari pihak terkait Perangkat Daerah Kabupaten.

3. Perencanaan harus dibuat bagi risiko dan peluang yang telah ditentukan untuk:
a. menangani risiko dan peluang;
b. mengintegrasikan dan mengimplementasikan tindakan untuk menangani risiko dan peluang dengan proses SMKI; dan
c. 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 Kabupaten 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 Kabupaten. 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 ISO 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 Kabupaten perlu mencakup Informasi terdokumentasi yang disyaratkan oleh ISO 27001:2013 yang mencakup namun tidak terbatas pada:
a. ruang lingkup SMKI;
b. kebijakan dan tujuan Keamanan Informasi;

c. metodologi ...

c. metodologi *assessment* dan penanganan risiko;
d. *statement of applicability*;
e. rencana penanganan risiko;
f. laporan *assessment* risiko;
g. pendefinisian tugas dan tanggung jawab Keamanan Informasi;
h. inventarisasi aset;
i. aturan terkait penggunaan aset;
j. kebijakan pengendalian akses;
k. prosedur operasional untuk manajemen Teknologi Informasi;
l. prinsip rekayasa Sistem secara aman;
m. kebijakan keamanan terkait penyedia jasa;
n. prosedur pengelolaan insiden;
o. prosedur keberlanjutan bisnis;
p. prasyarat hukum, regulasi dan kontraktual;
q. catatan terkait pelatihan, kemampuan, pengalaman dan kualifikasi;
r. hasil pemantauan dan pengukuran SMKI;
s. program audit internal;
t. hasil audit internal;
u. hasil dari tinjauan manajemen;
v. hasil dari tindakan korektif;
w. *log* dari aktivitas pengguna, pengecualiaan dan kejadian keamanan; dan
x. 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:
a. semua dokumentasi SMKI harus ditinjau paling sedikit satu kali dalam 1 (satu) tahun atau apabila terdapat perubahan dalam SMKI dan/atau Perangkat Daerah Kabupaten untuk menjamin kesesuaian dan kecukupannya dengan kondisi terkini SMKI dan Keamanan Informasi di Perangkat Daerah Kabupaten;
b. peninjauan harus dilakukan oleh pemilik dari dokumentasi dan dapat melibatkan pihak yang terkait dengan dokumentasi dan/atau proses yang relevan dengan dokumentasi tersebut;
c. setiap perubahan terhadap dokumentasi SMKI sebagai hasil dari peninjauan dokumentasi harus disetujui oleh manajemen yang relevan di Perangkat Daerah Kabupaten;

8.4. Terkait proses salinan, distribusi dan retensi dokumentasi, hal-hal berikut berlaku:
a. salinan dari dokumentasi SMKI harus didistribusikan kepada pihak internal yang terkait untuk memastikan operasional SMKI secara efektif;
b. akses kedokumentasi SMKI untuk pihak internal akan diberikan berdasarkan kebutuhan pengguna untuk mengakses dokumentasi tersebut (*need to know basis*);

c. 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;
d. daftar distribusi harus ditetapkan dan dipelihara untuk mengendalikan distribusi dari dokumentasi SMKI; dan
e. kecuali diputuskan berbeda, seluruh dokumen SMKI memiliki masa retensi selama 10 tahun.

9. Instansi harus mempertimbangkan penyediaan sumber daya dalam melaksanakan SMKI yang mencakup:
   9.1. Ketersediaan sumber daya yang dibutuhkan bagi pelaksanaan SMKI Perangkat Daerah Kabupaten 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 Kabupaten; dan
   9.4. Pelatihan dan program peningkatan kesadaran terkait dengan SMKI dan Keamanan Informasi Perangkat Daerah Kabupaten akan dilakukan secara berkala bagi seluruh pengguna Sistem Informasi Perangkat Daerah Kabupaten. 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:
    a. efektivitas alur pertukaran Informasi dalam Perangkat Daerah Kabupaten SMKI dan/atau dari dan ke pihak eksternal;
    b. tidak ada kebocoran Informasi sensitif milik Perangkat Daerah Kabupaten;
    c. alur komunikasi SMKI mencakup:
       1) komunikasi tatap muka;
       2) surat dan memo internal;
       3) email;
       4) website Perangkat Daerah Kabupaten;
       5) pengumuman Perangkat Daerah Kabupaten; dan
       6) material cetak.
    d. personil Perangkat Daerah Kabupaten yang tidak ditunjuk untuk memberikan materi Informasi tidak diperbolehkan untuk memberikan Informasi apapun;
    e. informasi terkait dengan SMKI dan/atau Keamanan Informasi yang berasal dari sumber eksternal harus dikirimkan kepada Dinas Komunikasi, Informatika, Persandian dan Statistik untuk peninjauan dan pendistribusian kepada pihak yang relevan dalam SMKI. Hal ini mencakup:
       1) penerbitan peraturan perundang-undangan yang baru maupun perubahan terhadap peraturan lama;
       2) usulan perubahan terhadap prasyarat Keamanan Informasi; dan

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 dokumentasikan dan dikomunikasikan kepada pihak yang terkait dengan SMKI. Proses pengendalian operasional SMKI adalah proses yang dilakukan untuk memastikan pelaksanaan operasional SMKI Perangkat Daerah Kabupaten 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 Kabupaten.
12. Metode untuk mencegah, mendeteksi dan menindak lanjuti 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 Kabupaten adalah aktivitas periodik yang dilakukan untuk mengevaluasi kinerja Keamanan Informasi dan efektivitas SMKI Perangkat Daerah Kabupaten. 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 Kabupaten;
    13.2. Proses pengukuran tersebut mencakup proses-proses berikut:
        a. Penentuan dari metrik pengukuran;
        b. Pengukuran dari metrik yang telah ditentukan;
        c. Analisis dan evaluasi dari hasil pengukuran.
    13.3. Dalam menentukan metrik pengukuran, harus mempertimbangkan aspek:
        a. sasaran SMKI yang diberikan pada kebijakan SMKI Perangkat Daerah Kabupaten;
        b. kontrol Keamanan Informasi yang diimplementasikan;
        c. metode dalam mengumpulkan data dan mengkalkulasi metrik;
        d. target pencapaian dari metrik;
        e. jadwal untuk melakukan pengukuran; dan
        f. 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 Kabupaten;
    13.9. Hasil dari proses pemantauan dan pengukuran efektivitas SMKI harus dianalisis dan dievaluasi untuk menentukan apakah implementasi dan operasi SMKI Perangkat Daerah Kabupaten:

a. sesuai dengan kebijakan, tujuan, standar dan prosedur SMKI Perangkat Daerah Kabupaten ;
b. memadai untuk menghadapi kebutuhan dan tantangan bisnis serta teknologi terkini; dan
c. sesuai dengan rencana SMKI yang sudah dibuat.

