PEMERINTAH DAERAH KABUPATEN SUMEDANG
DINAS KOMUNIKASI DAN INFORMATIKA, PERSANDIAN DAN STATISTIK
Alamat : Jl. Angkrek No.103 Sumedang, No.Tlp: (0261) 201225,
Website : diskominfosanditik.sumedangkab.go.id E-mail :
diskominfosanditik@sumedangkab.go.id , 45323

KEPUTUSAN

KEPALA DINAS KOMUNIKASI DAN INFORMATIKA, PERSANDIAN

DAN STATISTIK

Nomor : 53 Tahun 2023

Lampiran : 1 (satu) Berkas

TENTANG

PETUNJUK TEKNIS PELAKSANAAN SISTEM MANAJEMEN KEAMANAN INFORMASI MENGACU KEPADA STANDAR ISO 27001:2022 PADA DINAS KOMUNIKASI DAN INFORMATIKA, PERSANDIAN DAN STATISTIK KABUPATEN SUMEDANG

DENGAN RAHMAT TUHAN YANG MAHA ESA

KEPALA DINAS KOMUNIKASI DAN INFORMATIKA, PERSANDIAN DAN STATISTIK

Menimbang : a. Bahwa dalam rangka melindungi kerahasiaan, integritas, dan ketersediaan aset informasi Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang dari berbagai bentuk ancaman baik dari dalam maupun luar, Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang telah menetapkan sistem manajemen keamanan informasi Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang ;

Catatan :
- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

b. Bahwa berdasarkan hasil evaluasi manajemen keamanan informasi Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang yang telah ditetapkan perlu disesuaikan dengan standar ISO 27001:2022 tentang Sistem Manajemen Keamanan Informasi;

c. Bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, dan huruf b, perlu menetapkan Keputusan Kepala Dinas tentang Sistem Manajemen Keamanan Informasi Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang .

Mengingat : 1. Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Nomor 4843) sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang No 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik;

2. Undang-undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi;
3. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
4. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185, Tambahan Lembaran Negara Republik Indonesia Nomor 6400);
5. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 5 Tahun 2020 tentang Pedoman Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2020 Nomor 261);
6. Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2020 tentang Sistem Pengamanan dalam Penyelenggaraan Sistem Elektronik;

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

7. Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik Dan Standar Teknis Dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik
8. Peraturan Bupati 66 Tahun 2022 tentang Perubahan atas Peraturan Bupati Sumedang Nomor 47 Tahun 2021 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik
9. Keputusan Bupati Sumedang Nomor 67 Tahun 2022 tentang tentang Perubahan atas Peraturan Bupati Sumedang Nomor 50 Tahun 2021 tentang Manajemen Sistem Pemerintahan Berbasis Elektronik dan Audit Teknologi.
10. Keputusan Kepala Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang Nomor 45 Tahun 2023 tentang Manual Pelaksanaan Sistem Manajemen Keamanan Informasi Mengacu Kepada Standar Iso 27001:2022 Pada Dinas Komunikasi Dan Informatika, Persandian Dan Statistik Kabupaten Sumedang.

MEMUTUSKAN

Menetapkan : KEPUTUSAN KEPALA DINAS KOMUNIKASI DAN INFORMATIKA, PERSANDIAN DAN STATISTIK TENTANG PETUNJUK TEKNIS PELAKSANAAN PELAKSANAAN SISTEM MANAJEMEN KEAMANAN INFORMASI MENGACU KEPADA STANDAR ISO 27001:2022 PADA DINAS KOMUNIKASI DAN INFORMATIKA, PERSANDIAN DAN STATISTIK KABUPATEN SUMEDANG:

PERTAMA : Pengelolaan SMKI meliputi infrastruktur komputer, jaringan, Sistem Informasi/aplikasi, dan sumber daya manusia dan berpedoman pada standar ISO 27001:2022.

(1) Pengamanan Informasi dilakukan terhadap:

a. Aset Informasi; dan
b. Aset Pengolahan Informasi.

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

(2) Pengamanan Informasi sebagaimana dimaksud pada Diktum PERTAMA poin (1) dilaksanakan dengan cara Penyimpanan Informasi. Aset Informasi sebagaimana dimaksud dalam Diktum PERTAMA poin (1) 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.

Aset Pengolahan Informasi sebagaimana dimaksud dalam Diktum PERTAMA poin (1) huruf b berupa :

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

Penyimpanan Informasi sebagaimana dimaksud dalam Diktum PERTAMA poin (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.

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

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

(2) Ketentuan pelaksanaan dan uraian secara rinci SMKI sebagaimana dimaksud pada ayat (1) tercantum dalam Lampiran I yang merupakan bagian tidak terpisahkan dari Surat Keputusan Kepala Dinas ini.

KETIGA : (1) 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.

(1) Penyelenggaraan pemrosesan transaksi pada operasional Teknologi Informasi harus memenuhi prinsip kehati-hatian.

(2) penyelenggaran Teknologi Informasi wajib mengidentifikasi dan memantau aktivitas operasional Teknologi Informasi untuk memastikan efektivitas, efisiensi, dan keamanan dari aktivitas tersebut antara lain dengan:

a. menerapkan perimeter fisik dan lingkungan di area kerja dan Data Center;
b. mengendalikan hak akses secara memadai sesuai kewenangan yang ditetapkan;
c. menerapkan pengendalian terhadap Informasi yang diproses;
d. memastikan ketersediaan dan kecukupan kapasitas layanan jaringan komunikasi baik yang dikelola secara internal maupun oleh pihak lain penyedia jasa;

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

e. melakukan pemantauan kegiatan operasional Teknologi Informasi termasuk audit trail/riwayat; dan
f. melakukan pemantauan terhadap aplikasi yang digunakan oleh Perangkat Dinas Komunikasi dan Informatika, Persandian dan Statistik maupun pengguna

KEEMPAT : (1) Penyelenggara Teknologi Informasi wajib melakukan proses manajemen risiko dalam menerapkan SMKI.

(2) Proses manajemen risiko sebagaimana dimaksud pada Diktum KEEMPAT poin (1) meliputi:
a. identifikasi;
b. pengukuran;
c. pemantauan; dan
d. pengendalian atas risiko terkait penggunaan Teknologi Informasi.

(3) Manajemen risiko sebagaimana dimaksud pada ayat (2) meliputi :
a. pengembangan Sistem;
b. operasional Teknologi Informasi;
c. jaringan komunikasi;
d. penggunaan perangkat komputer;
e. pengendalian terhadap Informasi; dan
f. penggunaan pihak ketiga sebagai penyedia jasa Teknologi Informasi.

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

(5) Ketentuan mengenai manajemen risiko sebagaimana dimaksud pada ayat (2) tercantum dalam Lampiran II yang merupakan bagian tidak terpisahkan dari Surat Keputusan Kepala Dinas ini.

Catatan :
- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

KELIMA : (1) 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.

(2) Penyelenggaraan teknologi informasi harus menerapkan prinsip pengendalian terhadap aktivitas Teknologi Informasi melalui proses evaluasi dan monitoring secara berkala.

(3) Penyelenggara teknologi informasi 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.

(4) 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.

(5) Hasil dari tindakan perbaikan dan peningkatan sebagaimana dimaksud pada ayat (3) harus dilaporkan kepada Kepala Dinas Komunikasi dan Informatika, Persandian dan Statistik dan didokumentasikan.

(6) Apabila terjadi kebocoran Informasi yang mempunyai dampak luas pada Perangkat Dinas Komunikasi dan Informatika, Persandian dan Statistik terkait, maka Dinas Komunikasi dan Informatika, Persandian dan Statistik dapat menunjuk auditor independen untuk melakukan investigasi yang diperlukan.

(7) Penyelenggara Teknologi Informasi wajib menyediakan akses kepada auditor independen sebagaimana dimaksud pada ayat (1) untuk melakukan pemeriksaan seluruh aspek terkait penyelenggaraan Teknologi Informasi.

KEENAM : Keputusan Kepala Dinas Komunikasi dan Informatika, Persandian dan Statistik ini merupakan revisi dari Keputusan Kepala Dinas Komunikasi dan Informatika, Persandian dan Statistik Nomor 52 Tahun 2023 tentang Petunjuk Teknis Pelaksanaan Pelaksanaan Sistem Manajemen Keamanan Informasi Mengacu Kepada Standar

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

ISO 27001:2022 Pada Dinas Komunikasi Dan Informatika, Persandian Dan Statistik Kabupaten Sumedang.

KETUJUH : Keputusan Kepala Dinas Komunikasi dan Informatika, Persandian dan Statistik ini mulai berlaku pada tanggal ditetapkan.

Ditetapkan di : S u m e d a n g
Pada Tanggal : 07 Juli 2023

Balai Sertifikasi Elektronik

SUMEDANG
DIGITAL SIGNATURE

Ditandatangani Secara Elektronik Oleh:

BAMBANG RIANTO, S.STP, M.Si
NIP. 197704201996021001

Kepala Dinas Komunikasi dan Informatika, Persandian dan Statistik

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

Lampiran I : Surat Keputusan Kepala Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang
No : 53 Tahun 2023
Tanggal : 07 Juli 2023
Tentang : Petunjuk Teknis Pelaksanaan Pelaksanaan Sistem Manajemen Keamanan Informasi Mengacu Kepada Standar Iso 27001:2022 Pada Dinas Komunikasi Dan Informatika, Persandian Dan Statistik Kabupaten Sumedang

BAB I

PENDAHULUAN

A. Tujuan

Standar dan Prosedur 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

Standar ini berlaku untuk pengelolaan pengamanan seluruh informasi Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang yang dilaksanakan oleh Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang dan pihak ketiga baik sebagai pengelola dan/atau pengguna Teknologi Informasi dan Komunikasi (TIK).

C. Definisi

1. 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 maupun nonelektronik

Catatan :
- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

2. Sistem adalah suatu kesatuan yang terdiri komponen atau elemen yang dihubungkan bersama untuk memudahkan aliran Informasi, materi atau energi untuk mencapai suatu tujuan.
3. Teknologi Informasi adalah suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan/atau menyebarkan Informasi.
4. Teknologi Informasi dan komunikasi yang selanjutnya disingkat TIK adalah segala kegiatan yang terkait dengan pemrosesan, manipulasi, pengelolaan, dan pemindahan Informasi antar media.
5. Komputer adalah alat untuk memproses data elektronik, mengetik, optik, atau sistem yang melaksanakan fungsi logika, aritmatika, dan menyimpan.
6. Perangkat Lunak adalah satu atau sekumpulan program komputer, prosedur, dan/atau dokumentasi yang terkait dalam pengoperasian sistem elektronik.
7. Keamanan Informasi adalah suatu kondisi dimana terjaganya aspek kerahasiaan, integritas dan ketersediaan dari Informasi.
8. 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.
9. Aset Informasi adalah unit Informasi yang dapat dipahami, dibagi, dilindungi dan dimanfaatkan secara efektif.
10. Aset Pengolahan adalah suatu perangkat baik elektronik maupun non-elektronik yang dapat digunakan untuk membuat dan menyunting Informasi.
11. Penyimpanan Informasi adalah suatu proses menyimpan Informasi dengan menggunakan media baik elektronik maupun nonelektronik.
12. Data Center/Pusat Data adalah suatu fasilitas untuk menempatkan sistem komputer dan perangkat perangkat terkait, seperti Sistem komunikasi data dan penyimpanan data.

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

13. Akun adalah identifikasi pengguna yang diberikan oleh unit Pengelola TIK, bersifat unik dan digunakan bersamaan dengan kata sandi ketika akan memasuki sistem TIK.
14. Akun khusus adalah akun yang diberikan oleh unit Pengelola TIK sesuai kebutuhan tetapi tidak terbatas pada pengelolaan TIK (baik berupa aplikasi atau sistem), dan kelompok kerja (baik berupa acara kedinasan, tim, atau unit kerja).
15. Audit logging adalah catatan mengenai perubahan data dalam aplikasi, yang dicatat biasanya kolom mana yang berubah, siapa yang mengubah, diubah dari apa menjadi apa, kapan berubah
16. Aset fisik adalah jenis aset yang memiliki wujud fisik, misalnya perangkat komputer, perangkat jaringan dan komunikasi, media yang dapat dipindahkan, dan perangkat pendukung lainnya.
17. Aset informasi Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang adalah aset dalam bentuk:
    a. Data/dokumen, meliputi: data peraturan perundangan, data hak asasi manusia, data pemasyarakatan, data administrasi hukum umum, data imigrasi, data hak kekayaan intelektual, data gaji, data kepegawaian, data penawaran dan kontrak, dokumen perjanjian kerahasiaan, kebijakan kementerian, hasil penelitian, bahan pelatihan, prosedur operasional, rencana kelangsungan kegiatan, dan hasil audit;
    b. Perangkat lunak, meliputi: perangkat lunak aplikasi, perangkat lunak sistem, dan perangkat bantu pengembangan sistem;
    c. Aset fisik, meliputi: perangkat komputer, perangkat jaringan dan komunikasi, removable media, dan perangkat pendukung; dan
    d. Aset tak berwujud, meliputi: pengetahuan, pengalaman, keahlian, citra, dan reputasi.
18. Aset tak berwujud adalah jenis aset yang tidak memiliki wujud fisik, misalnya pengetahuan, pengalaman, keahlian, citra, dan reputasi. Aset ini mempunyai umur lebih dari satu tahun (aset tidak lancar) dan dapat diamortisasi selama periode pemanfaatannya, yang biasanya tidak lebih dari 40 (empat puluh tahun).

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

19. Backup adalah sebuah proses pembuatan gandaan/duplikat/ cadangan dari aset informasi yang dilakukan sebagai upaya pengamanan dan pemulihan sebagai bagian dari manajemen risiko.
20. Conduit adalah sebuah tabung atau saluran untuk melindungi kabel yang biasanya terbuat dari baja.
21. Daftar inventaris aset informasi adalah kumpulan informasi yang memuat bentuk, pemilik, lokasi, retensi, dan hal-hal yang terkait dengan aset informasi.
22. Denial of service adalah suatu kondisi dimana sistem tidak dapat memberikan layanan secara normal, yang disebabkan oleh suatu proses yang diluar kendali baik dari dalam maupun dari luar sistem.
23. Direktori adalah penamaan koleksi file (biasanya berbentuk hirarki). Ini merupakan cara untuk mengelompokkan file sehingga mudah untuk dikelola.
24. Dokumen SMKI Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang adalah dokumen terkait pelaksanaan SMKI yang meliputi antara lain dokumen standar, prosedur, dan catatan penerapan SMKI.
25. Fallback adalah suatu tindakan pembalikan/menarik diri dari posisi awal.
26. Fault logging adalah pencatatan permasalahan sistem informasi.
27. Hak akses khusus adalah akses terhadap sistem informasi sensitif, termasuk di dalamnya dan tidak terbatas pada sistem operasi, perangkat penyimpanan, file server, dan aplikasi-aplikasi sensitif. Hanya diberikan kepada pengguna yang membutuhkan, pemakaiannya terbatas dan dikontrol.
28. Hash totals adalah nilai pemeriksa kesalahan yang diturunkan dari penambahan satu himpunan bilangan yang diambil dari data (tidak wajib berupa data numerik) yang diproses atau dimanipulasi dengan cara tertentu.
29. Kata sandi adalah serangkaian kode yang dibuat Pengguna, bersifat rahasia dan pribadi yang digunakan bersamaan dengan Akun Pengguna.