14. Peninjauan Keamanan Informasi secara independen harus secara rutin dilakukan.
    14.1. Peninjauan tersebut harus mencakup:
        a. kontrol dan area Keamanan Informasi, seperti keamanan fisik, jaringan atau akses *logical*;
        b. kebijakan, proses dan prosedur yang relevan dengan SMKI;
        c. kepatuhan implementasi SMKI dan Keamanan Informasi dengan kebijakan, proses dan prosedur Keamanan Informasi Perangkat Daerah Kabupaten serta prasyarat hukum, peraturan perundangan-undangan serta kewajiban kontraktual terkait dengan SMKI;
        d. 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 Kabupaten harus melakukan proses audit internal dengan ketentuan sebagai berikut:
    15.1. Audit internal SMKI di Perangkat Daerah Kabupaten 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 Kabupaten;
    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:
        a. 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 Kabupaten;
        b. minor, ketidaksesuaian ini mengindikasikan sebuah kealpaan/problem 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 Kabupaten; dan
        c. 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 ketidak sesuaian 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 Kabupaten dan dikomunikasikan kepada Dinas Komunikasi, Informatika, Persandian dan Statistik;
15.10. Dinas Komunikasi, Informatika, Persandian dan Statistik dan auditor internal SMKI bertanggung jawab untuk memantau dan memverifikasi koreksi, tindakan korektif maupun peningkatan terkait ketidak sesuaian 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:
a. proses pengelolaan insiden Keamanan Informasi;
b. peninjauan internal SMKI;
c. proses audit internal SMKI;
d. proses pemantauan dan pengukuran SMKI;
e. peninjauan dan/atau proses audit eksternal terhadap SMKI atau Keamanan Informasi; dan
f. laporan dan masukan dari stakeholder yang terkait.
16.2. Setiap ketidak sesuaian yang terjadi, harus ditangani secara tepat dengan cara:
a. melakukan koreksi yang sesuai untuk mengendalikan dan memperbaiki ketidak sesuaian yang telah diidentifikasi; dan
b. menangani 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:
a. peninjauan terhadap ketidaksesuaian yang terjadi;
b. menentukan penyebab dari ketidaksesuaian;
c. 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 ...

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 Dinas Komunikasi, Informatika, Persandian dan Statistik 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:
    a. proses pengelolaan insiden Keamanan Informasi;
    b. peninjauan internal SMKI;
    c. proses audit internal SMKI;
    d. proses pemantauan dan pengukuran SMKI;
    e. peninjauan dan/atau proses audit eksternal terhadap SMKI atau Keamanan Informasi; dan
    f. 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
MANAJEMEN RISIKO

A. Tujuan

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

B. Ruang Lingkup

Ruang lingkup dari manajemen risiko memastikan Perangkat Daerah Kabupaten 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 Kabupaten terhadap penanganan risiko yang harus dilakukan.
2. Perangkat Daerah Kabupaten 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:
   a. kegiatan utama yang dilakukan oleh Perangkat Daerah Kabupaten;
   b. kebijakan internal Perangkat Daerah Kabupaten;
   c. Proses bisnis Perangkat Daerah Kabupaten;
   d. kewajiban hukum, peraturan perundangan-undangan dan kewajiban kontrak yang dimiliki oleh Perangkat Daerah Kabupaten; dan
   e. kondisi Teknologi Informasi dan Keamanan Informasi, baik internal maupun eksternal yang relevan dengan Perangkat Daerah Kabupaten.
3. Perangkat Daerah Kabupaten 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:
      a. mengidentifikasi ancaman, merupakan aktifitas untuk mengidentifikasi ancaman terhadap risiko Keamanan Informasi;
      b. ancaman didefinisikan sebagai potensi penyebab insiden yang tidak diinginkan yang dapat menyebabkan kerusakan/kerugian bagi Perangkat Daerah Kabupaten dan sistemnya;
      c. sebuah ancaman tidak dapat dikatakan sebuah risiko apabila tanpa kombinasi dengan kelemahan yang dapat dieskplotasi;
      d. mengidentifikasi kelemahan dilakukan setelah pengidentifikasian ancaman dilakukan;

e. kelemahan ...

e. kelemahan didefinisikan sebagai potensi kekurangan pada proses dan kontrol keamanan yang dapat dieksplotasi oleh satu ancaman atau lebih;
f. mengidentifikasi dampak merupakan aktifitas yang dilakukan untuk mengidentifikasi potensi dampak jika ancaman yang teridentifikasi, mengeksploitasi kelemahan yanga da;
g. risiko harus dialokasikan kepemilik risiko; dan
h. pemilik risiko bertanggung jawab untuk mengelola risiko yang telah teridentifikasi.

3.2 Analisis risiko:
a. menilai dampak potensial yang akan terjadi apabila risiko yang teridentifikasi terwujud;
b. kriteria dampak merupakan parameter untuk menentukan tingkat kerugian terhadap risiko yang terjadi.

Contoh kriteria dampak adalah sebagai berikut:

Tabel 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.	Tidak ada dampak terhadap reputasi Perangkat Daerah Kabupaten
2 (Sedang)	Penundaan proses bisnis 1 hari	Pelanggaran ringan dengan surat peringatan	Berdampak pada kebocoran atau kehilangan Aset Informasi yang bersifat publik.	Mengganggu kepercayaan sebagian kecil pihak eksternal. Berdampak pada reputasi Perangkat Daerah Kabupaten namun reputasi dapat dipulihkan dalam waktu tidak terlalu lama.
3 (Berat)	Penundaan proses bisnis 3 hari	Pelanggaran sedang yang dikenakan sanksi administratif	Berdampak pada kebocoran atau kehilangan Aset informasi yang bersifat terbatas.	Mengganggu kepercayaan sebagian besar pihak eksternal. Berdampak pada reputasi Perangkat Daerah Kabupaten dan pemulihan reputasi membutuhkan waktu yang lama.

4 (Sangat Berat)	Penundaan lebih dari 3hari	Pelanggaran berat dengan sanksi hukum	Berdampak pada kebocoran atau kehilangan Aset Informasi yang bersifat rahasia.	Mengganggu kepercayaan sebagian besar pihak eksternal, Berdampak pada reputasi Perangkat Daerah Kabupaten dan sangat sulit dilakukan pemulihan reputasi.

c. menilai kemungkinan realistis terjadinya risiko yang teridentifikasi; dan
d. Kriteria kecenderungan merupakan parameter untuk menentukan tingkat kejadian terhadap Risiko.

Contoh kriteria kecenderungan adalah sebagai berikut:

Tabel 1 Tabel Kecenderungan Risiko SMKI

Nilai	Tingkat	Kriteria Kecenderungan
		Frekuensi terjadinya
1	Rendah	Kejadian tidak lebih dari 2 kali/tahun
2	Sedang	Kejadian lebih dari 2 kali/tahun, namun
3	Tinggi	Kejadian lebih dari 5 kali/tahun, namun tidak lebih dari 10 kali/tahun
4	Ekstrim	Kejadian lebih dari 10 kali/tahun

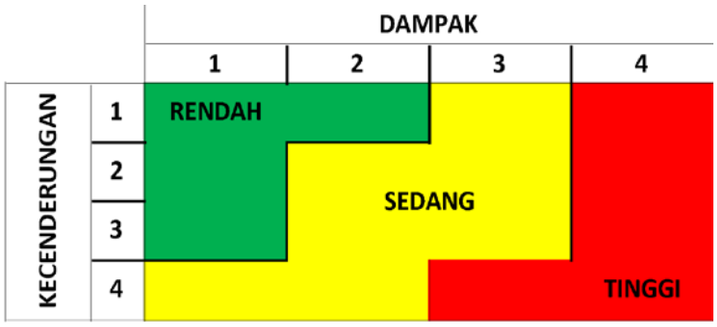
e. Evaluasi risiko:
   1) Membandingkan hasil analisis risiko dengan kriteria risiko yang sudah ditetapkan;
   2) Risiko yang masuk dalam kriteria penerimaan risiko akan diterima;
   3) Risiko yang tidak masuk dalam kriteria penerimaan risiko perlu mendapatkan penanganan; dan
   4) Setiap penanganan 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 kecenderungan yang menghasilkan tingkat risiko.

   Contoh table risiko adalah sebagai berikut:

   Tabel 1 Nilai Risiko SMKI



5. Dalam hal risiko tersebut tidak dapat diterima, Perangkat Daerah Kabupaten harus menerapkan penanganan risiko yang diperlukan yang mencakup:
   a. mengendalikan/*control* adalah merupakan tindakan pengendalian risiko dengan mengurangi dampak maupun kemungkinan terjadinya risiko melalui menerapkan suatu sistem atau aturan;
   b. menghindari/*avoid* adalah tindakan pengendalian risiko dengan tidak melakukan suatu aktivitas atau memilih aktivitas lain dengan *output* yang sama untuk menghindari terjadinya risiko; dan
   c. 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 Kabupaten terkait.
10. Perangkat Daerah Kabupaten harus melakukan proses pemantauan dan peninjauan risiko untuk memastikan efektifitas kontrol yang dilakukan yang mencakup:
    a. proses pemantauan dan peninjauan risiko adalah proses berkesinambungan untuk memastikan bahwa:
       1) risiko baru telah terindentifikasi, di-*assess* dan ditangani;
       2) setiap perubahan terhadap risiko yang sudah ada telah teridentifikasi, di-*assess* dan ditangani; dan
       3) kontrol keamanan yang sudah ada telah memadai dan efektif dalam menangani risiko;
    b. proses pemantauan dan peninjauan risiko harus dilakukan secara formal dan rutin; dan
    c. Perangkat Daerah Kabupaten harus menentukan frekuensi pemantauan dan peninjauan risiko.
11. Perangkat Daerah Kabupaten 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:
    a. 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;
    b. Setiap Informasi, aktivitas dan keputusan harus dikomunikasikan dan dikoordinasikan dengan pemiliki risiko, personil terkait dan Kepala Perangkat Daerah Kabupaten; dan
    c. Setiap komunikasi dan koordinasi eksternal terkait risiko Keamanan Informasi dan manajemen risiko harus disetujui oleh Kepala Perangkat Daerah Kabupaten.

BAB IV
SISTEM MANAJEMEN KEAMANAN INFORMASI

A. Tujuan

SMKI dengan tujuan sebagai berikut:

1. sebagai pedoman dalam pengelolaan Keamanan Informasi serta hubungan kerja dengan pihak eksternal;
2. menumbuhkan kesadaran pada SDM Pemerintah Daerah Kabupaten tentang arti penting Keamanan Informasi;
3. memastikan Keamanan Informasi terkait penggunaan perangkat; dan
4. *mobile* dan pelaksanaan aktivitas *teleworking*.

B. Ruang Lingkup

Ruang lingkup terkait dengan SMKI ini mengatur mengenai:

1. hubungan kerja dengan pihak berwenang, komunitas Keamanan Informasi dan pihak ketiga; dan
2. penggunaan perangkat *mobile* dan teknologi *teleworking*.

C. Kebijakan

1. Pengelolaan Data Center di Lingkungan Pemerintah Daerah Kabupaten ditetapkan dengan Keputusan Bupati.
2. Pengelola Data Center tersebut berkewajiban melakukan pengamanan dan pemeliharaan berkelanjutan atas aset pengolahan serta penyimpanan Informasi yang dikelola di Data Center dan Aset Informasi yang disimpan di Data Center.
3. Aset Informasi yang merupakan isi (*content*) dari sistem Informasi yang dimilikioleh Perangkat Daerah Kabupaten, dikelola oleh Perangkat Daerah Kabupaten masing-masing sesuai kepemilikannya (*ownership*).
4. Penanggung jawab Pemilik Aset Informasi adalah Kepala Perangkat Daerah Kabupaten. Pemilik Aset Informasi bertanggung jawab melakukan pengamanan dan pemeliharaan secara berkelanjutan atas Aset Informasi.
5. Perangkat Daerah Kabupaten harus menentukan tim Keamanan Informasi yang mempunyai tanggung jawab dalam berkoordinasi dengan pihak lain:
   a. mengidentifikasi pihak berwenang terkait Keamanan Informasi pada tingkat pemerintahan yang lebih tinggi (Kementerian Komunikasi dan Informatika, penegak hukum, *Indonesia security incident response team on internet infrastructure* (*idsirtii*) dan sebagainya) serta menjalin kerjasama dalam rangka pelaporan dan koordinasi penanganan bersama atas gangguan Keamanan Informasi;
   b. tim Keamanan Informasi wajib berpartisipasi dalam keanggotaan komunitas atau forum yang relevan terkait Keamanan Informasi sebagai sarana meningkatkan keterampilan dan pengetahuan serta *best practice* terkini atas Keamanan Informasi; dan
   c. seluruh anggota Tim Keamanan Informasi dan pihak ketiga wajib menandatangani Perjanjian Kerahasiaan (*Non-Disclosure Agreements*) yang mengikat para pihak untuk menjaga kerahasiaan Aset Informasi.

Kebijakan dalam penggunaan Perangkat *Mobile* dan *Teleworking:*

1. penggunaan perangkat *mobile*, baik milik pribadi atau milik Perangkat Daerah Kabupaten untuk mengakses dan/atau menyimpan Informasi milik Perangkat Daerah Kabupaten harus

sangat dibatasi sesuai dengan kebutuhan pekerjaan dengan mempertimbangkan prinsip kehati-hatian saat menggunakan perangkat *mobile* dengan menghindari meninggalkan perangkat tanpa pengawasan.

2. perangkat *mobile* harus mengaktifkan fitur otentikasi pengguna, seperti penggunaan *user name dan password,* sesuai dengan kebijakan terkait pengendalian akses.
3. Informasi sensitif harus dienkripsi atau dilindungi dengan password pada saat disimpan di mobile device, sesuai dengan klasifikasi Informasinya.
4. Informasi sensitif milik Perangkat Daerah Kabupaten yang disimpan pada perangkat *mobile device* harus di-*backup* secara berkala untuk menghindari hilangnya aspek ketersediaan dari Informasi.
5. aktivitas *teleworking* sebagai sarana pegawai untuk bekerja dari lokasi di luar area kerja Perangkat Daerah Kabupaten dengan mengakses jaringan internal secara remote melalui jaringan internet diperbolehkan namun sangat dibatasi hanya untuk personil yang diberi izin berdasarkan kebutuhan pekerjaannya.
6. akses kejaringan internal Perangkat Daerah Kabupaten dari jaringan internet harus menggunakan koneksi aman dengan menggunakan antara lain teknologi VPN.
7. kebijakan terkait teknologi *teleworking* sebagai sarana pegawai bekerja pada lokasi di luar Perangkat Daerah Kabupaten dengan mengakses jaringan internal Perangkat Daerah Kabupaten. teknologi ini diperbolehkan untuk digunakan dalam kondisi sebagai berikut:
   a. perangkat akses (misalnya komputer, *notebook*) yang digunakan untuk *teleworking* harus terinstalasi *firewall* dan antivirus;
   b. mekanisme aksester hadap Sistem atau aplikasi disesuaikan dengan klasifikasi Aset Informasi:
      1) Informasi publik : dapat diakses langsung.
      2) Informasi rahasia :
         a) harus menggunakan protokol HTTPS atau SSH; dan
         b) harus menggunakan VPN, sebelum kemudian mengakses melalui protokol HTTPS atau SSH.

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 Kabupaten Sumedang.

B. Ruang Lingkup

Ruang lingkup kebijakan keamanan sumber daya manusia terdiri dari:

1. pegawai dalam lingkungan Pemerintah Daerah Kabupaten;
2. pegawai dari pihak eksternal yang dalam aktivitas pekerjaannya memiliki akses ke Aset Informasi dan aset pengolahan dan penyimpanan Informasi dalam lingkungan Pemerintah Daerah Kabupaten.