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

30. Keamanan informasi adalah perlindungan aset informasi dari berbagai bentuk ancaman untuk memastikan kelangsungan kegiatan, menjamin kerahasiaan, keutuhan, dan ketersediaan aset informasi.
31. Komunitas keamanan informasi adalah kelompok/komunitas yang memiliki pengetahuan/keahlian khusus dalam bidang keamanan informasi atau yang relevan dengan keamanan informasi, seperti: Indonesia Security Incident Response Team on Internet and Infrastructure (ID-SIRTII), Unit cybercrime POLRI, ISC2, ISACA.
32. Koneksi eksternal (remote access) adalah suatu akses jaringan komunikasi dari luar organisasi ke dalam organisasi.
33. Kriptografi adalah ilmu yang mempelajari cara menyamarkan informasi dan mengubah kembali bentuk tersamar tersebut ke informasi awal untuk meningkatkan keamanan informasi. Dalam kriptografi terdapat dua prinsip yaitu enkripsi dan dekripsi.
34. Malicious code adalah semua jenis program yang membahayakan termasuk makro atau script yang dapat dieksekusi dan dibuat dengan tujuan untuk merusak sistem komputer.
35. Master disk adalah media yang digunakan sebagai sumber dalam melakukan instalasi perangkat lunak.
36. Mobile computing adalah penggunaan perangkat komputasi yang dapat dipindah, misalnya notebook dan personal data assistant (PDA) untuk melakukan akses, pengolahan data, dan penyimpanan.
37. Penanggung jawab pengendalian dokumen adalah pihak yang memiliki kewenangan dan bertanggung jawab dalam proses pengendalian dokumen SMKI.
38. Pengguna adalah pegawai Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang dan atau pihak ketiga serta tidak terbatas pada pengelola TIK dan kelompok kerja yang diberikan hak mengakses sistem TIK di lingkungan Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang.
39. Pemilik aset informasi adalah unit kerja yang memiliki kewenangan terhadap aset informasi.

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

40. Pencatatan waktu (timestamp) adalah catatan waktu dalam tanggal dan/atau format waktu tertentu saat suatu aktivitas/transaksi terjadi. Format ini biasanya disajikan dalam format yang konsisten, yang memungkinkan untuk membandingkan dua aktivitas/ transaksi yang berbeda berdasarkan dengan waktu.
41. Perangkat jaringan adalah peralatan jaringan komunikasi data seperti: modem, hub, switch, router, dan lain-lain.
42. Perangkat lunak adalah kumpulan beberapa perintah yang dieksekusi oleh mesin komputer dalam menjalankan pekerjaannya.
43. Perangkat pendukung adalah peralatan pendukung untuk menjamin beroperasinya perangkat keras dan perangkat jaringan serta untuk melindunginya dari kerusakan. Contoh perangkat pendukung adalah Uninterruptible Power Supply (UPS), pembangkit tenaga listrik/ generator, antena komunikasi.
44. Perangkat pengolah informasi adalah setiap sistem pengolah informasi, layanan atau infrastruktur seperti komputer, faksimili, telepon, mesin fotocopy.
45. Perjanjian escrow adalah perjanjian dengan pihak ketiga untuk memastikan apabila pihak ketiga tersebut bangkrut (mengalami failure) maka Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang berhak untuk mendapatkan kode program (source code).
46. Perjanjian kerahasiaan adalah perikatan antara para pihak yang mencantumkan bahan rahasia, pengetahuan, atau informasi yang mana pihak-pihak ingin berbagi satu sama lain untuk tujuan tertentu, tetapi ingin membatasi akses dengan pihak lain.
47. Petugas Pelaksana Pengelolaan Proses Kelangsungan Kegiatan adalah pegawai yang ditunjuk oleh Pimpinan Unit Eselon I untuk mengelola proses kelangsungan kegiatan pada saat keadaan darurat.
48. Pihak ketiga adalah semua unsur di luar pengguna unit TIK Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang yang bukan bagian dari Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang, misal mitra kerja Dinas

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang (seperti: konsultan, penyedia jasa komunikasi, pemasok dan pemelihara perangkat pengolah informasi), dan kementerian/lembaga lain.

49. Proses pendukung adalah proses-proses penunjang yang mendukung suatu proses utama yang terkait seperti proses pengujian perangkat lunak dan proses perubahan perangkat lunak.
50. Rencana kontijensi adalah suatu rencana ke depan pada keadaan yang tidak menentu dengan skenario, tujuan, teknik, manajemen, pelaksanaan, serta sistem penanggulangannya telah ditentukan secara bersama untuk mencegah dan mengatasi keadaan darurat.
51. Rollback adalah sebuah mekanisme yang digunakan untuk mengembalikan sistem ke kondisi semula sebelum perubahan diimplementasikan. Mekanisme ini biasanya terdapat pada basis data.
52. Routing adalah sebuah mekanisme yang digunakan untuk mengarahkan dan menentukan rute/jalur yang akan dilewati paket dari satu perangkat ke perangkat yang berada di jaringan lain.
53. Sanitasi adalah proses penghilangan informasi yang disimpan secara permanen dengan menggunakan medan magnet besar atau perusakan fisik.
54. Sistem Informasi adalah serangkaian perangkat keras, perangkat lunak, sumber daya manusia, serta prosedur dan atau aturan yang diorganisasikan secara terpadu untuk mengolah data menjadi informasi yang berguna untuk mencapai suatu tujuan.
55. Sistem Manajemen Keamanan Informasi (SMKI) adalah sistem manajemen yang meliputi kebijakan, organisasi, perencanaan, penanggung jawab, proses, dan sumber daya yang mengacu pada pendekatan risiko bisnis untuk menetapkan, mengimplementasikan, mengoperasikan, memantau, mengevaluasi, mengelola, dan meningkatkan keamanan informasi.
56. Sub network (subnet) adalah pengelompokkan secara logis dari perangkat jaringan yang terhubung.
57. System administrator adalah sebuah akun khusus untuk mengelola sistem informasi.

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

58. System utilities adalah sebuah sistem perangkat lunak yang melakukan suatu tugas/fungsi yang sangat spesifik, biasanya disediakan oleh sistem operasi, dan berkaitan dengan pengelolaan sumber daya sistem, seperti memory, disk, printer, dan sebagainya.
59. Teleworking adalah penggunaan teknologi telekomunikasi untuk memungkinkan pegawai bekerja di suatu lokasi yang berada di luar kantor untuk mengakses jaringan internal kantor.

D. Kebijakan

1. Pengelolaan Data Informasi di Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang ditetapkan dengan Surat Keputusan Kepala Dinas.
2. Pengelola Data Informasi 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 dimiliki oleh Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang, dikelola oleh Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang masing-masing sesuai kepemilikannya (ownership).
4. Penanggung jawab Pemilik Aset Informasi adalah Direktur Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang. Pemilik Aset Informasi bertanggung jawab melakukan pengamanan dan pemeliharaan secara berkelanjutan atas Aset Informasi.
5. Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang 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 (id sirtii) dan sebagainya) serta

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

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.

6. Kebijakan dalam penggunaan Perangkat Mobile dan Teleworking:

a. penggunaan perangkat mobile, baik milik pribadi atau milik Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang untuk mengakses dan/atau menyimpan Informasi milik Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang harus sangat dibatasi sesuai dengan kebutuhan pekerjaan dengan mempertimbangkan prinsip kehati-hatian saat menggunakan perangkat mobile dengan menghindari meninggalkan perangkat tanpa pengawasan.

b. perangkat mobile harus mengaktifkan fitur otentikasi pengguna, seperti penggunaan username dan password, sesuai dengan kebijakan terkait pengendalian akses.

c. Informasi sensitif harus dienkripsi atau dilindungi dengan password pada saat disimpan di mobile device, sesuai dengan klasifikasi Informasinya.

d. Informasi sensitif milik Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang yang disimpan pada perangkat mobile device harus di-backup secara berkala untuk menghindari hilangnya aspek ketersediaan dari Informasi.

e. aktivitas teleworking sebagai sarana pegawai untuk bekerja dari lokasi di luar area kerja Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang dengan mengakses jaringan internal secara remote melalui jaringan internet diperbolehkan

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

namun sangat dibatasi hanya untuk personil yang diberi izin berdasarkan kebutuhan pekerjaannya.

f. akses ke jaringan internal Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang dari jaringan internet harus menggunakan koneksi aman dengan menggunakan antara lain teknologi VPN.

g. kebijakan terkait teknologi teleworking sebagai sarana pegawai bekerja pada lokasi di luar Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang dengan mengakses jaringan internal Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang. Teknologi ini diperbolehkan untuk digunakan dalam kondisi sebagai berikut:
   1) perangkat akses (misalnya komputer, notebook) yang digunakan untuk teleworking harus terinstal firewall dan antivirus;
   2) mekanisme akses terhadap Sistem atau aplikasi disesuaikan dengan klasifikasi Aset Informasi:
      a) Informasi publik : dapat diakses langsung.
      b) Informasi rahasia :
         i) harus menggunakan protokol HTTPS atau SSH; dan
         ii) harus menggunakan VPN, sebelum kemudian mengakses melalui protokol HTTPS atau SSH.

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

BAB II

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 Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang.

B. Ruang Lingkup

Ruang lingkup kebijakan keamanan sumber daya manusia terdiri dari:

1. pegawai dalam lingkungan Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang;
2. pegawai dari pihak eksternal yang dalam aktivitas pekerjaannya memiliki akses ke Aset Informasi dan aset pengolahan dan penyimpanan Informasi dalam lingkungan Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang.

C. Kebijakan

1. calon pegawai di lingkungan Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang 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 Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang dan pegawai dari pihak eksternal yang dalam aktivitas pekerjaannya memiliki akses ke Aset Informasi dan aset pengolahan dan penyimpanan Informasi dalam lingkungan Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang harus menandatangani perjanjian kerahasiaan NDA (non

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

disclosure agreement) sesuai dengan perjanjian dengan memperhatikan tingkat sensitivitas dari aset yang diakses.

4. setiap pegawai internal maupun eksternal harus mematuhi seluruh kebijakan dan prosedur Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang/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 Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang harus dikembalikan setelah pemberhentian kepegawaian;
    b) seluruh hak akses Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang harus dinonaktifkan atau dihapus setelah pemberhentian kepegawaian; dan
    c) seluruh hak akses Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang harus disesuaikan setelah perubahan status kepegawaian.

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

BAB III

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 Surat Keputusan Kepala Dinas terkait SMKI; dan
2. penanganan Aset Pengolahan dan penyimpanan Informasi dalam ruang lingkup Surat Keputusan Kepala Dinas.

C. Kebijakan

1. Kepala Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang menetapkan pemilik Aset Informasi di setiap unit Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang, beserta perangkat fisik pengolah Informasi yang terkait.
2. Pemilik Aset Informasi memiliki tanggung jawab untuk:
   a) mengidentifikasi seluruh Aset Informasi dan fasilitas pengolahan dan penyimpanan Informasi;
   b) mendokumentasikannya dalam daftar inventaris aset SMKI, serta senantiasa memperbaharui daftar inventaris aset SMKI tersebut sesuai kondisi terkini; dan
   c) memastikan bahwa setiap aset telah diklasifikasikan dan dilindungi secara memadai.
3. Aset Pengolahan dan Penyimpanan Informasi yang diinventarisasi adalah aset dalam bentuk:

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

a) perangkat keras, meliputi perangkat keras yang digunakan untuk mengolah dan menyimpan Informasi dalam bentuk fisik maupun elektronik, yang mencakup namun tidak terbatas pada komputer, notebook, server, hard disk drive, USB disk;
b) Perangkat Lunak, meliputi Perangkat Lunak yang digunakan untuk mengolah Informasi dalam bentuk elektronik, yang mencakup namun tidak terbatas pada Sistem operasi, aplikasi, dan database;
c) perangkat jaringan, meliputi perangkat keras dan lunak yang digunakan untuk membentuk dan infrastruktur jaringan telekomunikasi, yang mencakup namun tidak terbatas pada hub, switch, router, firewall, IDS, IPS, dan network monitoring tools;
d) perangkat pendukung meliputi perangkat digunakan untuk mendukung operasional perangkat pengolahan dan penyimpanan Informasi yang mencakup namun tidak terbatas pada genset, UPS, 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 colocation, 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 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

Catatan :
- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

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 Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang harus dikembalikan setelah personil pengguna tidak memiliki hubungan kepegawaian lagi dengan Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang, 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. Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang 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.