C. Kebijakan

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

b. seluruh ...

b. seluruh hak akses Perangkat Daerah Kabupaten harus dinonaktifkan atau dihapus setelah pemberhentian kepegawaian; dan
c. seluruh hak akses Perangkat Daerah Kabupaten harus disesuaikan setelah perubahan status kepegawaian.

BAB VI
PENGELOLAAN ASET

A. Tujuan

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

B. Ruang Lingkup

Ruang lingkup kebijakan terkait pengelolaan Aset Informasi terdiri dari:

1. klasifikasi, pelabelan dan penanganan Informasi dalam ruang lingkup Peraturan Bupati Sumedang terkait SMKI; dan
2. penanganan Aset Pengolahan dan penyimpanan Informasi dalam ruang lingkup Peraturan Bupati Sumedang.

C. Kebijakan

1. Kepala Dinas Komunikasi, Informatika, Persandian dan Statistik menetapkan pemilik Aset Informasi di setiap unit Perangkat Daerah Kabupaten, beserta perangkat fisik pengolah Informasi yang terkait.
2. Pemilik Aset Informasi memiliki tanggung jawab untuk:
   a. mengidentifikasi seluruh Aset Informasi dan fasilitas pengolahan dan penyimpanan Informasi;
   b. mendokumentasikannya dalam daftar inventaris aset SMKI, serta senantiasa memperbaharui daftar inventaris aset SMKI tersebut sesuai kondisi terkini; dan
   c. memastikan bahwa setiap aset telah diklasifikasikan dan dilindungi secara memadai.
3. Aset Pengolahan dan Penyimpanan Informasi yang diinventaris adalah aset dalam bentuk:
   a. perangkat keras, meliputi perangkat keras yang digunakan untuk mengolah dan menyimpan Informasi dalam bentuk fisik maupun elektronik, yang mencakup namun tidak terbatas padakomputer, *notebook, server*, *harddisk drive,* USB *disk*;
   b. Perangkat Lunak, meliputi Perangkat Lunak yang digunakan untuk mengolah Informasi dalam bentuk elektronik, yang mencakup namun tidak terbatas pada Sistem operasi, aplikasi, dan *database*;
   c. perangkat jaringan, meliputi perangkat keras dan lunak yang digunakan untuk membentuk dan infrastruktur jaringan telekomunikasi, yang mencakup namun tidak terbatas pada hub, *switch*, *router*, *firewall*, IDS, IPS, dan *network monitoring tools*;
   d. perangkat pendukung meliputi perangkat digunakan untuk mendukung operasional perangkat pengolahan dan penyimpanan Informasi yang mencakup namun tidak terbatas pada genset, UPS, AC, rak server, lemari penyimpanan Informasi dan CCTV;
   e. 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
   f. sumber daya manusia meliputi personil baik internal maupun eksternal yang terlibat dalam pengolahan dan penyimpanan Informasi.

4. Pemilik…

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

Tabel 1 Klasifikasi Aset Informasi

Klasifikasi Aset Informasi	Deskripsi
Rahasia *(Confidential)*	Aset Informasi yang sangat peka dan berisiko tinggi yang pembocoran atau penyalahgunaan akses terhadapnya bisa mengganggu kelancaran operasional secara temporer atau mengganggu citra dan reputasi instansi.

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.

12. Untuk kepentingan penyelenggaraan pengelolaan Aset Informasi dalam Kebijakan SMKI perlu diberikan penjelasan contoh Aset Informasi rahasia dan internal, yaitu:

Tabel 2 Contoh Penjelasan Klasifikasi Aset Informasi

Klasifikasi Aset Informasi	Contoh
Rahasia *(Confidential)*	*User ID, password, Personal Identification Number(PIN), Log* sistem, hasil *penetration test,* data konfigurasi sistem, *Internet Protocol.*
Internal *(Internal Use Only)*	Panduan penggunaan sistem dan aplikasi, kebijakan dan prosedur SMKI, dokumen.

13. Setiap pemilik Informasi harus memperhatikan Keamanan Informasi yang tersimpan dalam media penyimpanan Informasi antara lain:
    a. dalam hal data yang tersimpan di dalam media bersifat rahasia, perlu diberikan proteksi kata sandi untuk melindungi data;
    b. dalam hal tidak lagi dibutuhkan atau digunakan, seluruh data yang tersimpan di dalam media harus sepenuhnya dihapus sehingga tidak lagi dapat dipulihkan;
    c. data yang tersimpan di dalam media yang akan dibuang harus mendapatkan perlakuan khusus guna meminimalkan terjadinya kebocoran Informasi kepada pihak yang tidak sah, yaitu:
        1) data yang tersimpan di dalam media yang memuat Informasi rahasia harus dibuang dengan cara dihancurkan atau dibakar; dan
        2) data yang tersimpan di dalam media yang memuat Informasilainnya harus dilakukan penghapusan total dengan cara tertentu yang tidak lagi dapat dipulihkan.
14. Panduan terkait pelabelan dan penanganan Aset Informasi berdasarkan klasifikasi Aset Informasi adalah sebagai berikut

Tabel 3 Pelabelan dan penanganan Aset Informasi

Klasifikasi Tipe	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"*	● Menggunakan 2 amplop, dimana amplop pertama dimasukkan kedalam amplop kedua; ● 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.	● Tersedia untuk personil internal PERANGKAT DAERAH KABUPATEN pemilik Informasi. ● Distribusi kepada pihak eksternal dibatasi berdasakan kebutuhan pekerjaan maupun operasional di lingkungan Pemda Kabupaten Sumedang. ● Distribusi kepada pihak eksternal perlu seijin pemilik Informasi ● Sensitifitas	● Distribusi kepada pihak eksternal sangat dibatasi untuk kebutuhan pekerjaan. ● Apabila memungkinkan, Informasi rahasia tidak disalin oleh pihak eksternal (*eyes only*). ● Distribusi kepada pihak eksternal perlu seijin pemilik Informasi. ● Sensitifitas dan kritikalitas Informasi perlu diberitahukan kepada pihak eksternal ● Pihak ketiga harus disertai perjanjian kerahasiaan (NDA - *non*

dan ...

		dan kritikalitas Informasi perlu diberitahukan kepada pihak eksternal.	*disclosure agreement*)
Pencetakan Informasi	Tidak ada pembatasan.	Dibatasi hanya untuk kebutuhan internal.	● Pencetakan hanya pada *printer* organisasi dan diusahakan tidak mencetak menggunakan jasa pencetakan eksternal
Surat menyurat internal (di dalam kantor)	Pastikan nama dan alamat tujuan sudah benar.	● Pastikan nama dan alamat tujuan sudah benar. ● Mengikuti ketentuan penggunaan amplop untuk surat internal	● Pastikan nama dan alamat tujuan sudah benar. ● Mengikuti ketentuan penggunaan amplop untuk surat internal. ● MengInformasikan kepada penerima akan pengiriman Informasi tersebut. ● Mengkonfirmasi kepada penerima
Surat menyurat eksternal (ke luar kantor)	Pastikan nama dan alamat tujuan sudah benar.	● Pastikan nama dan alamat dan tujuan sudah benar. ● Mengikuti ketentuan penggunaan amplop untuk surat eksternal. ● Menggunakan jasa kurir pengiriman tercatat dengan tanda pengiriman.	● Pastikan nama dan alamat tujuan sudah benar. ● Mengikuti ketentuan penggunaan amplop untuk surat eksternal. ● Menggunakan jasa kurir pengiriman tercatat dengan tanda pengiriman. ● Menginformasikan kepada penerima akan pengiriman