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

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 tabel 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
Rahasia (Confidential)	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

Catatan :
- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

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 Informasi Lainnya 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

Catatan :
- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

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 Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang pemilik	• Distribusi kepada pihak eksternal sangat dibatasi untuk kebutuhan pekerjaan. • Apabila memungkinkan, Informasi rahasia

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  “Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah.”
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

		Informasi. • Distribusi kepada pihak eksternal dibatasi berdasarkan kebutuhan pekerjaan maupun operasional di lingkungan Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang. • Distribusi kepada pihak eksternal perlu seijin pemilik Informasi • Sensitivitas dan kritikalitas Informasi perlu diberitahukan kepada pihak eksternal.	tidak disalin oleh pihak eksternal (eyes only). • Distribusi kepada pihak eksternal perlu seijin pemilik Informasi. • Sensitivitas dan kritikalitas Informasi perlu diberitahukan kepada pihak eksternal • Pihak ketiga harus disertai perjanjian kerahasiaan (NDA - *non disclosure agreement*)
Pencetakan Informasi	Tidak ada pembatasan.	Dibatasi hanya untuk kebutuhan internal.	Pencetakan hanya pada printer organisasi dan diusahakan tidak mencetak menggunakan jasa percetakan 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

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

			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. • Menginformas ikan kepada penerima akan pengiriman Informasi tersebut. • Mengkonfirmasi kepada penerima bahwa Informasi yang dikirim sudah diterima
Pengiriman ke pihak internal melalui email	• Pengiriman e-mail harus menggunakan akun email Perangkat Daerah Kabupaten/ Unit Kerja • Tidak diperlukan penanganan khusus.	• Pengiriman email harus menggunakan akun email Perangkat Daerah Kabupaten / Unit Kerja. • Pastikan alamat email tujuan benar. • Pengiriman Informasi, termasuk forwarding / meneruskan email hanya boleh dilakukan oleh pemilik Informasi.	• Pengiriman email harus menggunakan akun email Perangkat Daerah Kabupaten /Unit Kerja • Memberi Password pada Informasi yang dikirim melalui email dan password diinformasikan kepada penerima secara terpisah • Tidak mencantumkan

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

			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 email harus menggunakan akun email Perangkat Daerah Kabupaten/ Unit Kerja • Tidak diperlukan penanganan khusus.	• Pengiriman email harus menggunakan akun email Perangkat Daerah Kabupaten / Unit Kerja • Pastikan alamat email tujuan sudah benar	• Tidak disarankan menggunakan email untuk mengirim Informasi dengan klasifikasi ini. • Pengiriman email harus menggunakan akun email Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang/Unit Kerja • Pastikan alamat email tujuan sudah benar • Memberi password pada Informasi yang dikirim melalui email dan password diinformasikan kepada penerima secara terpisah
Penyimpanan Informasi hardcopy	Tidak diperlukan penanganan khusus.	Tidak diperlukan penanganan khusus.	Disimpan secara aman dalam tempat penyimpanan yang terkunci.

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

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 (scrap paper)	• 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

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

			format).
Pengamanan pada komputer penyimpan Informasi	Tidak diperlukan penanganan khusus	• *Screensaver lock* harus aktif jika meninggalkankomputer / terminal. • Sign-off komputer / terminal jika tidak digunakan atau pulang kerja.	• *Screensaver lock* 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 Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang

15. Informasi yang dianggap kritikal oleh Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang 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 dibackup beserta metode dan frekuensi dari backup harus ditentukan bersama dengan personil yang bertugas melaksanakan proses backup serta harus dinyatakan secara jelas dalam sebuah rencana backup resmi;

Catatan :
- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

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. Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang menyediakan akses internet dan email kepada pegawainya hanya untuk kebutuhan pekerjaan dan operasional Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang.
18. Ketentuan dalam penggunaan internet dan email adalah sebagai berikut:
    a) pengguna dilarang menggunakan akses internet dan email Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang untuk kegiatan melanggar hukum dan aktivitas yang dapat membahayakan keamanan jaringan Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang;
    b) pengguna dilarang untuk menggunakan akses internet dan email Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang 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 Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang.
19. Pengguna disarankan untuk tidak membagi Informasi pribadi melalui situs internet atau media sosial.

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

20. Pengguna dilarang untuk mendistribusikan Informasi Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang yang bersifat rahasia tanpa izin dari pemilik Informasi.
21. Pesan penyangkalan ini harus dituliskan pada akhir setiap e-mail. “Pesan ini mungkin berisi Informasi rahasia dan hanya ditujukan kepada pihak yang dituju. Apabila anda bukanlah pihak yang dituju, anda dilarang untuk mengungkapkan, menyebarkan atau menyalin isi email ini. Apabila anda mendapatkan email ini tanpa sengaja mohon segera hubungi pengirim email dan hapus email ini segera. Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang tidak bertanggung jawab untuk pengiriman Informasi ini secara lengkap dan tepat dan juga tidak bertanggung jawab untuk keterlambatan dalam pengiriman email ini.”
22. Bidang Keamanan Informasi dan Persandian yang mengelola akun email Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang berhak untuk mem-block akun email Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang pada saat terdapat bukti memadai terkait penyalahgunaan dan/atau pelanggaran keamanan.

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  “Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah.”
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

BAB IV

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 Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang 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 Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang 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 Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

Sumedang 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 Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang;
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 didokumentasikan secara formal; dan
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 Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang meliputi:
   a) penggunaan layanan jaringan (network services) hanya diperbolehkan secara terbatas, sesuai kebutuhan ketugasan dan kepentingan Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang, layanan lainnya yang tidak diperlukan harus di nonaktifkan;
   b) jaringan komunikasi dalam lingkungan Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang harus

Catatan :
- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

dipisahkan kedalam domain jaringan yang terpisah sesuai dengan kebutuhan bisnis dan operasional, dalam rangka untuk mengamankan jaringan internal Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang dan aset di jaringan tersebut;

c) akses secara remote ke jaringan internal Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang 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 Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang 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 ke setiap 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 Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang aktif.

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

b) pendaftaran, modifikasi dan pencabutan hak akses pengguna mencakup proses pembuatan user ID, memberikan hak akses kepada user ID serta mencabut hak akses dan user ID.
c) pendaftaran, modifikasi dan pencabutan hak akses pengguna harus disetujui oleh atasan dari pengguna yang memohon hak akses tersebut dan pemilik Informasi dan/atau Sistem. Persetujuan tersebut harus diberikan sesuai dengan aturan pemberian akses.
d) identitas pengguna harus diotorisasi secara formal oleh pejabat berwenang pada pemilik Aset Informasi. Akses atas sistem dan aplikasi hanya dapat diaktifkan jika proses otorisasi telah selesai.
e) identitas pengguna pada Sistem, seperti user ID, harus bersifat unik untuk memungkinkan mengidentifikasi dan meminta pertanggungjawaban pengguna.
f) pemberian Informasi 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 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 Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang.
h) hak akses khusus (privileged access rights) dari sistem Informasi dalam lingkungan Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang, seperti administrator, root, hak akses untuk memodifikasi database atau hak akses untuk membuat,

Catatan :
- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

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 Dinas Komunikasi dan Informatika, Persandian dan Statistik 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 Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang harus memiliki karakteristik sebagai berikut:

      1) memiliki panjang minimum 8 karakter;

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

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

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 Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang atau nama pengguna;

e) password untuk mengakses Sistem Informasi dalam lingkungan Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang harus diganti paling sedikit setiap 3 (tiga) bulan sekali;
f) pada saat penggantian, password sebelumnya tidak boleh digunakan kembali sampai setelah 3 siklus pergantian password;
g) prosedur 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 Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang 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;

Catatan :
- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
"Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

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 Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik

Catatan :
- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

Kabupaten Sumedang harus mempertimbangkan keamanan sebagai berikut yaitu penggunaan program utility khusus seperti registry cleaner atau sistem monitoring yang dapat mengambil alih kendali sistem/aplikasi atau mendapatkan hak akses khusus pada Sistem/aplikasi harus sangat dibatasi berdasarkan kebutuhan operasional pengguna.

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

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

BAB V
KRIPTOGRAFI

A. Tujuan

Tujuan dari kebijakan terkait teknologi kriptografi adalah untuk memastikan penggunaan teknologi kriptografi yang sesuai dan efektif untuk melindungi kerahasiaan, keaslian dan/atau integritas dari Informasi dalam lingkungan Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang.

B. Ruang Lingkup

Ruang Lingkup kebijakan terkait teknologi kriptografi adalah penggunaan teknologi kriptografi dalam pengolahan dan penyimpanan Informasi di lingkungan Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang.

C. Kebijakan

1. Kontrol kriptografi dapat digunakan untuk menjamin kerahasiaan dan integritas dari Informasi sensitif di lingkungan Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang.
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.

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

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.

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

BAB VI
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 Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang; dan
2. mencegah terjadinya kerusakan atau gangguan pada Aset Informasi dan aset pengolahan dan penyimpanan Informasi pada lingkungan Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang 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 Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang 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 Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

Kabupaten Sumedang 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 Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang; 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 Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang.

4. pengendalian akses pengunjung ke dalam area di lingkungan Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang 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 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.

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

5. Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang harus memperhatikan aspek pengamanan terhadap perangkat yang digunakan melalui:
    a) seluruh perangkat harus ditempatkan di lokasi yang aman, sedemikian rupa sehingga terlindungi dari terjadinya pencurian, akses oleh pihak yang tidak berwenang, kebakaran, air, debu, dan sebagainya;
    b) seluruh perangkat di dalam area harus dipelihara, di inspeksi 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 Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang, 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 Dinas Komunikasi dan Informatika, Persandian dan Statistik 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 di lokasi yang aman, sedemikian rupa sehingga terlindungi dari terjadinya kebakaran, kebocoran, debu, dan sebagainya;

Catatan :
- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

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.

Catatan :
- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

BAB VII
KEAMANAN OPERASIONAL SISTEM INFORMASI

A. Tujuan

Tujuan dari kebijakan keamanan operasional Sistem Informasi adalah untuk:

1. memastikan pengoperasian aset pengolahan dan penyimpanan Informasi di Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang secara benar dan aman;
2. memastikan terlindunginya Aset Informasi beserta aset pengolahan dan penyimpanan Informasi di Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang 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 Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang.

B. Ruang Lingkup

Ruang lingkup dari kebijakan keamanan operasional sistem Informasi adalah pengoperasian aset pengolahan dan penyimpanan Informasi di lingkungan Dinas Komunikasi dan Informatika, Persandian dan Statistik 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:

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

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 Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang 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 Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang untuk menangani ancaman malware; dan
   d. setiap insiden terkait dengan malware harus dilaporkan kepada administrator sistem dan dikategorikan sebagai insiden Keamanan Informasi.
7. Seluruh Aset Informasi yang berada di dalam fasilitas pengolahan Informasi wajib dilakukan backup, dengan persyaratan berikut:
   a. backup mencakup aplikasi, database,dan 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

Catatan :
- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

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 Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang harus di sinkronisasi dengan sumber waktu yang akurat dan telah disepakati.
11. Proses dan prosedur untuk mengendalikan instalasi perangkat lunak pada Sistem operasional harus diterapkan dan diimplementasikan 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.

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

14. Setiap sistem Informasi di lingkungan Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang dapat dilakukan proses audit yang mencakup proses verifikasi terhadap sistem Informasi dan/atau Informasi Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang 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 Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang 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 Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang, dan harus segera dihapus setelah proses audit telah selesai dilakukan.
15. Semua fasilitas pemrosesan Informasi harus dilakukan pengelolaan manajemen kapasitasnya, dengan ketentuan sebagai berikut :
    a) Setiap penanggung jawab sistem di Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang harus melakukan manajemen kapasitas untuk setiap pengembangan infrastruktur dan sistem aplikasi baru maupun yang sedang berjalan dengan mempertimbangkan proyeksi terhadap kebutuhan operasional, dan infrastruktur berdasarkan kebutuhan bisnis yang akan datang dan sistem informasi organisasi. Selain itu proyeksi tersebut perlu juga mempertimbangkan kondisi sistem informasi organisasi saat ini dan tren proyeksi perkembangan sistem selama ini.
    b) Pengukuran kapasitas terhadap infrastruktur dilakukan secara periodik.

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

c) Identifikasi kebutuhan untuk perubahan atau penambahan kapasitas infrastruktur dilakukan berdasarkan pada:
   1) Tercapainya Ambang batas/ *Threshold*;
   2) Persyaratan/kebutuhan bisnis;
   3) Laporan insiden terkait kapasitas;
   4) Laporan/usulan kapasitas dari Tim Teknis.

d) Penggunaan seluruh sumber daya pengolahan informasi dalam sistem informasi organisasi harus dipantau, dilakukan proses *tuning* untuk menjamin kinerja sistem yang diharapkan dapat selalu tersedia dan tidak terjadinya kegagalan sistem karena kapasitas yang tidak mencukupi.

e) Semua aktivitas atau proses dalam sistem informasi baik yang sedang berjalan maupun yang akan dijalankan harus mengidentifikasi *item* kebutuhan kapasitas sistem, sebagai contoh adalah kapasitas memori atau *storage* dalam *server,* utilisasi CPU *server* atau utilisasi *backbone jaringan* WAN.

f) Dalam proses manajemen kapasitas perhatian lebih perlu diberikan untuk sistem atau perangkat pengolahan informasi yang memiliki biaya tinggi secara finansial, waktu maupun penggunaan sumber daya manusia. Untuk sistem dengan biaya tinggi tersebut pemilik atau pengelola sistem perlu memantau secara seksama penggunaan dan utilisasi sistem.

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

BAB VIII
KEAMANAN KOMUNIKASI

A. Tujuan

Tujuan dari kebijakan keamanan komunikasi adalah untuk:

1. memastikan perlindungan atas Informasi pada jaringan komputer beserta fasilitas pendukung pengolahan Informasi;
2. menjaga Keamanan Informasi yang dipertukarkan, baik di dalam Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang maupun antar Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang 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 Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang harus diamankan untuk menjamin:
   a) pencegahan akses tanpa izin ke jaringan, layanan jaringan dan fasilitas pemrosesan Informasi dalam jaringan;
   b) keamanan dari Informasi milik Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang yang dikirimkan melalui jaringan; dan
   c) integritas dan ketersediaan dari layanan jaringan Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang.

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

2. Tugas dan tanggung jawab untuk pengelolaan jaringan dan keamanan harus dialokasikan dan apabila memungkinkan dipisahkan dari penanggung jawab operasional sistem aplikasi dan Data Center.
3. Konfigurasi dari jaringan, perangkat aktif dan perangkat keamanan jaringan harus ditinjau secara berkala untuk:
   a. memastikan kesesuaian dengan kondisi terkini; dan
   b. mengidentifikasi kerawanan pada jaringan, layanan jaringan dan fasilitas pemrosesan Informasi dalam jaringan.
4. Jaringan internal Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang harus dipisahkan dari jaringan eksternal dengan menggunakan security gateway atau firewall dan harus dikonfigurasikan untuk:
   a) memfilter traffic tanpa izin maupun traffic yang mencurigakan; dan
   b) apabila memungkinkan memfilter dan mencegah infeksi malware ke jaringan internal;
5. Koneksi ke security gateway atau firewall harus di otentikasikan, diotorisasi dan diamankan dengan metode pengamanan yang sesuai, misalnya dengan virtual private network (VPN), secure shell (SSH) atau metode kriptografi.
6. Kebijakan dan log firewall harus ditinjau paling sedikit 1 (satu) kali dalam tiga bulan.
7. Koneksi eksternal harus diputuskan secara otomatis setelah tidak aktif selama 5 menit.
8. Akses dari jaringan eksternal yang dilakukan oleh vendor pihak ketiga hanya dapat diberikan untuk kebutuhan troubleshooting dan harus secara formal disetujui dan didokumentasikan dan harus dibatasi waktunya sesuai dengan kebutuhan dari akses.
9. Jaringan internal Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang harus disegmentasi baik secara fisik maupun logic untuk meningkatkan keamanan dan untuk mengendalikan akses dan traffic jaringan berdasarkan kritikalitas dari sistem dalam jaringan Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang.