			Informasi tersebut. ● Mengkorfirmasi kepada penerima bahwa Informasi yang dikirim sudah diterima
Pengiriman ke pihak internal melalui *email*	● Pengiriman e-mail harus menggunakan akun e-mail Perangkat Daerah Kabupaten/ U nit Kerja ● Tidak diperlukan penanganan khusus.	● Pengiriman e-mail harus menggunakan akun e-mail Perangkat Daerah Kabupaten / Unit Kerja. ● Pastikan alamat email tujuan benar. ● Pengiriman Informasi, termasuk forwarding / meneruskan email hanya boleh dilakukan oleh pemilik Informasi.	● Pengiriman e-mail harus menggunaka n akun e-mail Perangkat Daerah Kabupaten /Unit Kerja ● Memberi Password pada Informasi yang dikirim melalui email ● dan password dInformasikan kepada penerima secara terpisah ● Tidak mencantumka n Informasi rahasia di *body text* e-mail ● Pengiriman Informasi, termasuk forwarding /meneruskan email hanya boleh dilakukan oleh pemilik Informasi.
Pengiriman ke pihak eksternal melalui *email*	● Pengiriman e-mail harus menggunakan akun e-mail Perangkat Daerah Kabupaten/ Unit Kerja ● Tidak diperlukan penanganan khusus.	● Pengiriman e-mail harus menggunakan akun e-mail Perangkat Daerah Kabupaten /Unit Kerja ● Pastikan alamat email tujuan sudah benar	● Tidak disarankan menggunakan e-mail untuk mengirim Informasi dengan klasifikasi ini. ● Pengiriman e-mail harus menggunakan akun e-mail Perangkat Daerah

			Kabupaten/ Unit Kerja ● Pastikan alamat email tujuan sudah benar ● Memberi password pada Informasi yang dikirim melalui email dan *password* dInformasikan 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	● Penyimpanan pada komputer atau media penyimpanan harus yang menggunakan *password*. ● *File* yang disimpan harus diberi *password.* ● 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*)	• Tidak diperlukan penanganan khusus. • Masih dapat digunakan kembali sebagai kertas untuk pekerjaan (*scrappaper*)	• Memperhatikan masa retensi Informasi yang disetujui oleh pemilik Informasi. • Masih dapat digunakan kembali untuk kebutuhan mencetak Informasi dengan klasifikasi yang sama.	• Memperhatikan masa retensi Informasi yang disetujui oleh pemilik Informasi • 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	• *Screen saverlock* harus aktif jika meninggalkan komputer / terminal. • *Sign-off* komputer / terminal jika tidak digunakan atau pulang kerja.	• *Screen saverlock* harus aktif jika meninggalkan komputer / terminal. • *Sign-off* komputer/ terminal jika tidak digunakan atau pulang kerja. • *File* perlu dienkripsi / *password*
Kehilangan atau kebocoran Informasi	Tidak diperlukan penanganan khusus.	Harus dilaporkan kepada pemilik Informasi	Harus dilaporkan kepada pemilik Informasi dan unit kerja pengelola insiden Keamanan Informasi di lingkungan Pemerintah Daerah Kabupaten

15. Informasi yang dianggap kritikal oleh Perangkat Daerah Kabupaten harus di *backup* secara memadai untuk menjamin ketersediaannya.
16. Hal yang perlu dipertimbangkan dalam proses backup Informasi meliputi:
    a. pemilik Informasi bertanggung jawab untuk menentukan Informasi yang membutuhkan *backup*, frekuensi dan metode *backup* serta waktu retensi untuk setiap *backup* Informasi yang ada;
    b. pernyataan formal terkait Informasi yang dibutuhkan untuk di-*backup* beserta metode dan frekuensi dari *backup* harus ditentukan bersama dengan personil yang bertugas

melaksanakan ...

melaksanakan proses backup serta harus dinyatakan secara jelas dalam sebuah rencana backup resmi;

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

17. Perangkat Daerah Kabupaten menyediakan akses *internet* dan *email* kepada pegawainya hanya untuk kebutuhan pekerjaan dan operasional Pemerintah Daerah Kabupaten.
18. Ketentuan dalam pengguaan internet dan email adalah sebagai berikut:
    a. pengguna dilarang menggunakan akses internet dan *email* Perangkat Daerah Kabupaten untuk kegiatan melanggar hukum dan aktifitas yang dapat membahayakan keamanan jaringan Pemerintah Kabupaten Sumedang;
    b. pengguna dilarang untuk menggunakan akses internet dan *email* Perangkat Daerah Kabupaten untuk mengakses, mendistribusikan, mengunggah dan/atau mengunduh:
        1) materi pornografi;
        2) materi bajakan seperti, perangkat lunak, *file* musik dan *video*/*film*;
        3) materi yang melecehkan, mendiskriminasikan, yang membakar emosi atau menimbulkan kebencian atau membuat pernyataan palsu atau yang bersifat merusak mengenai orang lain;
        4) situs yang dapat menimbulkan risiko serangan malware, penyusupan atau *hacking* ke jaringan Pemerintah Daerah Kabupaten.
19. Pengguna disarankan untuk tidak membagi Informasi pribadi melalui situs internet atau media sosial.
20. Pengguna dilarang untuk mendistribusikan Informasi Pemerintah Daerah Kabupaten yang bersifat rahasia tanpa izin dari pemilik Informasi.
21. Pesan penyangkalan ini harus dituliskan pada akhir setiap e-mail. “Pesan ini mungkin berisi Informasi rahasia dan hanya ditujukan kepada pihak yang dituju. Apabila anda bukanlah pihak yang dituju, anda dilarang untuk mengungkapkan, menyebarkan atau menyalin isi emai lini. Apabila anda mendapatkan email ini tanpa sengaja mohon segera hubungi pengirim email dan hapus email ini segera. Pemerintah Daerah Kabupaten tidak bertanggung jawab untuk pengiriman Informasi ini secara lengkap dan tepat dan juga tidak bertanggung jawab untuk keterlambatan dalam pengiriman email ini.”
22. Dinas Komunikasi, Informatika, Persandian dan Statistik yang mengelola akun *email* Perangkat Daerah Kabupaten berhak untuk mem-*block* akun *email* Pemerintah Daerah Kabupaten pada saat terdapat bukti memadai terkait penyalahgunaan dan/atau pelanggaran keamanan.

BAB VII
PENGENDALI 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 Kabupaten yang mencakup:

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

C. Kebijakan

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

i. setiap ...

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

atau ...

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

g. pemilik aset harus melakukan tinjauan secara berkala atas seluruh hak akses pengguna secara berkala, dengan tambahan tinjauan insidental yang dilakukan pada saat:
1) terjadinya proses kepegawaian, seperti promosi, mutasi, terminasi; dan
2) terjadinya perubahan struktur Perangkat Daerah Kabupaten.

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

i. hak akses khusus harus disetujui dan didokumentasikan secara formal.

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

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

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

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

n. jejak audit (*log*) untuk hak akses khusus pada Sistem Informasi dalam lingkungan Pemerintah Kabupaten Sumedang harus diaktifkan.

4. Setiap pengguna harus mempunyai tanggung jawab dalam penggunaan *User ID* dan *password* yaitu:
a. Pengguna harus menjaga kerahasiaan dan keamanan *password* pribadi atau kelompok serta Informasi otentikasi rahasia lainnya*;*
b. pengguna harus segera mengganti Informasi otentikasi rahasia jika terindikasi bahwa Informasi tersebut telah diketahui oleh orang lain;
c. *password* yang diberikan untuk pertama kalinya adalah bersifat sementara, dimana pengguna wajib menggantinya pada kesempatan pertama pada saat mengakses sistem atau aplikasi;
d. *password* untuk mengakses sistem Informasi dalam lingkungan Perangkat Daerah Kabupaten harus memiliki karakteristik sebagai berikut:
1) memiliki panjang minimum 8 karakter;
2) mengandung kombinasi huruf besar, huruf kecil dan nomor;
3) tidak terdiri dari kata atau nomor yang mudah ditebak seperti password, admin, 12345678 atau abc123; dan
4) tidak terdiri dari Informasi pribadi seperti ulang tahun pengguna, nama Perangkat Daerah Kabupaten atau nama pengguna;
e. *password* untuk mengakses Sistem Informasi dalam lingkungan Pemerintah Daerah Kabupaten harus diganti paling sedikit setiap 3 (tiga) bulan sekali;

f. pada ...

f. pada saat penggantian, *password* sebelumnya tidak boleh digunakan kembali sampai setelah 3 siklus pergantian *password*;
g. prosedur *log in* dari sistem harus menjamin keamanan dari *password* dengan cara:
   1) tidak menampilkan *password* yang dimasukkan; dan
   2) tidak menyediakan pesan bantuan pada saat proses *log in* yang dapat membantu pengguna yang tidak berwenang;
h. pengguna wajib menggunakan kata sandi yang berbeda untuk keperluan ketugasan dan pribadi.

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

Parameter Otentikasi	Rahasia & Internal	Publik
Jumlah gagal *log in* sebelum	3	10
Durasi *time out* sebelum	5 menit	16 menit

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

BAB VIII
KRIPTOGRAFI

A. Tujuan

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

B. Ruang Lingkup

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

C. Kebijakan

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

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 Kabupaten; dan
2. mencegah terjadinya kerusakan atau gangguan pada Aset Informasi dan aset pengolahan dan penyimpanan Informasi pada lingkungan Pemerintah Daerah Kabupaten 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 di dalamnya terdapat Informasi dan fasilitas pengolahan Informasi Perangkat Daerah Kabupaten 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 Kabupaten harus dilindungi dengan menerapkan pengamanan fisik pada perimeter area tersebut dengan kriteria:
   a. konstruksi dinding, atap dan lantai yang kuat;
   b. pintu akses menuju area harus dilengkapi dengan mekanisme kontrol akses, seperti: *access door lock*;
   c. pintu dan jendela harus senantiasa dalam kondisi terkunci, khususnya pada saat tanpa penjagaan;
   d. perangkat CCTV perlu terpasang pada sisi eksterior dan interior area;
   e. tidak diperbolehkan menyimpan bahan berbahaya yang mudah terbakar;
   f. area bongkar muat atau penerimaan barang harus diamankan dan dipantau untuk mencegah akses tanpa izin ke Data Center, disaster *recovery center* dan ruang arsip Pemerintah Daerah Kabupaten; dan
   g. 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 Kabupaten.
4. pengendalian akses pengunjung kedalam area dilingkungan Perangkat Daerah Kabupaten harus memperhatikan keamanan fisik yang meliputi:
   a. kunjungan kedalam area tersebut harus disetujui secara formal oleh pengelolaan area tersebut;
   b. selama kunjungan di dalam area tersebut, pengunjung harus senantiasa didampingi oleh petugas yang telah mendapatkan otorisasi;

c. kartu …

c. kartu identitas pengunjung perlu diverifikasi, disimpan oleh petugas selama kunjungan, dan dikembalikan sesudah selesai kunjungan; dan
d. setiap pengunjung ke dalam area harus tercatat, mencakup jam masuk dan keluar, serta selalu dimonitor kesesuaiannya dengan rekaman CCTV.

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

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

BAB 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 Kabupaten secara benar dan aman;
2. memastikan terlindunginya Aset Informasi beserta aset pengolahan dan penyimpanan Informasi di Pemerintah Daerah Kabupaten 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 Kabupaten.

B. Ruang Lingkup

Ruang lingkup dari kebijakan keamanan operasional sistem Informasi adalah pengoperasian aset pengolahan dan penyimpanan Informasi dilingkungan Pemerintah Kabupaten Sumedang.

C. Kebijakan

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

7. seluruh ...

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

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

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

b. setiap proses audit yang membutuhkan akses kepada sistem Informasi dan/atau Informasi Perangkat Daerah Kabupaten harus disetujui oleh pemilik dari sistem dan/atau Informasi tersebut;
c. hak akses untuk kebutuhan audit harus dibatasi hanya hak akses *read only*; dan
d. instalasi dari *tools* yang digunakan untuk proses audit hanya dapat dilakukan oleh personil yang berwenang yaitu administrator jaringan dan sistem TI di Perangkat Daerah Kabupaten, 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 didalam Perangkat Daerah Kabupaten maupun antar Perangkat Daerah Kabupaten 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 Kabupaten harus diamankan untuk menjamin:
   a. pencegahan akses tanpa izin kejaringan, layanan jaringan dan fasilitas pemrosesan Informasi dalam jaringan;
   b. keamanan dari Informasi milik Perangkat Daerah Kabupaten yang di kirimkan melalui jaringan; dan
   c. integritas dan ketersediaan dari layanan jaringan Perangkat Daerah Kabupaten.
2. Tugas dan tanggung jawab untuk pengelolaan jaringan dan keamanan harus dialokasikan dan apabila memungkinkan dipisahkan dari penanggung jawab opersional sistem aplikasi dan Data Center.
3. Konfigurasi dari jaringan, perangkat aktif dan perangkat keamanan jaringan harus ditinjau secara berkala untuk:
   a. memastikan kesesuaian dengan kondisi terkini; dan
   b. mengidentifikasi kerawanan pada jaringan, layanan jaringan dan fasilitas pemrosesan Informasi dalam jaringan.
4. Jaringan internal Perangkat Daerah Kabupaten harus dipisahkan dari jaringan eksternal dengan menggunakan *security gateway* atau *firewall* dan harus dikonfigurasikan untuk:
   a. memfilter *traffic* tanpa izin maupun *traffic* yang mencurigakan; dan
   b. apabila memungkinkan memfilter dan mencegah infeksi *malware* kejaringan 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 di dokumentasikan dan harus dibatasi waktunya sesuai dengan kebutuhan dari akses.

Jaringan ...