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

10. Segmentasi jaringan harus ditinjau paling sedikit 1 (satu) kali dalam tiga bulan untuk menjamin kesesuaian dengan prasyarat keamanan terkini.
11. Routing jaringan harus dilakukan berdasarkan pengendalian terhadap alamat sumber dan tujuan.
12. Tanggung jawab untuk merubah routing jaringan hanya diberikan kepada administrator jaringan yang diberi izin.
13. Aturan untuk routing harus ditinjau paling tidak satu kali dalam tiga bulan untuk mendeteksi dan mengoreksi adanya kesalahan atau routing tanpa otorisasi.
14. Perangkat jaringan harus ditempatkan pada lokasi yang aman untuk menghindari akses tanpa izin dan ancaman fisik maupun lingkungan.
15. Akses, baik fisik maupun logical ke perangkat jaringan harus dibatasi untuk tujuan administrasi dan pemeliharaan jaringan.
16. Port dan layanan jaringan, baik fisik maupun logical, yang tidak digunakan tidak boleh diaktifkan.
17. Akses ke port yang digunakan untuk kebutuhan diagnostik dan konfigurasi perangkat jaringan dan keamanan jaringan, seperti console port, harus sangat dibatasi dan diberikan kepada:
    a) Administrator jaringan dan keamanan jaringan Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang;
    b) Pihak ketiga yang telah disetujui dan bekerja untuk kepentingan Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang;
    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 Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang.

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

20. Mekanisme keamanan, tingkat layanan dan prasyarat lain untuk semua layanan jaringan harus diidentifikasi dan dimasukkan kedalam perjanjian layanan jaringan.
21. Akses ke layanan jaringan Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang 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 Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang.
23. Layanan jaringan Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang 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, Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang 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 kerahasian 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.

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

BAB IX

AKUISISI, PENGEMBANGAN DAN PEMELIHARAAN SISTEM

A. Tujuan

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

1. memastikan Keamanan Informasi sebagai bagian tak terpisahkan dari siklus hidup (life cycle) sistem Informasi. Termasuk persyaratan untuk sistem Informasi yang menyediakan layanan melalui jaringan publik.
2. memastikan Keamanan Informasi didesain dan diimplementasikan 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. Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang Kerja harus menetapkan dan mendokumentasikan secara jelas persyaratan Keamanan Informasi yang relevan sebelum pengembangan, perluasan, atau pengadaan sistem Informasi baru.
2. Persyaratan keamanan harus diidentifikasi secara jelas di dalam dokumen persyaratan dan spesifikasi perangkat lunak (Software Requirement and Specification).
3. Spesifikasi ini harus disetujui oleh pemilik Informasi, pemilik proses bisnis dan pengembang sistem, sebelum fase pengkodean (coding) dalam pengembangan sistem.
4. Informasi yang digunakan oleh aplikasi Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang yang

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

ditransmisikan melalui jaringan publik (internet) harus diamankan dari aktivitas penipuan, kemungkinan adanya perselisihan kontrak, dan pengungkapan dan/atau perubahan Informasi tanpa izin.

5. Pengamanan Informasi terhadap Informasi yang ditransmisikan melalui sistem Informasi yang digunakan dapat mencakup namun tidak terbatas pada:
   a. proses 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 Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang meliputi:
   a) aturan untuk pengembangan Sistem harus ditetapkan dan diimplementasikan untuk proses pengembangan Sistem di Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang yang mencakup:
      1) pengamanan dari lingkungan pengembangan, seperti pemisahan lingkungan pengembangan baik secara fisik dan/atau logical, pengendalian akses, pengelolaan perubahan;
      2) panduan secure coding;
      3) pengendalian versi aplikasi;
      4) penyimpanan dari source code; 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 Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang;

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

8. Apabila platform operasional, misalnya sistem operasi, database dan/atau middleware, dari Sistem Informasi Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang mengalami perubahan, aplikasi kritikal Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang harus ditinjau dan di uji untuk memastikan tidak ada dampak buruk terhadap operasional dan keamanan Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang;
9. Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang harus menetapkan lingkungan pengembangan yang aman untuk pengembangan dan integrasi sistem Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang. 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. Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang harus mengawasi aktivitas pengembangan sistem yang dialih dayakan (outsourced). Hal ini dapat mencakup:
    a) perjanjian terkait lisensi dan kepemilikan Sistem;
    b) pengujian penerimaan sistem untuk menguji kualitas dan akurasi dari Sistem;
    c) prasyarat dokumentasi untuk Sistem;
    d) perjanjian dengan pihak ketiga sebagai penjamin;
    e) hak untuk melakukan audit proses pengembangan dan kontrol yang diimplementasikan oleh vendor.
11. Pengujian dari fitur keamanan Sistem harus dilakukan pada saat pengembangan Sistem Informasi Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang;
12. Pengujian ini dilakukan berdasarkan prasyarat keamanan Sistem yang telah ditetapkan;

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

13. Kriteria dan jadwal untuk pengujian penerimaan Sistem harus ditetapkan untuk sistem Informasi baru, upgrade dan versi baru dari Sistem Informasi Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang;
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.

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

BAB X
MANAJEMEN KONFIGURASI

A. Tujuan

Pedoman ini disusun sebagai memberikan panduan tentang tata cara pengelolaan konfigurasi layanan IT melalui manajemen informasi Configuration Item (CI) yang tepat dan memungkinkan orang membuat keputusan-keputusan di saat yang tepat, serta memudahkan untuk melaksanakan penanganan konfigurasi layanan TI.

B. Ruang Lingkup

Pedoman ini digunakan di lingkungan Unit Teknologi Informasi untuk menjalankan aktivitas Teknologi Informasi dalam mengatur pengelolaan konfigurasi layanan IT yang meliputi pengidentifikasian CI dan pencatatan. Laporan Hasil Konfigurasi, konsolidasi CI dan sistem pelaporan ini berlaku untuk layanan-layanan IT di Lingkungan Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang.

C. Kebijakan

1. Identifikasi Configuration Item (CI)

   Dimana hal-hal yang perlu diperhatikan untuk melakukan *IT Configuration Management* adalah sebagai berikut:

   a) Konfigurasi perangkat TI harus distandarisasi untuk memudahkan pengelolaan dan perawatan sistem yang terkait dengannya.
   b) Pengelolaan konfigurasi perangkat TI juga bertujuan untuk melindungi perangkat TI dari ancaman eksploitasi teknis terhadap kelemahan yang diakibatkan oleh kesalahan konfigurasi sistem.
   c) Standarisasi konfigurasi perangkat TI oleh Unit Information Technology dan pelaksanaannya dilakukan oleh Unit Kerja IT terkait.
   d) Proses backup dilakukan sebelum dilakukan proses perubahan konfigurasi.

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

Aliran Proses dalam melakukan Identifikasi Configuration Item (CI) adalah:

a) Configuration Management Team menentukan strategi untuk mendapatkan informasi CI, dan merencanakan kegiatan untuk mengidentifikasi CI.
b) Unit Kerja IT terkait mengidentifikasi dan menyusun CI dari setiap layanan yang menjadi tanggung jawabnya.

2. Rekonsiliasi Pelaporan Konfigurasi

   Aliran Proses dalam melakukan Rekonsiliasi Pelaporan Konfigurasi adalah:

   a) Configuration management database dilakukan proses backup minimal 3 bulan sekali.
   b) Configuration Management Team menentukan lingkup rekonsiliasi dan lingkup CI.

3. Pengendalian Konfigurasi

   Aliran Proses dalam melakukan Pengendalian Konfigurasi adalah:

   a) Unit Kerja IT terkait memeriksa CI dan kelengkapan informasi CI melalui Laporan Hasil Konfigurasi, lalu memastikan keabsahan CI.
   b) Unit Kerja IT terkait melakukan pengecekan hasil penambahan, penghapusan, atau perubahan informasi CI dalam Laporan Hasil Konfigurasi setelah mendapatkan notifikasi closed RFC dan menghasilkan Laporan Hasil Konfigurasi yang telah diperbarui setiap ada perubahan.

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

BAB XI

HUBUNGAN KERJA DENGAN PEMASOK (SUPPLIER)

A. Tujuan

Tujuan dari kebijakan mengenai hubungan kerja dengan pemasok (supplier) adalah untuk memastikan perlindungan atas aset Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang dalam jangkauan akses pemasok dan memelihara tingkat layanan yang disetujui dari Keamanan Informasi sesuai dengan perjanjian dengan pemasok.

B. Ruang Lingkup

Ruang lingkup dari kebijakan mengenai hubungan kerja dengan pemasok (supplier) adalah para pemasok dalam lingkungan Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang.

C. Kebijakan

1. Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang harus mempertimbangkan aspek Keamanan Informasi dalam hubungan dengan pemasok mulai dari pemilihan, penunjukan, monitoring, evaluasi, sampai dengan terminasi.
2. Pemilihan dari penyedia jasa Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang harus mengikuti kriteria berikut:
   a) kompetensi, pengalaman dan catatan dari Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang;
   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);

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

3. Berdasarkan pengelompokan pemasok yang telah bekerja sama, Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang 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. Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang menetapkan persyaratan Keamanan Informasi bagi setiap pemasok yang mengakses Aset Informasi, serta senantiasa memantau kepatuhan pemasok terhadap persyaratan tersebut. Pemasok yang menangani Aset Informasi dengan klasifikasi rahasia perlu menandatangani Perjanjian Kerahasiaan.
5. Kewajiban supplier dan tingkat layanan harus ditetapkan secara formal dalam kontrak kerja;
6. Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang harus memastikan pengelolaan delivery layanan dari pemasok dengan memperhatikan:
    a) layanan yang diserahkan kepada Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang 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. Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang dapat melakukan audit terhadap penyediaan layanan yang diberikan pemasok;
8. Ketentuan dalam pelaksanaan audit kepada pemasok sebagai berikut:

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

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 Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang serta integritas dan ketersediaan dari Informasi dan layanan Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang;
11. Perubahan terhadap layanan yang diberikan oleh supplier harus disetujui oleh manajemen Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang yang relevan dan diformalisasikan dalam kontrak kerja.

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

BAB XII

PENANGANAN INSIDEN KEAMANAN INFORMASI

A. Tujuan

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

B. Ruang Lingkup

Ruang lingkup dari kebijakan penanganan insiden Keamanan Informasi adalah:

1. Tanggung jawab dan prosedur;
2. Pelaporan atas kejadian insiden Keamanan Informasi; dan
3. Pelaporan atas kelemahan Keamanan Informasi.

C. Kebijakan

1. Kejadian Keamanan Informasi adalah sebuah kejadian pada sistem, layanan ataupun jaringan yang dapat mengindikasikan adanya pelanggaran Keamanan Informasi atau kegagalan keamanan atau kejadian yang mungkin memiliki keterkaitan dengan Keamanan Informasi.
2. Kelemahan Keamanan Informasi adalah sebuah kelemahan yang teridentifikasi pada sistem, layanan atau jaringan yang dapat dieksploitasi oleh pihak yang tidak bertanggung jawab dan dapat menyebabkan pelanggaran terhadap kebijakan Keamanan Informasi.
3. Insiden Keamanan Informasi adalah kejadian Keamanan Informasi yang tidak diinginkan dan tidak diperkirakan dimana kejadian tersebut menimbulkan gangguan terhadap operasional bisnis dan mengancam Keamanan Informasi.
4. Guna memastikan proses penanganan insiden yang responsif dan efektif, perlu dikembangkan berbagai prosedur yang mencakup:
   a. perencanaan dan persiapan penanganan insiden;
   b. pemantauan, analisis, dan pelaporan atas insiden;
   c. pencatatan atas aktivitas penanganan insiden;

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

d. penanganan bukti forensik;
e. penilaian dan pengambilan keputusan atas insiden dan kelemahan Keamanan Informasi; dan
f. pemulihan insiden.

5. Seluruh pegawai Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang dan pihak ketiga wajib melaporkan berbagai kejadian insiden Keamanan Informasi maupun yang masih bersifat dugaan atas kelemahan Keamanan Informasi sesegera mungkin, sesuai prosedur pelaporan insiden yang berlaku.
6. Setiap kejadian insiden Keamanan Informasi harus dianalisis, diklasifikasikan, dan ditentukan skala prioritas penanganannya. Penanganan insiden serta pemulihannya dilakukan berdasarkan klasifikasi dan prioritas yang telah ditetapkan.
7. Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang 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 Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang;
      2) minor, apabila insiden tersebut menyebabkan gangguan yang tidak menghentikan proses operasional pekerjaan Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang.
   b) insiden Keamanan Informasi diklasifikasikan berdasarkan tingkat kepentingannya menjadi berikut:
      1) emergency, apabila insiden tersebut dapat atau telah menghentikan proses operasional Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang dan/atau insiden tersebut mempengaruhi secara langsung pimpinan dalam

Catatan :
- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

lingkungan Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang;

2) normal, apabila insiden tersebut tidak menghentikan proses operasional Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang dan/atau insiden tersebut mempengaruhi secara langsung pimpinan dalam lingkungan Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang.

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.

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

BAB XIII
MANAJEMEN PERUBAHAN

A. Tujuan

Tujuan dari dokumen ini adalah untuk memastikan bahwa perubahan dari suatu pengelolaan sistem informasi yang mempunyai dampak terhadap aspek keamanan informasi bagi operasional layanan TIK organisasi dapat dikendalikan.

B. Ruang Lingkup

Ruang Lingkup dari pengelolaan perubahan ini meliputi :

1. semua pengelolaan perubahan sistem informasi yang mencakup infrastruktur, aplikasi, manusia, dan informasi.
2. perubahan yang dimaksud dalam dokumen ini tidak terbatas pada perubahan yang terjadi pada sistem informasi tetapi termasuk pada perubahan struktur organisasi dan alur kerja yang ada pada perusahaan.
3. pengelolaan perubahan ini juga dilakukan untuk patch, release aplikasi, perubahan kapasitas pada infrastruktur yang sudah siap untuk dilakukan perubahan pada lingkungan produksi.