9. Jaringan internal Perangkat Daerah Kabupaten 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 Kabupaten.
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. Akseske *port* yang digunakan untuk kebutuhan diagnostik dan konfigurasi perangkat jaringan dan keamanan jaringan, seperti *console port,* harus sangat dibatasi dan diberikan kepada:
    a. Administrator jaringan dan keamanan jaringan Perangkat Daerah Kabupaten;
    b. Pihak ketiga yang telah disetujui dan bekerja untuk kepentingan Perangkat Daerah Kabupaten;
    c. Aplikasi *monitoring* jaringan dan keamanan jaringan yang telah disetujui.
18. Semua perangkat jaringan harus dapat diidentifikasi secara fisik maupun logical dengan penamaan yang disepakati dan konsisten.
19. Perangkat jaringan yang dimiliki oleh pihak eksternal harus secara memadai dipisahkan dari perangkat jaringan milik Perangkat Daerah Kabupaten.
20. Mekanisme keamanan, tingkat layanan dan prasyarat lain untuk semua layanan jaringan harus diidentifikasi dan dimasukkan kedalam perjanjian layanan jaringan.
21. Akses kelayanan jaringan Perangkat Daerah Kabupaten 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 Kabupaten.
23. Layanan jaringan Perangkat Daerah Kabupaten 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 Kabupaten harus memperhatikan perjanjian kerahasiaan merupakan perikatan formal antara pemilik Aset Informasi dengan penerima Informasi, yang ketentuan di dalamnya memuat:
    a. pemberian izin penggunaan Informasi dari pemilik Aset Informasi kepada penerima Informasi untuk keperluan dan periode waktu yang spesifik, dimana pihak penerima Informasi wajib menjaga

kerahasiaan Informasi serta mengupayakan pencegahan terjadinya kebocoran atau penyebaran Informasi secara tidak sah;

b. hak dari pemilik Aset Informasi untuk melakukan audit dan pemantauan aktivitas penerima Informasi berkaitan dengan penggunaan Informasi sensitif; dan
c. konsekuensi yang harus ditanggung penerima Informasi apabila terjadi pelanggaran atas perjanjian kerahasiaan.

BAB 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 (*life cycle)* sistem Informasi. Termasuk persyaratan untuk sistem Informasi yang menyediakan layanan melalui jaringan publik.
2. memastikan Keamanan Informasi di desain dan di implementasikan dalam siklus hidup (*life cycle*) 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 Kabupaten Kerja harus menetapkan dan mendokumentasikan secara jelas persyaratan Keamanan Informasi yang relevan sebelum pengembangan, perluasan, atau pengadaan sistem Informasi baru.
2. Persyaratan keamanan harus di identifikasi 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 Kabupaten yang ditransimisikan melalui jaringan publik (internet) harus diamankan dari aktivitas penipuan, kemungkinan adanya perselisihan kontrak, dan pengungkapan dan/atau perubahan Informasi tanpa izin.
5. Pengamanan Informasi terhadap Informasi yang ditransmisikan melalui sistem Informasi yang digunakan dapat mencakup namun tidak terbatas pada:
   a. proses otentikasi dan otorisasi terhadap pengguna aplikasi;
   b. perlindungan untuk memastikan kerahasiaan dan integritas Informasi yang dipertukarkan melalui jaringan publik;
   c. perlindungan terhadap *session* transaksi untuk menghindari duplikasi dan/atau modifikasi; dan
   d. mengamankan jalur komunikasi antara pihak-pihak yang terlibat.
6. Keamanan dalam proses pengembangan dan dukungan yang perlu dipertimbangkan oleh Perangkat Daerah Kabupaten meliputi:
   a. aturan untuk pengembangan Sistem harus ditetapkan dan di implementasikan untuk proses pengembangan Sistem di Perangkat Daerah Kabupaten yang mencakup:
      1) pengamanan dari lingkungan pengembangan, seperti pemisahan lingkungan pengembangan baik secara fisik dan/atau *logical*, pengendalian akses, pengelolaan perubahan;
      2) panduan *secure coding*;

3) pengendalian ...

3) pengendalian versi aplikasi;
4) penyimpanan dari *source code*; dan
5) metode pengujian untuk mengidentifikasi dan memperbaiki *vulnerability*.

7. Perubahan terhadap sistem selama siklus pengembangan sistem harus dikendalikan melalui proses manajemen perubahan yang berlaku di Perangkat Daerah Kabupaten;
8. Apabila platform operasional, misalnya sistem operasi, *database* dan/atau *middleware*, dari Sistem Informasi Perangkat Daerah Kabupaten mengalami perubahan, aplikasi kritikal Perangkat Daerah Kabupaten harus ditinjau dan di uji untuk memastikan tidak ada dampak buruk terhadap operasional dan keamanan Perangkat Daerah Kabupaten;
9. Perangkat Daerah Kabupaten harus menetapkan lingkungan pengembangan yang aman untuk pengembangan dan integrasi sistem Perangkat Daerah Kabupaten. Hal ini dapat mencakup namun tidak terbatas pada:
   a. pemisahan lingkungan pengembangan baik secara fisik dan /atau logical;
   b. pengendalian akses;
   c. perpindahan data dari dan kelingkungan pengembangan;
10. Perangkat Daerah Kabupaten harus mengawasi aktivitas pengembangan sistem yang dialih dayakan (*out sourced*). Hal ini dapat mencakup:
    a. perjanjian terkait lisensi dan kepemilikan Sistem;
    b. pengujian penerimaan sistem untuk menguji kualitas dan akurasi dari Sistem;
    c. prasyarat dokumentasi untuk Sistem;
    d. perjanjian dengan pihak ketiga sebagai penjamin;
    e. hak untuk melakukan audit proses pengembangan dan kontrol yang diimplementasikan oleh vendor.
11. Pengujian dari fitur keamanan Sistem harus dilakukan pada saat pengembangan Sistem Informasi Perangkat Daerah Kabupaten;
12. Pengujian ini dilakukan berdasarkan prasyarat keamanan Sistem yang telah ditetapkan;
13. Kriteria dan jadwal untuk pengujian penerimaan Sistem harus ditetapkan untuk sistem Informasi baru, *upgrade* dan versi baru dari Sistem Informasi Perangkat Daerah Kabupaten;
14. Pengujian penerimaan Sistem harus dilakukan sesuai dengan kriteria dan jadwal yang ditetapkan.
15. Pengamanan terhadap data hasil pengujian perlu diperhatikan sebagai berikut:
    a. data untuk pengujian sistem harus dipilih secara hati-hati untuk menghindari pengungkapan atau perubahan Informasi sensitif oleh pihak yang tidak berhak, serta melindungi dari kemungkinan kerusakan dan kehilangan Informasi;
    b. *masking* data harus dilakukan apabila data operasional yang sensitif digunakan untuk keperluan pengujian; dan
    c. 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 kerjadengan pemasok (*supplier*) adalah untuk memastikan perlindungan atas aset Perangkat Daerah Kabupaten dalam jangkauan akses pemasok dan memelihara tingkat layanan yang dsetujui 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 Kabupaten.

C. Kebijakan

1. Perangkat Daerah Kabupaten 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 Kabupaten harus mengikuti kriteria berikut:
   a. kompetensi, pengalaman dan catatan dari Perangkat Daerah Kabupaten;
   b. kepastian dari kemampuan penyedia jasa untuk menyediakan layanan; dan
   c. kepastian dari kemampuan penyedia jasa untuk menjaga ketersediaan dari penyediaan layanan pada saat kondisi normal atau kondisi bencana (apabila terjadi bencana alam atau kegagalan dalam penyediaan layanan);
3. Berdasarkan pengelompokan pemasok yang telah bekerja sama, Perangkat Daerah Kabupaten 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 Kabupaten 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 menanda tangani Perjanjian Kerahasiaan.
5. Kewajiban supplier dan tingkat layanan harus ditetapkan secara formal dalam kontrak kerja;
6. Perangkat Daerah Kabupaten harus memastikan pengelolaan *delivery* layanan dari pemasok dengan memperhatikan:
   a. layanan yang diserahkan kepada Perangkat Daerah Kabupaten oleh pihak *supplier* harus secara berkala dipantau, dan ditinjau;
   b. proses pemantauan dilakukan untuk memverifikasi kesesuaian dari tingkat layanan yang diberikan dan prasyarat Keamanan Informasi dengan perjanjian kerja;
   c. proses peninjauan dilakukan untuk mengidentifikasi problem terkait penyediaan layanan dan aspek Keamanan Informasi dalam penyediaan layanan oleh *supplier*; dan
   d. peninjauan dari penyediaan layanan oleh *supplier* harus dilaksanakan paling sedikit satu kali dalam tiga bulan;
7. Perangkat Daerah Kabupaten dapat melakukan audit terhadap penyediaan layanan yang diberikan pemasok;