C. Kebijakan

1. Seluruh perubahan dalam infrastruktur TIK dan sistem aplikasi harus dikelola dan dikendalikan untuk menghindari terjadinya kegagalan dalam sistem informasi.
2. Pengendalian perubahan diterapkan pada infrastruktur dan sistem harus mengacu pada prosedur yang mempertimbangkan antara lain:
   a) Analisis potensi risiko dan dampak yang muncul terhadap perubahan tersebut termasuk dampak terhadap keamanan informasi organisasi yang dapat muncul dari perubahan tersebut;
   b) Dokumentasi atas log perubahan sesuai urutan waktu perubahan;
   c) Perencanaan dan pengujian perubahan;

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

d) Penyediaan rencana fallback untuk pemulihan bila terjadi kegagalan perubahan;
e) Tersedianya persetujuan formal untuk usulan perubahan;
f) Komunikasi seluruh detail dari perubahan kepada personel yang relevan;
g) Review dan pemantauan terhadap pelaksanaan perubahan.

3. Berdasarkan tingkat kepentingannya, perubahan digolongkan menjadi :
   a) Perubahan darurat (emergency), perubahan dengan prioritas tinggi, yang jika tidak segera diimplementasikan, berpotensi menimbulkan dampak yang signifikan bagi pelayanan operasional Pemerintah Kabupaten Sumedang. Perubahan ini harus direview sesuai manajemen perubahan Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang. Risiko signifikan misalnya : mengganggu kinerja/pencapaian sasaran organisasi, menyebabkan keluhan (complaint) user, tertundanya pekerjaan/proyek, mengganggu operasional layanan DC atau layanan TI lainnya.
   b) Perubahan normal, adalah perubahan yang telah direncanakan terlebih dahulu baik yang tipenya perubahan major atau minor. Perubahan dengan prioritas sedang, yang jika tidak diimplementasikan dapat menyebabkan gangguan lanjutan pada sistem/layanan TI, infrastruktur atau perangkat pendukung lainnya.
   c) Perubahan standar, perubahan dengan prioritas biasa, yang menjadi bagian dari operasional layanan TI atau bagian dari perawatan yang sudah ditetapkan sebagai bagian dari perawatan atau menjadi tugas rutin dari pelaksana/Helpdesk TI.
4. Implementasi perubahan harus dipastikan dilakukan pada waktu yang tepat dan tidak mengganggu proses operasional.
5. Setiap perubahan yang dilakukan perlu disetujui dan didokumentasikan.

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

BAB XIV
EVALUASI KINERJA

A. Tujuan

Standar ini bertujuan untuk memberi suatu acuan dan pedoman cara mengelola evaluasi kinerja Sistem Manajemen Keamanan Informasi pada Dinas Komunikasi, Informasi, Persandian dan Statistik sehingga kinerja sistem dapat terus dipantau untuk dapat menjadi panduan dalam perbaikan berkesinambungan untuk dapat terus melindungi informasi dari ancaman kehilangan kerahasiaan (*Confidentiality*), keutuhan (*Integrity*) dan ketersediaan (*Availability*).

B. Ruang Lingkup

Ruang lingkup dari evaluasi kinerja ini sesuai dengan batasan ruang lingkup implementasi Sistem Manajemen Keamanan Informasi.

C. Kebijakan

1. Pengukuran Sasaran Keamanan Informasi
    a) Wakil Manajemen beserta tim keamanan menyusun rencana sasaran keamanan informasi berdasarkan hasil penilaian risiko yang telah dilakukan pada tahap perencanaan
    b) Sasaran keamanan informasi yang telah disusun diajukan kepada pimpinan puncak untuk proses persetujuan
    c) Berdasarkan sasaran yang telah disetujui, setiap koordinator melakukan pengukuran dan evaluasi sesuai dengan frekuensi pengukuran dan evaluasi;
    d) Hasil pengukuran dan evaluasi dilaporkan kepada Wakil Manajemen untuk ditinjau dan diberikan persetujuan
    e) Seluruh hasil pengukuran dan evaluasi sasaran keamanan informasi dilaporkan kepada pimpinan puncak pada saat rapat tinjauan manajemen

Catatan :
- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

2. Internal Audit

Pelaksanaan Internal Audit dilakukan dengan beberapa tahapan proses sebagai berikut :

a. Persyaratan Umum

1) Audit Internal dilakukan minimal 1 (satu) kali setahun. Rencana Audit Tahunan untuk berbagi jenis audit disusun dalam Formulir Program Audit Tahunan, sedang rencana audit internal untuk 1(satu) jenis audit seperti audit ISO 27001 disusun dalam Formulir Rencana Audit Internal.
2) Audit dilakukan tidak ditujukan untuk mencari kesalahan tetapi untuk memberi masukan terhadap efektivitas penerapan SMKI.
3) Kepala Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang selaku Manajemen Puncak menunjuk Auditor Internal untuk menjalankan proses audit internal di Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang.
4) Auditor Internal dapat berasal dari internal Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang atau dari pihak eksternal yang ditetapkan dan bertindak sebagai auditor internal bagi Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang.
5) Kepala Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang menetapkan Auditor untuk melaksanakan Internal Audit berdasarkan kepada kualifikasi Auditor:
   a) Auditor harus independen terhadap area yang diaudit.
   b) Pengalaman kerja yang memadai (pengalaman kerja yang berhubungan dengan standard Keamanan informasi, dapat dipertimbangkan) .
   c) Pernah mengikuti pelatihan awareness ISO 27001:2022.
   d) Pernah mengikuti pelatihan Internal Auditor Sistem Manajemen Keamanan Informasi.

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

6) Auditor internal dapat terdiri dari 1 (satu) orang atau lebih. Jika lebih dari 1 (satu) orang, maka perlu ditetapkan seorang Ketua Tim Audit (Lead Auditor) dan yang lain sebagai anggota tim Auditor. Jika hanya 1 (satu) orang maka auditor internal bertindak sebagai Ketua Tim Audit yang menjalankan tugas dan fungsi seluruh proses audit.

b. Pengelolaan Program Audit Tahunan

1) Pimpinan SMKI bertanggung jawab menyusun program audit tahunan yang minimal terdiri dari:
   a) Jenis audit
   b) Ruang lingkup audit.
   c) Jadwal tiap jenis audit secara garis besar, dan
   d) Auditor
2) Program Audit dapat disusun di awal tahun atau sebelum proses audit keamanan informasi dan sebagai acuan dalam membuat rencana audit dan penunjukan Tim Internal Auditor.
3) Kepala Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang menetapkan auditor internal melalui :
   a) Penerbitan Surat Keputusan Tim Auditor Internal untuk auditor internal dari Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang, atau
   b) Kontrak dengan pihak eksternal yang akan ditugaskan melakukan audit internal atas nama Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang

   Dalam hal kondisi tertentu Kepala Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang dapat mendelegasikan penetapan Audit Internal Kepada Kepala Bidang Informatika selaku Perwakilan Manajemen.

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

c. Perencanaan Audit

1) Auditor Internal menyiapkan rencana audit berkoordinasi dengan Kepala Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang dengan mempertimbangkan ketersediaan *Auditee.* Rencana Audit didokumentasikan menggunakan Formulir Rencana Audit Internal, dan memuat informasi antara lain:
   a) Satuan Kerja (Bidang/SubBidang)
   b) Standar/Kriteria Audit
   c) Jadwal Audit
   d) Proses/area yang diaudit
   e) *Auditee*
   f) Auditor
   g) Lokasi
2) Rencana audit didistribusikan kepada auditee sebelum audit dilaksanakan.
3) Sebelum pelaksanaan Audit, Auditor dapat menyiapkan *Checklist* Audit atau daftar pertanyaan sebagai alat bantu untuk memperlancar proses audit.
4) *Auditee* mempersiapkan bukti/catatan pelaksanaan SMKI sesuai ruang lingkup audit di unit kerjanya.

d. Pelaksanaan Audit

1) Auditor Internal memimpin Rapat Pembukaan (*Opening Meeting*) dan menyampaikan tujuan, ruang lingkup dan jadwal Internal Audit yang telah disusun.
2) Auditor Internal melaksanakan Internal Audit sesuai dengan ruang lingkup dan jadwal yang telah ditetapkan. Metode audit meliputi antara lain:
   a) Melakukan pemeriksaan dokumen SMKI yang berlaku;
   b) Wawancara dengan auditee untuk mengumpulkan dan memverifikasi bukti penerapan SMKI;

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

c) Observasi secara langsung (*on-site*) dan/atau secara *remote (video conference/virtual*) terhadap lokasi dan penerapan kontrol keamanan informasi;

d) Menggunakan teknik sampling dalam proses pengumpulan informasi dan bukti penerapan

3) Setelah melakukan Audit *on-site* dan/atau *remote*, Auditor mengemukakan temuan berupa :

a) Ketidaksesuaian Major yaitu bila memenuhi kriteria sebagai berikut:

- Adanya persyaratan ISO 27001:2022 yang tidak dilaksanakan secara keseluruhan di unit kerja atau proses yang diaudit;
- Risiko ketidaksesuaian berada pada tingkat/level: Tinggi / Sangat Tinggi

b) Ketidaksesuaian Minor yaitu bila memenuhi kriteria sebagai berikut:

- Adanya persyaratan ISO 27001:2022 yang tidak dilaksanakan di salah satu atau sebagian kecil dari unit kerja/proses yang diaudit;
- Risiko ketidaksesuaian berada pada tingkat/level: Sangat Rendah / Rendah/Sedang

Peluang peningkatan (*Opportunity For Improvement/OFI*) yaitu temuan yang tidak mempengaruhi efektivitas SMKI namun bila dilakukan akan meningkatkan kinerja SMKI.

4) Temuan dicatat dalam Formulir Permintaan Tindakan Perbaikan .

5) Auditor memastikan *Auditee* menandatangani Formulir Permintaan Tindakan Perbaikan sebagai persetujuan terhadap ketidaksesuaian yang ditemukan dan batas waktu tindakan perbaikannya.

6) Auditor bertanggung jawab menyiapkan kesimpulan Audit, yang mengemukakan :

a) Kesesuaian penerapan sistem manajemen terhadap kriteria Audit.

b) Kondisi ketidaksesuaian dengan merujuk persyaratan ISO 27001:2022.

c) Saran perbaikan terhadap ketidaksesuaian, jika diperlukan

d) Hal-hal yang sebaiknya ditingkatkan (*improvement*).

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

7) Auditor melaporkan hasil Audit kepada Kepala Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang untuk dirangkum dan dilaporkan pada saat Rapat Tinjauan Manajemen.

e. Menyelesaikan Audit

1) Auditor bertanggung jawab menyimpan dan memelihara Formulir Permintaan Tindakan Perbaikan, sebagai acuan untuk menindaklanjuti ketidaksesuaian dan mengevaluasi pelaksanaan Audit secara keseluruhan.
2) Audit dinyatakan selesai bila semua kegiatan pada jadwal Audit telah dilaksanakan dan Laporan Audit sudah didistribusikan

f. Tindak-lanjut Audit

1) Formulir Permintaan Tindakan Perbaikan wajib ditindaklanjuti oleh *Auditee* dengan mengisi tindakan perbaikan, penyebab ketidaksesuaian dan rencana tindakan korektif dan dikembalikan kepada Auditor dengan batas waktu tujuh (7) hari kerja setelah laporan audit diterima auditee. Apabila ada kondisi yang menyebabkan batas waktu terlewati, maka auditee perlu berkoordinasi dengan Auditor dan/atau untuk diteruskan kepada Kepala Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang untuk pengaturan ulang batas waktunya.
2) Sesuai Permintaan Tindakan Perbaikan, *Auditee* melakukan tindakan perbaikan terhadap ketidaksesuaian yang ditemukan saat internal Audit, sesuai dengan batas waktu yang telah disepakati.
3) Auditor melakukan verifikasi terhadap tindakan perbaikan, rencana tindakan korektif yang telah dilaksanakan dan menilai efektivitasnya.
4) Apabila tindakan perbaikan dan rencana tindakan korektif dinyatakan efektif, maka status ketidaksesuaian dinyatakan telah selesai atau status ditutup.
5) Auditor Internal melakukan verifikasi akhir terhadap Formulir Tindakan Perbaikan.

3. Tinjauan Manajemen

a. Top Manajemen dan/atau CISO merencanakan proses tinjauan manajemen dengan langkah-langkah sebagai berikut:

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

1) Menyiapkan program tinjauan manajemen dalam periode tahunan. Pelaksanaan tinjauan Manajemen minimal 1 kali dalam setahun.
2) Menetapkan agenda rapat sebagai standar persyaratan yang wajib dibahas dalam rapat tinjauan manajemen.
3) Membuat undangan rapat tinjauan manajemen dan menginformasikan undangan tersebut kepada pimpinan puncak dan departemen yang terlibat dalam SMKI
4) Memimpin proses opening meeting dan memandu proses rapat tinjauan manajemen

b. Agenda wajib rapat harus mencakup hal sebagai berikut :
   1) Tindak Lanjut dari Rapat Tinjauan Manajemen Sebelumnya
   2) Isu eksternal dan internal yang relevan dengan SMKI
   3) *Feedback* terhadap kinerja keamanan informasi:
      a) Ketidaksesuaian dan tindakan korektif/perbaikan;
      b) Hasil pemantauan dan pengukuran;
      c) Hasil Internal Audit SMKI; dan
      d) Pemenuhan terhadap sasaran keamanan informasi.
   4) *Feedback* dari pihak yang berkepentingan
   5) Hasil penilaian risiko dan status rencana penanganan risiko
   6) Peluang untuk perbaikan berkelanjutan.

c. Peserta rapat melakukan proses rapat tinjauan manajemen sesuai dengan agenda input meeting yang telah ditetapkan

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

d. Pengendali Dokumen mencatat seluruh hasil rapat tinjauan manajemen yang dituangkan dalam Notulen rapat dan Menyiapkan notulen rapat dan disampaikan pada pimpinan puncak untuk diketahui dan disetujui
e. Top Management menyetujui hasil notulen rapat dan menyerahkan kembali kepada Wakil Manajemen untuk didistribusikan kepada peserta rapat
f. Peserta rapat menerima hasil notulen rapat dan melaksanakan seluruh hasil rapat tersebut
g. Pengendali dokumen menyimpan seluruh bukti rapat tinjauan manajemen seperti Notulen rapat, daftar hadir dan slide presentasi (jika ada)

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

d) Tinjauan Manajemen

a) Top Manajemen dan/atau CISO merencanakan proses tinjauan manajemen dengan langkah-langkah sebagai berikut:
   1) Menyiapkan program tinjauan manajemen dalam periode tahunan. Pelaksanaan tinjauan Manajemen minimal 1 kali dalam setahun.
   2) Menetapkan agenda rapat sebagai standar persyaratan yang wajib dibahas dalam rapat tinjauan manajemen.
   3) Membuat undangan rapat tinjauan manajemen dan menginformasikan undangan tersebut kepada pimpinan puncak dan departemen yang terlibat dalam SMKI
   4) Memimpin proses opening meeting dan memandu proses rapat tinjauan manajemen
b) Peserta rapat melakukan proses rapat tinjauan manajemen sesuai dengan agenda input meeting yang telah ditetapkan.
c) Pengendali Dokumen mencatat seluruh hasil rapat tinjauan manajemen yang dituangkan dalam Notulen rapat dan Menyiapkan notulen rapat dan disampaikan pada pimpinan puncak untuk diketahui dan disetujui
d) Top Management menyetujui hasil notulen rapat dan menyerahkan kembali kepada Wakil Manajemen untuk didistribusikan kepada peserta rapat
e) Peserta rapat menerima hasil notulen rapat dan melaksanakan seluruh hasil rapat tersebut
f) Pengendali dokumen menyimpan seluruh bukti rapat tinjauan manajemen seperti Notulen rapat, daftar hadir dan slide presentasi (jika ada)

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

BAB XV

PENANGANAN KETIDAKSESUAIAN DAN PERBAIKAN

A. Tujuan

Untuk menetapkan tindakan yang diperlukan untuk melakukan koreksi (perbaikan), apabila sesuatu hal terjadi agar kejadian yang sama tidak terulang kembali.

B. Ruang Lingkup

Prosedur ini berlaku di seluruh jajaran Dinas Komunikasi, Informasi, Persandian dan Statistik dan diterapkan terhadap masalah yang muncul, baik yang ditemukan secara internal maupun yang berasal eksternal.

C. Kebijakan

1. Identifikasi Potensi dan Ketidaksesuaian
   a) Masing-masing satuan kerja melakukan identifikasi (potensi) ketidaksesuaian atau penyimpangan yang terjadi berdasarkan hasil :
      1) Pemantauan, Pengukuran, dan Evaluasi Kegiatan
      2) Hasil Audit Internal/eksternal
      3) Laporan insiden/kerusakan/gangguan;
      4) Keluhan dari pihak-pihak terkait
      5) Rekomendasi Tinjauan Manajemen;
      6) Laporan insiden/kerusakan/gangguan lainnya,
   b) Pimpinan terkait melakukan analisa akar penyebab (potensi) ketidaksesuaian berdasarkan hasil identifikasi (potensi) ketidaksesuaian tersebut.
   c) Analisa potensi akar penyebab ketidaksesuaian dapat ditetapkan dengan metode analisa alat perbaikan, sebagai pertimbangan alternatif faktor penyebab seperti :
      1) Faktor pekerja/karyawan (*Human*)
      2) Faktor metode/cara yang digunakan (*Method*) pekerja
      3) Faktor penggunaan peralatan (*Machine*)

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

4) Faktor kondisi lingkungan (*Working Environment*)

d) Faktor tersebut dapat dipertimbangkan melalui kegiatan diskusi antara pimpinan terkait, dan atau melibatkan pihak eksternal terkait.

e) Hasil kesepakatan dan analisa bersama dari diskusi, dapat ditetapkan salah satu atau lebih sebagai penyebab (potensi) ketidaksesuaian, sehingga dapat disimpulkan tindakan koreksi yang dapat dilakukan secara tepat. Untuk menetapkan faktor penyebab tersebut perlu dilakukan pengukuran dan atau pengujian, guna didapat sebuah keputusan tindakan koreksi atau pencegahan yang tepat berdasarkan analisis data yang representatif.

2. Pelaksanaan Tindakan Koreksi

a) Satuan kerja terkait melakukan identifikasi masalah / gangguan / kerusakan atau ketidaksesuaian (non conformity) baik dari hasil:
   1) Pemantauan rutin.
   2) Laporan gangguan/insiden.
   3) Hasil internal/eksternal audit
   4) Laporan identifikasi masalah lainnya

b) Satuan kerja terkait melakukan perbaikan masalah / gangguan / kerusakan atau ketidaksesuaian (nonconformity).

c) Pimpinan Unit Kerja terkait memeriksa dan menganalisa apakah perbaikan/penyelesaian masalah sudah efektif menyelesaikan akar masalah (root cause analysis):
   1) Jika sudah, lanjutkan ke langkah point g
   2) Jika belum, lakukan analisa penyebab masalah dan lanjutkan ke langkah point d.

d) Pimpinan Satuan Kerja terkait melakukan analisa penyebab masalah dan menugaskan tindakan korektif untuk mengatasi penyebab masalah agar masalah tidak berulang.

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

e) Satuan kerja terkait melakukan tindakan korektif dan pengendalian sesuai dengan penugasan yang diterima.
f) Pimpinan Satuan Kerja terkait memonitor dan mereview efektivitas tindakan koreksi atau perubahan yang telah dilakukan:
    1. Jika sudah tepat dan efektif, lanjut ke langkah point g
    2. Jika belum tepat, kembali ke langkah point c
g) Satuan kerja terkait mencatat dan melaporkan status tindakan perbaikan dan tindakan korektif.

Pimpinan Satuan Kerja terkait menerima laporan tindakan perbaikan dan tindakan korektif, termasuk status penyelesaiannya.

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

BAB XIV

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. Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang 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. Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang 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. Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang harus menetapkan prasyarat untuk keberlanjutan Keamanan Informasi dan diintegrasikan dengan prasyarat keberlanjutan bisnis Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang untuk menjamin keberlanjutan dari

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

Keamanan Informasi di Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang, pada saat dan setelah terjadinya gangguan besar atau bencana.

4. Prasyarat Keamanan Informasi dapat diintegrasikan pada siklus process business continuity management (BCM) yang mencakup:
   a) memahami kebutuhan Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang;
   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 Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang serta pemberian layanan Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang kepada pelanggan.
6. Apabila prasyarat redundan tidak dapat dipenuhi, maka proses alternatif perlu ditetapkan untuk menjamin ketersediaan dari proses bisnis dan operasional Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang serta delivery dari layanan Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang 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 disebut sebagai fasilitas backup site.

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

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.

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

BAB XV
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 Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang.

B. Ruang Lingkup

Ruang lingkup dari kebijakan mengenai kepatuhan:

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

C. Kebijakan

1. Dinas Komunikasi dan Informatika, Persandian dan Statistik 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 Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang harus diidentifikasikan, didokumentasikan dan dipelihara;
3. Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang harus mematuhi hak atas kekayaan intelektual yang terkait dengan material yang digunakan oleh Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang seperti:
   a) penggunaan perangkat lunak dan material yang bersifat proprietary harus mematuhi undang-undang terkait hak atas kekayaan intelektual (haki) yang berlaku;

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

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 Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang harus dilindungi dari kehilangan, pemalsuan, kerusakan, atau penyalahgunaan sesuai dengan peraturan perundangan-undangan, regulasi, dan persyaratan kontrak dan bisnis;
5. Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang harus memastikan privasi dan perlindungan terhadap Informasi terkait dengan pribadi (personally identifiable information) sesuai dengan prasyarat hukum, perundangan, regulasi dan kontraktual;
6. Kepala Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang harus secara rutin memantau dan meninjau kepatuhan dari personil, proses kerja dan pemrosesan Informasi dalam area tanggung jawabnya terhadap kebijakan dan standar Keamanan Informasi Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang serta prasyarat Keamanan Informasi yang berlaku;
7. Pada saat terjadi ketidaksesuaian, pimpinan Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang bertanggung jawab untuk menangani ketidaksesuaian yang terjadi sesuai dengan kebijakan terkait penanganan ketidaksesuaian dan peningkatan SMKI;
8. Sistem Informasi Satuan Kerja Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang 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

Catatan :
- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

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.

Ditetapakan di : S u m e d a n g
Pada Tanggal : 07 Juni 2023

Balai Sertifikasi Elektronik

SUMEDANG
DIGITAL SIGNATURE

Ditandatangani Secara Elektronik Oleh:

BAMBANG RIANTO, S.STP, M.Si
NIP. 197704201996021001

Kepala Dinas Komunikasi dan Informatika, Persandian dan Statistik

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

Lampiran II : Surat Keputusan Kepala Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang
No : 53 Tahun 2023
Tanggal : 07 Juli 2023
Tentang : Gambaran Umum dan Teknis Pelaksanaan IT Manajemen Risiko Pada Dinas Komunikasi dan Informatika, Persandian dan Statistik Kabupaten Sumedang

1. Latar Belakang

   IT Risk Management dilakukan dalam rangka mendukung proses kontrol Lembaga pada saat melaksanakan kegiatan Teknologi Informasi dimana Kontrol ini sebagai panduan manajemen agar pelaksanaan kegiatan Teknologi Informasi dapat terhindar dari hal-hal yang tidak diinginkan oleh Dinas terkait.

2. Maksud dan Tujuan

   Petunjuk Teknis ini bertujuan untuk mengatur pengelolaan risiko terkait TI Operasional di Lembaga agar pelaksanaan proses bisnis berbasis TI dapat dilindungi secara efisien dan efektif

3. Ruang Lingkup

   Petunjuk Teknis ini hanya berlaku di lingkungan Penyelenggara Sistem Manajemen Keamanan Informasi Lembaga dalam menjalankan aktivitas Teknologi Informasi pada kegiatan identifikasi risiko TI, penilaian risiko TI, pengendalian risiko TI dan pemantauan risiko TI.

4. Ketentuan Umum
   a. Identifikasi dan Penilaian Risiko (*Risk Assessment*)
      Dimana ketentuan yang perlu diperhatikan dalam melakukan identifikasi penilaian risiko adalah sebagai berikut:
      1) Unit yang menangani kegiatan Manajemen Aset dan Risiko menggunakan pendekatan manajemen risiko yang terpadu untuk melakukan identifikasi, pengukuran, pemantauan dan pengendalian risiko secara efektif.

Catatan :
- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

2) Unit yang menangani kegiatan Manajemen Aset dan Risiko melakukan identifikasi risiko dengan melihat asset dan proses yang dimiliki dan dijalankan oleh Lembaga saat ini dengan menganalisa sensitivitas dan kritikalitas dari masing-masing aset dan proses yang ada.
3) Unit yang menangani kegiatan Manajemen Aset dan Risiko melakukan identifikasi ancaman dan kerawanan dari aset yang dimiliki oleh bank saat ini.
4) Unit yang menangani kegiatan Manajemen Aset dan Risiko untuk melakukan Analisa dan menentukan Nilai risiko dasar (*Inherent Risk*) dengan melihat Analisa dampak dan Kemungkinan / kecenderungan dari masing-masing risiko.
5) Pengukuran dampak merupakan pengukuran terhadap seberapa besar dampak yang ditimbulkan oleh sebuah resiko apabila risiko tersebut terjadi (tereksploitasi). Kriteria dampak ini dikategorikan dalam 5 tingkatan.
6) Pelaksanaan analisa dampak ini mengacu pada tujuan pengamanan terhadap aset yang berkaitan dengan proses bisnis dan akibat yang ditimbulkan berdasarkan kerugian dari aspek seperti berikut:
   a) Kerahasiaan dan Integritas pada suatu data dan informasi yang dikelola Lembaga
   b) Ketersediaan informasi dalam menunjang operasional layanan Lembaga.
7) Berdasarkan analisa dampak dari Kedua aspek tersebut maka kriteria evaluasi dampak risiko yang digunakan oleh Lembaga dapat dilihat pada tabel berikut.

Level Dampak	Reputasi	Operasional	Hukum	Privasi
1 (Sangat Ringan)	Terdapat pemberitaan negatif namun tidak mengakibatkan penurunan kepercayaan stakeholder	Penundaan proses bisnis 1 hari	Terdapat permasalahan hukum (misal pelanggaran) namun belum menjadi tuntutan	Tidak Terdapat kebocoran data pribadi

Catatan :
- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

Level Dampak	Reputasi	Operasional	Hukum	Privasi
2 (Ringan)	Terdapat pemberitaan negatif namun tidak mengakibatkan penurunan kepercayaan stakeholder	Penundaan proses bisnis 12 jam	Terdapat permasalahan hukum (misal pelanggaran) namun belum menjadi tuntutan	Tidak Terdapat kebocoran data pribadi
3 (Sedang)	Terdapat pemberitaan negatif yang dapat mempengengaruhi kepercayaan sebagian kecil dari stakeholder	Penundaan proses bisnis 2 jam	Tuntutan hukum dengan dampak relatif kecil	Terdapat kebocoran data pribadi
4 (Berat)	Terdapat pemberitaan negatif yang dapat mengakibatkan penurunan kepercayaan sebagian besar dari stakeholder	Penundaan pada saat sistem tidak berjalan lebih 30 menit	Tuntutan hukum berdampak pada kinerja/performa organisasi	Terdapat kebocoran data pribadi
5 (Sangat Berat)	Terdapat pemberitaan negatif yang dapat menghilangkan kepercayaan dari stakeholder	Penundaan pada saat sistem tidak berjalan lebih 10 menit	Tuntutan hukum mengancam eksistensi dan manajemen puncak organisasi	Terdapat kebocoran data pribadi

8) Pengukuran Kemungkinan / kecenderungan terjadinya risiko dikategorikan ke dalam 5 tingkatan. Tabel di bawah ini adalah keterangan lengkap mengenai tingkatan kemungkinan / kecenderungan yang berlaku di Lembaga beserta penjelasannya masing-masing.

Level Kemungkinan / Kecenderungan		Deskripsi
5	**Sangat Mungkin**	Terjadi lebih dari 15 kali dalam 1 tahun
4	**Mungkin**	Terjadi 11 – 14 kali dalam 1 tahun
3	**Besar Kemungkinan**	Terjadi 7-10 kali dalam 1 tahun
2	**Kecil Kemungkinan**	Terjadi 3- 6 kali dalam 1 tahun
1	**Tidak Mungkin**	Terjadi hanya 1-2 kali dalam 1 tahun

9) Setelah tingkat Kemungkinan / kecenderungan dan dampak dari tiap risiko diidentifikasi, selanjutnya dilakukan penentuan nilai risiko dasar. Nilai risiko inheren adalah tingkatan risiko yang timbul apabila tidak adanya kontrol.