8. Ketentuan ...

8. Ketentuan dalam pelaksanaan audit kepada pemasok sebagai berikut:
   a. tanggung jawab untuk mengaudit tingkat layanan dimiliki oleh pihak, baik internal maupun eksternal, yang memiliki independensi dari pengguna layanan yang diberikan oleh supplier dan ditunjuk secara formal;
   b. audit terhadap penyediaan layanan oleh *supplier* harus dilakukan paling sedikit satu kali dalam satu tahun; dan
   c. setiap ketidaksesuaian yang ditemukan dalam proses peninjauan dan audit harus dikelola dan ditindak lanjuti;
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 Kabupaten serta integritas dan ketersediaan dari Informasi dan layanan Perangkat Daerah Kabupaten;
11. Perubahan terhadap layanan yang diberikan oleh *supplier* harus disetujui oleh manajemen Perangkat Daerah Kabupaten 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 yangmencakup:
   a. perencanaan dan persiapan penanganan insiden;
   b. pemantauan, analisis, dan pelaporan atas insiden;
   c. pencatatan atas aktivitas penanganan insiden;
   d. penanganan bukti forensik;
   e. penilaian dan pengambilan keputusan atas insiden dan kelemahan Keamanan Informasi; dan
   f. pemulihan insiden.
5. Seluruh pegawai dan pihak ketiga wajib melaporkan berbagai kejadian insiden Keamanan Informasi maupun yang masih bersifat dugaan atas kelemahan Keamanan Informasi sesegera mungkin, sesuai prosedur pelaporan insiden yang berlaku.
6. Setiap kejadian insiden Keamanan Informasi harus dianalisis, diklasifikasikan, dan ditentukan skala prioritas penanganannya. Penanganan insiden beserta pemulihannya dilakukan berdasarkan klasifikasi dan prioritas yang telah ditetapkan.
7. Perangkat Daerah Kabupaten harus mengklasifikasikan insiden Keamanan Informasi untuk memprioritaskan penanganan insiden. Klasifikasi insiden tersebut adalah sebagai berikut:
   a. insiden Keamanan Informasi diklasifikasikan berdasarkan dampaknya menjadi berikut:
      1) mayor, apabila insiden tersebut menyebabkan terhentinya proses operasional pekerjaan Perangkat Daerah Kabupaten;

2) minor …

2) minor, apabila insiden tersebut menyebabkan gangguan yang tidak menghentikan proses operasional pekerjaan Perangkat Daerah Kabupaten.

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

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 Komunikasi, Informatika, Persandian dan Statistik 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 mengenai kelangsungan usaha (*business continuity*) adalah untuk memastikan ketersediaan layanan TIK beserta fasilitas pengolahan Informasi dalam kondisi darurat dan memulihkan layanan seperti sedia kala dalam kondisi kembali normal.

B. Ruang Lingkup

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

1. keberlanjutan Keamanan Informasi; dan
2. redundansi fasilitas pengolahan Informasi.

C. Kebijakan

1. Perangkat Daerah Kabupaten 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 Kabupaten 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 Kabupaten harus menetapkan prasyarat untuk keberlanjutan Keamanan Informasi dan diintegrasikan dengan prasyarat keberlanjutan bisnis Perangkat Daerah Kabupaten untuk menjamin keberlanjutan dari Keamanan Informasi di Perangkat Daerah Kabupaten, pada saat dan setelah terjadinya gangguan besar atau bencana.
4. Prasyarat Keamanan Informasi dapatdi integrasikan pada siklus process *business continuity management* (BCM) yang mencakup:
   a. memahami kebutuhan Perangkat Daerah Kabupaten;
   b. menentukan strategi BCM;
   c. mengembangkan dan mengimplementasikan rencana penanggulangan / keberlanjutan bisnis;
   d. 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 Kabupaten serta pemberian layanan Perangkat Daerah Kabupaten kepada pelanggan.
6. Apabila prasyarat redundan tidak dapat dipenuhi, maka proses alternatif perlu ditetapkan untuk menjamin ketersediaan dari proses bisnis dan operasional Perangkat Daerah Kabupaten serta *delivery* dari layanan Perangkat Daerah Kabupaten kepada pelanggan.
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 ...

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

BAB 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 Perangkat Daerah Kabupaten.

B. Ruang Lingkup

Ruang lingkup dari kebijakan mengenai kepatuhan:

1. kepatuhan dengan prasyarat hukum dan kontraktual; dan
2. peninjauan Keamanan Informasi.

C. Kebijakan

1. Pemerintah Daerah Kabupaten Sumedang 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 Kabupaten harus diidentifikasikan, didokumentasikan dan dipelihara;
3. Perangkat Daerah Kabupaten harus mematuhi hak atas kekayaan intelektual yang terkait dengan material yang digunakan oleh Perangkat Daerah Kabupaten seperti:
   a. penggunaan perangkat lunak dan material yang bersifat *proprietary* harus mematuhi undang-undang terkait hak atas kekayaan intelektual (haki) yang berlaku;
   b. bukti dari lisensi atau izin resmi harus didapatkan dan disimpan untuk seluruh materi berlisensi/*copyright* yang di-install;
   c. lisensi yang bersifat berlangganan/harus diperbaharui dalam jangka waktu tertentu, harus dikelola untuk memastikan penggunaannya secara legal dan berkesinambungan; dan
   d. penggunaan lisensi dari materi berlisensi/*copyright* harus dikendalikan dengan baik;
4. Dokumen penting Perangkat Daerah Kabupaten harus dilindungi dari kehilangan, pemalsuan, kerusakan, atau penyalah gunaan sesuai dengan peraturan perundangan-undangan, regulasi, dan persyaratan kontrak dan bisnis;
5. Perangkat Daerah Kabupaten 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 Kabupaten harus secara rutin memantau dan meninjau kepatuhan dari personil, proses kerja dan pemrosesan Informasi dalam area tanggung jawabnya terhadap kebijakan dan standard Keamanan Informasi Perangkat Daerah Kabupaten serta prasyarat Keamanan Informasi yang berlaku;
7. Pada saat terjadi ketidak sesuaian, pimpinan Perangkat Daerah Kabupaten bertanggung jawab untuk menangani ketidaksesuaian yang terjadi sesuai dengan kebijakan terkait penanganan ketidaksesuaian dan peningkatan SMKI;

8. Sistem ...

8. Sistem Informasi Perangkat Daerah Kabupaten harus ditinjau untuk menganalisis kepatuhan teknis dengan kebijakan dan standar keamanan yang berlaku serta dengan prasyarat Keamanan Informasi yang relevan dan berlaku, paling tidak satu kali dalam satu tahun; dan
9. Apabila diperlukan, peninjauan tersebut dapat melibatkan personil yang memiliki kualifikasi dibidang Keamanan Informasi untuk mendapatkan pemahaman yang mendalam mengenai risiko Keamanan Informasi yang mungkin muncul dari pengecualian tersebut.

BUPATI SUMEDANG,

ttd

DONY AHMAD MUNIR

Salinan sesuai dengan aslinya
KEPALA BAGIAN HUKUM SETDA
KABUPATEN SUMEDANG,

DODI YOHANDI, S.H., M.Kn.
NIP. 19650129 199803 1 001