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

10) Nilai risiko dasar (*Inherent Risk*) diperoleh dari hasil perhitungan antara tingkat Kemungkinan / kecenderungan dan juga dampak dari risiko sebagai berikut ini:
    a) Nilai risiko = Kemungkinan / kecenderungan × Dampak
    b) Kriteria risiko dasar (*Inherent Risk*) adalah sebagai berikut:
        - Nilai 1 – 5 : Low
        - Nilai 5 - 10 : Low to Moderate
        - Nilai 10 - 15 : Moderate
        - Nilai 15 – 20 : Moderate to High
        - Nilai 20 – 25 : High
11) Berikut adalah deskripsi tingkat Nilai risiko dasar (*Inherent Risk*) yang dijadikan acuan dalam melakukan penilaian risiko:

Peringkat	Level	Definisi Peringkat
Low (1)	1	Dengan mempertimbangkan aktivitas bisnis yang dilakukan Lembaga, kemungkinan kerugian yang dihadapi Lembaga dari Risiko Operasional tergolong sangat rendah selama periode waktu tertentu pada masa datang. Contoh karakteristik Lembaga yang termasuk dalam peringkat Low (1) antara lain sebagai berikut: a. Proses bisnis Lembaga memiliki karakteristik yang sangat sederhana. Layanan tidak bervariasi, mekanisme proses bisnis sangat sederhana, volume transaksi rendah, struktur organisasi tidak kompleks, tidak terdapat aksi korporasi yang signifikan, dan penggunaan alih daya sangat minimal. b. Sumber daya manusia sangat memadai, baik dari sisi kecukupan kuantitas maupun kualitas sumber daya manusia. Data historis

Catatan :
- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

Peringkat	Level	Definisi Peringkat
		kerugian akibat kesalahan manusia tidak signifikan. c. Teknologi informasi sangat matang (mature) dan tidak terdapat perubahan signifikan dalam sistem teknologi informasi. Kerentanan teknologi informasi terhadap gangguan atau serangan sangat rendah. Infrastruktur pendukung sangat andal dalam mendukung aktivitas Lembaga. d. Frekuensi dan materialitas fraud internal dan eksternal sangat rendah dan kerugian yang disebabkan tidak signifikan dibandingkan dengan volume transaksi. e. Ancaman gangguan proses bisnis sebagai akibat dari kejadian eksternal sangat rendah
Low to Moderate (2)	2	Dengan mempertimbangkan aktivitas bisnis yang dilakukan Lembaga, kemungkinan kerugian finansial yang dihadapi Lembaga dari Risiko Operasional rendah selama periode waktu tertentu pada masa datang. Contoh karakteristik Lembaga yang termasuk dalam peringkat Low to Moderate (2) antara lain sebagai berikut: a. Proses bisnis Lembaga memiliki karakteristik yang sangat sederhana. Layanan relatif kurang bervariasi, mekanisme proses bisnis sederhana, volume transaksi relatif rendah, struktur organisasi kurang kompleks, aksi korporasi kurang signifikan, dan penggunaan alih daya minimal. b. Sumber daya manusia memadai, baik dari sisi kecukupan kuantitas maupun kualitas sumber daya manusia. Data historis kerugian akibat kesalahan manusia kurang signifikan.

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

Peringkat	Level	Definisi Peringkat
		c. Teknologi informasi relatif sudah matang (mature) dan tidak terdapat perubahan signifikan dalam sistem teknologi informasi. Kerentanan teknologi informasi terhadap gangguan atau serangan rendah. Infrastruktur pendukung andal dalam mendukung aktivitas Lembaga. d. Frekuensi dan materialitas fraud internal dan eksternal rendah dan kerugian yang disebabkan kurang signifikan dibandingkan dengan volume transaksi Lembaga. e. Ancaman gangguan aktivitas sebagai akibat dari kejadian eksternal rendah.
Moderate (3)	3	Dengan mempertimbangkan aktivitas bisnis yang dilakukan Lembaga, kemungkinan kerugian finansial yang dihadapi Lembaga dari Risiko Operasional tergolong cukup tinggi selama periode waktu tertentu pada masa datang. Contoh karakteristik Lembaga yang termasuk dalam peringkat Moderate (3) ini antara lain sebagai berikut: a. Proses Bisnis Lembaga memiliki karakteristik yang cukup kompleks. Layanan cukup bervariasi, mekanisme bisnis cukup kompleks, volume transaksi cukup tinggi, struktur organisasi cukup kompleks, aksi korporasi cukup signifikan, dan penggunaan alih daya cukup signifikan. b. Sumber daya manusia cukup memadai, baik dari sisi kecukupan kuantitas maupun kualitas. Data historis kerugian akibat kesalahan manusia cukup signifikan. c. Teknologi informasi menuju proses kematangan dan dapat terjadi perubahan

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

Peringkat	Level	Definisi Peringkat
		signifikan dalam sistem teknologi informasi. Teknologi informasi cukup rentan terhadap gangguan atau serangan. Infrastruktur pendukung cukup andal dalam mendukung aktivitas Lembaga. d. Frekuensi dan materialitas fraud internal dan eksternal cukup tinggi dan kerugian yang disebabkan cukup signifikan dibandingkan dengan volume transaksi. e. Ancaman gangguan aktivitas sebagai akibat dari kejadian eksternal cukup tinggi.
Moderate to High (4)	4	Dengan mempertimbangkan aktivitas bisnis yang dilakukan Lembaga, kemungkinan kerugian yang dihadapi Lembaga dari Risiko Operasional tergolong tinggi selama periode waktu tertentu pada masa datang. Contoh karakteristik Lembaga yang termasuk dalam peringkat Moderate to High (4) antara lain sebagai berikut: a. Proses bisnis Lembaga memiliki karakteristik yang kompleks. Layanan bervariasi, mekanisme bisnis kompleks, volume transaksi tinggi, struktur organisasi kompleks, aksi korporasi signifikan, dan penggunaan alih daya signifikan. b. Sumber daya manusia memadai, baik dari sisi kecukupan kuantitas maupun kualitas. Data historis kerugian akibat kesalahan manusia signifikan. c. Teknologi informasi belum matang dan terjadi perubahan signifikan dalam sistem Teknologi informasi. Teknologi informasi rentan terhadap gangguan atau serangan.

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

Peringkat	Level	Definisi Peringkat
		Infrastruktur pendukung kurang andal dalam mendukung aktivitas Lembaga. d. Frekuensi dan materialitas fraud internal dan eksternal tinggi dan kerugian yang disebabkan signifikan dibandingkan dengan volume transaksi. e. Ancaman gangguan aktivitas sebagai akibat dari kejadian eksternal tinggi.
High (5)	5	Dengan mempertimbangkan aktivitas bisnis yang dilakukan Lembaga, kemungkinan kerugian yang dihadapi Lembaga dari Risiko Operasional tergolong sangat tinggi selama periode waktu tertentu pada masa datang. Contoh karakteristik Lembaga yang termasuk dalam peringkat High (5) antara lain sebagai berikut: a. Proses bisnis Lembaga memiliki karakteristik yang sangat kompleks. Layanan sangat bervariasi, mekanisme bisnis sangat kompleks, volume transaksi sangat tinggi, struktur organisasi sangat kompleks, aksi korporasi signifikan, dan penggunaan alih daya sangat tinggi. b. Sumber daya manusia tidak memadai, baik dari sisi kecukupan kuantitas maupun kualitas. Data historis kerugian akibat kesalahan manusia sangat signifikan. c. Teknologi informasi belum matang dan terjadi perubahan signifikan dalam sistem teknologi informasi. Teknologi informasi sangat rentan terhadap gangguan atau serangan. Infrastruktur pendukung tidak andal dalam mendukung aktivitas Lembaga.

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

Peringkat	Level	Definisi Peringkat
		d. Frekuensi dan materialitas fraud internal dan eksternal sangat tinggi dan kerugian yang disebabkan sangat signifikan dibandingkan dengan volume transaksi. e. Ancaman gangguan aktivitas sebagai akibat dari kejadian eksternal sangat tinggi

12) Berikut adalah deskripsi tingkat kualitas penerapan manajemen risiko yang dijadikan acuan dalam melakukan penilaian risiko:

Peringkat	Level	Definisi Peringkat
Strong (1)	1	Kualitas penerapan Manajemen Risiko untuk Risiko Operasional sangat memadai. Terdapat kelemahan minor yang tidak signifikan sehingga dapat diabaikan. Contoh karakteristik Lembaga yang termasuk dalam peringkat Strong (1) antara lain sebagai berikut: a. Perumusan tingkat Risiko yang akan diambil (risk appetite) dan toleransi Risiko (risk tolerance) sangat memadai dan telah sejalan dengan sasaran strategis dan strategi Lembaga secara keseluruhan. b. Manajemen Puncak memiliki kesadaran (awareness) dan pemahaman yang sangat baik mengenai Manajemen Risiko untuk Risiko Operasional. c. Budaya Manajemen Risiko untuk Risiko Operasional sangat kuat dan telah diinternalisasikan dengan sangat baik pada seluruh level organisasi. d. Pelaksanaan tugas Manajemen Puncak secara keseluruhan sangat memadai. e. Fungsi Manajemen Risiko untuk Risiko Operasional independen, memiliki tugas dan tanggung jawab yang jelas serta telah berjalan dengan sangat baik. f. Delegasi kewenangan telah berjalan dengan sangat baik.

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

Peringkat	Level	Definisi Peringkat
		g. Strategi Risiko Operasional sangat sejalan dengan tingkat Risiko yang akan diambil dan toleransi Risiko Operasional. h. Kebijakan dan prosedur Manajemen Risiko serta penetapan limit Risiko Operasional sangat memadai dan tersedia untuk seluruh area Manajemen Risiko untuk Risiko Operasional, sejalan dengan penerapan, dan dipahami dengan baik oleh pegawai. i. Proses Manajemen Risiko untuk Risiko Operasional sangat memadai dalam mengidentifikasi, mengukur, memantau, dan mengendalikan Risiko Operasional. j. *Business continuity management* sangat andal dan sangat teruji. k. Sistem Informasi Manajemen Risiko Operasional sangat baik sehingga menghasilkan Laporan Risiko Operasional yang komprehensif dan terintegrasi kepada Manajemen Puncak. l. Sumber daya manusia sangat memadai dari sisi kuantitas maupun kompetensi pada fungsi Manajemen Risiko untuk Risiko Operasional. m. Sistem pengendalian intern sangat efektif dalam mendukung pelaksanaan Manajemen Risiko untuk Risiko Operasional. n. Pelaksanaan kaji ulang independen oleh satuan kerja audit internal dan fungsi yang melakukan kaji ulang independen sangat memadai baik dari sisi metodologi, frekuensi, maupun pelaporan kepada Manajemen Puncak. o. Secara umum tidak terdapat kelemahan yang signifikan berdasarkan hasil kaji ulang independen. p. Tindak lanjut atas kaji ulang independen telah dilaksanakan dengan sangat memadai.
Satisfactory (2)	2	Kualitas penerapan Manajemen Risiko untuk Risiko Operasional memadai. Terdapat beberapa kelemahan minor yang dapat diselesaikan pada aktivitas bisnis normal. Contoh karakteristik Lembaga yang termasuk dalam peringkat Satisfactory (2) antara lain sebagai berikut: a. Perumusan tingkat Risiko yang akan diambil (risk appetite) dan toleransi Risiko (risk tolerance) memadai dan telah sejalan dengan sasaran strategis dan strategi secara keseluruhan.

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

Peringkat	Level	Definisi Peringkat
		b. Manajemen Puncak memiliki kesadaran (awareness) dan pemahaman yang baik mengenai Manajemen Risiko untuk Risiko Operasional. c. Budaya Manajemen Risiko untuk Risiko Operasional kuat dan telah diinternalisasikan dengan baik pada seluruh level organisasi. d. Pelaksanaan tugas Manajemen Puncak secara umum memadai. Terdapat beberapa kelemahan tetapi tidak signifikan dan dapat diperbaiki dengan segera. e. Fungsi Manajemen Risiko untuk Risiko Operasional independen, memiliki tugas dan tanggung jawab yang jelas, dan telah berjalan dengan baik. Terdapat kelemahan minor, tetapi dapat diselesaikan pada aktivitas bisnis normal. f. Delegasi kewenangan telah berjalan dengan baik. g. Strategi Risiko Operasional sejalan dengan tingkat Risiko yang akan diambil dan toleransi Risiko Operasional. h. Kebijakan dan prosedur Manajemen Risiko serta penetapan limit Risiko Operasional memadai dan tersedia untuk seluruh area Manajemen Risiko untuk Risiko Operasional, sejalan dengan penerapan, dan dipahami dengan baik oleh pegawai meskipun terdapat kelemahan minor. i. Proses Manajemen Risiko untuk Risiko Operasional memadai dalam mengidentifikasi, mengukur, memantau, dan mengendalikan Risiko Operasional. j. *Business continuity management* andal dan teruji. k. Sistem Informasi Manajemen Risiko Operasional baik termasuk pelaporan Risiko Operasional kepada Manajemen Puncak. Terdapat kelemahan minor yang dapat diperbaiki dengan mudah. l. Sumber daya manusia memadai, baik dari segi kuantitas maupun kompetensi pada fungsi Manajemen Risiko untuk Risiko Operasional. m. Sistem pengendalian intern efektif dalam mendukung pelaksanaan Manajemen Risiko untuk Risiko Operasional. n. Pelaksanaan kaji ulang independen oleh satuan kerja audit internal dan fungsi yang melakukan kaji ulang independen memadai baik dari sisi metodologi,

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

Peringkat	Level	Definisi Peringkat
		frekuensi, maupun pelaporan kepada Manajemen Puncak. o. Terdapat kelemahan yang tidak signifikan berdasarkan hasil kaji ulang independen. p. Tindak lanjut atas kaji ulang independen telah dilaksanakan dengan memadai.
Fair (3)	3	Kualitas penerapan Manajemen Risiko untuk Risiko Operasional cukup memadai. Meskipun persyaratan minimum terpenuhi, terdapat beberapa kelemahan yang membutuhkan perhatian manajemen. Contoh karakteristik Lembaga yang termasuk dalam peringkat Fair (3) antara lain sebagai berikut: a. Perumusan tingkat Risiko yang akan diambil (risk appetite) dan toleransi Risiko (risk tolerance) cukup memadai tetapi tidak selalu sejalan dengan sasaran strategis dan strategi secara keseluruhan. b. Manajemen Puncak memiliki kesadaran (awareness) dan pemahaman yang cukup baik mengenai Manajemen Risiko untuk Risiko Operasional. c. Budaya Manajemen Risiko untuk Risiko Operasional cukup kuat dan telah diinternalisasikan dengan cukup baik tetapi belum selalu dilaksanakan secara konsisten. d. Pelaksanaan tugas Manajemen Puncak secara umum cukup memadai. e. Fungsi Manajemen Risiko untuk Risiko Operasional cukup baik, tetapi terdapat beberapa kelemahan yang perlu mendapat perhatian manajemen. f. Delegasi kewenangan telah berjalan dengan cukup baik. g. Strategi Risiko Operasional cukup sejalan dengan tingkat Risiko yang akan diambil dan toleransi Risiko Operasional. h. Kebijakan dan prosedur Manajemen Risiko serta penetapan limit Risiko Operasional cukup memadai tetapi tidak selalu konsisten dengan penerapan. i. Proses Manajemen Risiko untuk Risiko Operasional cukup memadai dalam mengidentifikasi, mengukur, memantau, dan mengendalikan Risiko Operasional. j. *Business continuity management* cukup andal. k. Sistem Informasi Manajemen Risiko memenuhi ekspektasi minimum tetapi terdapat beberapa kelemahan termasuk pelaporan kepada Manajemen Puncak yang membutuhkan perhatian manajemen.

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

Peringkat	Level	Definisi Peringkat
		l. Sumber daya manusia cukup memadai dari sisi kuantitas maupun kompetensi pada fungsi Manajemen Risiko untuk Risiko Operasional. m. Sistem pengendalian intern cukup efektif dalam mendukung pelaksanaan Manajemen Risiko untuk Risiko Operasional. n. Pelaksanaan kaji ulang independen oleh satuan kerja audit internal dan fungsi yang melakukan kaji ulang independen cukup memadai. Terdapat beberapa kelemahan pada metodologi, frekuensi, dan/atau pelaporan kepada Manajemen Puncak yang membutuhkan perhatian manajemen. o. Terdapat kelemahan yang cukup signifikan berdasarkan hasil kaji ulang independen yang memerlukan perhatian manajemen. p. Tindak lanjut atas kaji ulang independen telah dilaksanakan dengan cukup memadai.
Marginal (4)	4	Kualitas penerapan Manajemen Risiko untuk Risiko Operasional kurang memadai. Terdapat kelemahan signifikan pada berbagai aspek Manajemen Risiko untuk Risiko Operasional yang membutuhkan tindakan perbaikan segera. Contoh karakteristik Lembaga yang termasuk dalam peringkat Marginal (4) antara lain sebagai berikut: a. Perumusan tingkat Risiko yang akan diambil (risk appetite) dan toleransi Risiko (risk tolerance) kurang memadai dan tidak sejalan dengan sasaran strategis dan strategi secara keseluruhan. b. Kelemahan signifikan pada kesadaran (awareness) dan pemahaman Manajemen Puncak mengenai Manajemen Risiko untuk Risiko Operasional. c. Budaya Manajemen Risiko untuk Risiko Operasional kurang kuat dan belum diinternalisasikan dengan baik pada setiap level organisasi. d. Pelaksanaan tugas Manajemen Puncak secara umum kurang memadai. Terdapat kelemahan pada berbagai aspek penilaian yang memerlukan perbaikan segera. e. Kelemahan signifikan pada fungsi Manajemen Risiko untuk Risiko Operasional yang memerlukan perbaikan segera. f. Delegasi kewenangan lemah.

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

Peringkat	Level	Definisi Peringkat
		g. Strategi Risiko Operasional kurang sejalan dengan tingkat Risiko yang akan diambil dan toleransi Risiko Operasional. h. Kelemahan signifikan pada kebijakan dan prosedur Manajemen Risiko serta penetapan limit Risiko Operasional. i. Proses Manajemen Risiko untuk Risiko Operasional kurang memadai dalam mengidentifikasi, mengukur, memantau, dan mengendalikan Risiko Operasional. j. *Business continuity management* kurang andal. k. Kelemahan signifikan pada Sistem Informasi Manajemen Risiko Operasional termasuk pelaporan kepada Manajemen Puncak yang memerlukan perbaikan segera. l. Sumber daya manusia kurang memadai dari sisi kuantitas maupun kompetensi pada fungsi Manajemen Risiko untuk Risiko Operasional. m. Sistem pengendalian intern kurang efektif dalam mendukung pelaksanaan manajemen Risiko Operasional. n. Pelaksanaan kaji ulang independen oleh satuan kerja audit internal dan fungsi yang melakukan kaji ulang independen kurang memadai. Terdapat kelemahan pada metodologi, frekuensi, dan/atau pelaporan kepada Manajemen Puncak yang membutuhkan perbaikan segera. o. Terdapat kelemahan yang signifikan berdasarkan hasil kaji ulang independen yang memerlukan perbaikan segera. p. Tindak lanjut atas kaji ulang independen kurang memadai.
Unsatisfactory (5)	5	Kualitas penerapan Manajemen Risiko untuk Risiko Operasional tidak memadai. Terdapat kelemahan signifikan pada berbagai aspek Manajemen Risiko untuk Risiko Operasional yang tindakan penyelesaiannya di luar kemampuan manajemen. Contoh karakteristik Lembaga yang termasuk dalam peringkat Unsatisfactory (5) antara lain sebagai berikut: Perumusan tingkat Risiko yang akan diambil (risk appetite) dan toleransi Risiko (risk tolerance) tidak memadai dan tidak terdapat kaitan dengan sasaran strategis dan strategi Lembaga secara keseluruhan.

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

Peringkat	Level	Definisi Peringkat
		Kesadaran (awareness) dan pemahaman Manajemen Puncak sangat lemah mengenai Manajemen Risiko untuk Risiko Operasional. Budaya Manajemen Risiko untuk Risiko Operasional tidak kuat atau belum ada sama sekali. Pelaksanaan tugas Manajemen Puncak tidak memadai. Terdapat kelemahan signifikan pada hampir seluruh aspek penilaian dan tindakan penyelesaiannya di luar kemampuan Lembaga. Kelemahan signifikan pada fungsi Manajemen Risiko untuk Risiko Operasional yang membutuhkan perbaikan fundamental. Delegasi kewenangan sangat lemah. Strategi Risiko Operasional tidak sejalan dengan tingkat Risiko yang akan diambil dan toleransi Risiko Operasional. Kelemahan sangat signifikan pada kebijakan dan prosedur Manajemen Risiko serta penetapan limit Risiko Operasional. Proses Manajemen Risiko untuk Risiko Operasional tidak memadai dalam mengidentifikasi, mengukur, memantau, dan mengendalikan Risiko Operasional. *Business continuity management* tidak andal. Kelemahan fundamental pada Sistem Informasi Manajemen Risiko Operasional. Sumber daya manusia tidak memadai dari segi kuantitas maupun kompetensi pada fungsi Manajemen Risiko untuk Risiko Operasional. Sistem pengendalian intern tidak efektif dalam mendukung pelaksanaan Manajemen Risiko untuk Risiko Operasional. Pelaksanaan kaji ulang independen oleh satuan kerja audit internal dan fungsi yang melakukan kaji ulang independen tidak memadai. Terdapat kelemahan pada metodologi, frekuensi, dan/atau pelaporan kepada Manajemen Puncak yang memerlukan perbaikan fundamental. Terdapat kelemahan yang sangat signifikan berdasarkan hasil kaji ulang independen yang memerlukan perbaikan segera. Tindak lanjut atas kaji ulang independen tidak memadai atau tidak ada.

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

13) Berikut adalah matrix risiko yang digunakan sebagai acuan dalam melakukan penilaian risiko:

Risiko Inheren	Kualitas Penerapan Manajemen Risiko				
	Strong	Satisfactory	Fair	Marginal	Unsatisfactory
Low	1	1	2	3	3
Low to Moderate	1	2	2	3	4
Moderate	2	2	3	4	4
Moderate to High	2	3	4	4	5
High	3	3	4	5	5

14) Information Security (IS) Manajer melakukan Analisa terkait dengan kontrol yang telah diimplementasi.
15) Unit yang menangani kegiatan Manajemen Aset dan Risiko melakukan Analisa dan menentukan nilai kualitas penerapan manajemen risiko.
16) Unit yang menangani kegiatan Manajemen Aset dan Risiko membuat laporan hasil identifikasi risiko (Risk Register).
17) Unit yang menangani kegiatan Manajemen Aset dan Risiko membuat laporan hasil penilaian risiko dan Profil Risiko TI.
18) Secara berkala, penilaian risiko harus dikaji ulang dan dikinikan minimum 3 bulan.
19) Laporan hasil identifikasi risiko (Risk Register), laporan hasil penilaian risiko dan Profil Risiko TI harus direview terlebih dahulu oleh Koordinator Unit yang menangani kegiatan Manajemen Aset dan Risiko, khusus untuk penilaian risiko dan Profil Risiko TI harus dilakukan review sampai kepada Information Security (IS) Manager.

b. Pengendalian Risiko

Dimana ketentuan yang perlu diperhatikan dalam melakukan pengendalian risiko adalah sebagai berikut:

1) Unit yang menangani kegiatan Manajemen Aset dan Risiko menentukan tindak lanjut pengendalian dan penanggung jawab dari masing-masing risiko yang ada.

Catatan :
- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

2) Unit yang menangani kegiatan Manajemen Aset dan Risiko membuat laporan terkait dengan pengendalian risiko (Risk Treatment) secara berkala.
3) Berikut adalah ketentuan treatment option yang digunakan sebagai acuan dalam melakukan treatment risiko:

No	Treatment Option	Definisi	Contoh
1	Accept	Risiko yang memiliki **risk level low dan low to moderate** yang mana perusahan telah melakukan penerapan kontrol berupa kebijakan, prosedur, aktivitas atau teknologi guna menghadapi risiko tersebut	Terjadinya kebakaran dimana Lembaga telah menerapkan prosedur penanganan kebakaran, smoke detector, alat pemadam kebakaran dan lokasi alternatif pada saat kebakaran yang mana apabila risiko tersebut terjadi sudah dapat ditangani secara cepat dengan kontrol yang sudah diterapkan
2	Avoid	Risiko yang memiliki **risk level moderate, moderate to High, dan High** yang mana pengendalian risiko dilakukan dengan menghindari risiko tersebut dengan cara tidak melakukan aktivitas yang menimbulkan risiko tersebut	Terdapat aplikasi A (free software) yang memiliki risiko berupa malware dimana dilakukan pengendalian risiko dengan menghindari untuk melakukan install aplikasi tersebut yang dapat mengandung risiko bagi Lembaga kedepannya
3	Transfer	Risiko yang memiliki **risk level moderate, moderate to High, dan High** yang mana pengendalian risiko dilakukan dengan mengalihkan risiko tersebut kepada pihak lain	Terdapat pengadaan laptop dimana terdapat risiko laptop tersebut akan rusak di kemudian hari maka dilakukan pengendalian dengan melakukan transfer risiko laptop tersebut dengan menerapkan garansi pada laptop tersebut oleh pihak ketiga yang mana apabila laptop tersebut rusak Bank tidak perlu

Catatan :
- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

No	Treatment Option	Definisi	Contoh
		berupa asuransi ataupun garansi	mengeluarkan biaya lagi untuk memperbaiki laptop tersebut
4	Mitigate	Risiko yang memiliki **risk level moderate, moderate to High, dan High** yang mana pengendalian risiko dilakukan dengan memitigasi risiko tersebut dengan menerapkan kontrol tambahan berupa kebijakan, prosedur, aktifitas atau teknologi untuk dapat menurunkan dampak yang terjadi dari risiko tersebut	Terdapat potensi terserangnya virus pada laptop atau server dimana virus tersebut memberikan dampak bagi laptop atau server yang ada dimana melakukan pengendalian risiko dengan melakukan mitigasi dengan menerapkan kontrol tambahan berupa implementasi antivirus dengan tujuan untuk memitigasi risiko virus yang ada

4) Laporan hasil pengendalian risiko harus direview terlebih dahulu oleh Koordinator Unit yang menangani kegiatan Manajemen Aset dan Risiko.

c. Pemantauan Risiko

Dimana ketentuan yang perlu diperhatikan dalam melakukan pemantauan risiko adalah sebagai berikut:

1) Information Security (IS) Manager melakukan pemantauan secara berkala dari pelaksanaan tindak lanjut pengendalian risiko yang telah ditentukan.
2) Unit yang menangani kegiatan Manajemen Aset dan Risiko memberikan feedback dari proses tindak lanjut pengendalian risiko.
3) Information Security (IS) Manager dan Unit yang menangani kegiatan Manajemen Aset dan Risiko harus melakukan

Catatan :
- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

verifikasi feedback terkait dengan proses tindak lanjut pengendalian risiko

4) Unit yang menangani kegiatan Manajemen Aset dan Risiko harus melakukan pengkinian terhadap laporan penilaian risiko dan tabel profil risiko
5) Information Security (IS) Manager, Koordinator Unit yang menangani kegiatan Manajemen Aset dan Risiko harus mendapatkan laporan penilaian risiko dan tabel profil risiko terupdate

d. Kertas Kerja Pengelolaan Risiko

1) Berikut adalah contoh kertas kerja yang digunakan dalam melakukan pengelolaan risiko:

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX

Risk Description										Pre-Treatment								Treatment Tahap 1				Post-Treatment Tahap 1						
No.	Asset/Process	Object Type	Source of Risk / Threat	Cause / Vulnerabilities	Impact	Impact Category			Risk Owner	Existing Controls	Risiko Inheren (1)	Risiko Inheren (2)	Kulitas Management Risiko (1)	Kulitas Management Risiko (2)	Risk Score	Flag	Risk Level	Treatment Option	Control 1	IT Process Reference (COBIT 2019)	ISMS Reference (ISO 27001:2013)	Risiko Inheren (1)	Risiko Inheren (2)	Kulitas Management Risiko (1)	Kulitas Management Risiko (2)	Risk Level	Comments	Target Date
						Confidentialty / Privasi	Integrity	Avaliability																				

2) Lampiran Daftar Risiko

Daftar risiko Dinas Komunikasi, Informatika, Persandian dan Statistik dibuat terpisah dari surat keputusan ini.

Ditetapkan di : S u m e d a n g
Pada Tanggal : 07 Juli 2023

Balai Sertifikasi Elektronik

SUMEDANG
DIGITAL SIGNATURE

Ditandatangani Secara Elektronik Oleh:

BAMBANG RIANTO, S.STP, M.Si
NIP. 197704201996021001

Kepala Dinas Komunikasi dan Informatika, Persandian dan Statistik

Catatan :

- ✓ UU ITE No 11 Tahun 2008 Pasal 5 ayat 1
  "Informasi Elektronik dan/atau Dokumen Elektronik dan/atau hasil cetaknya merupakan alat bukti hukum yang sah."
- ✓ Dokumen ini telah ditandatangani secara elektronik menggunakan **sertifikat elektronik** yang di terbitkan **BSrE.**
- ✓ Surat ini dapat dibuktikan keasliannya dengan terdaftar di http://e-office.sumedangkab.go.id, kode: ZMI5OGUX