BUPATI KATINGAN
PROVINSI KALIMANTAN TENGAH

PERATURAN BUPATI KATINGAN
NOMOR 38 TAHUN 2023

TENTANG

SISTEM MANAJEMEN KEAMANAN INFORMASI DI LINGKUNGAN PEMERINTAH DAERAH KABUPATEN KATINGAN

DENGAN RAHMAT TUHAN YANG MAHA ESA

BUPATI KATINGAN,

Menimbang :

a. bahwa dalam rangka melindungi kerahasiaan, keutuhan dan ketersediaan aset informasi di lingkungan Pemerintah Kabupaten Katingan dari berbagai ancaman keamanan informasi baik internal maupun eksternal, perlu diterapkan pengelolaan keamanan informasi;

b. bahwa berdasarkan pertimbangan sebagaimana dimaksud pada huruf a, perlu menetapkan Peraturan Bupati tentang Sistem Manajemen Keamanan Informasi di Lingkungan Pemerintah Daerah Kabupaten Katingan;

Mengingat :

1. Undang-Undang Nomor 5 Tahun 2002 tentang Pembentukan Kabupaten Katingan, Kabupaten Seruyan, Kabupaten Sukamara, Kabupaten Lamandau, Kabupaten Gunung Mas, Kabupaten Pulang Pisau, Kabupaten Murung Raya, dan Kabupaten Barito Timur di Provinsi Kalimantan Tengah (Lembaran Negara Republik Indonesia Tahum 2002 Nomor 18, Tambahan Lembaran Republik Indonesia Nomor 4180);

2. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843) sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 251, Tambahan Lembaran Negara Republik Indonesia Nomor 5952);

3. Undang-Undang Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-Undangan (Lembaran Negara Republik Indonesia Tahun 2011 Nomor 82, Tambahan Lembaran Negara Republik Indonesia Nomor 5234) sebagaimana telah beberapa kali diubah terakhir dengan Undang-Undang Nomor 13 Tahun 2022 tentang Perubahan Kedua atas Undang-Undang Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang - Undangan (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 143, Tambahan Lembaran Negara Republik Indonesia Nomor 6801);

4. Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 244, Tambahan Lembaran Negara Republik Indonesia Nomor 5587) sebagaimana telah beberapa kali diubah terakhir dengan Undang-Undang Nomor 6 Tahun 2023 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 2 Tahun 2022 tentang Cipta Kerja Menjadi Undang-Undang (Lembaran Negara Republik Indonesia Tahun 2023 Nomor 41, Tambahan Lembara Negara Republik Indonesia Nomor 6856);

5. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);

6. Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik (Berita Negara Republik Indonesia Tahun 2016 Nomor 1829);

7. Peraturan Menteri Komunikasi dan Informatika Nomor 41/PER/M.KOMINFO/11/2007 tentang Panduan Umum Tata Kelola Teknologi Informasi dan Komunikasi Nasional;

8. Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi (Berita Negara Republik Indonesia Tahun 2016 Nomor 551);

9. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 59 Tahun 2020 tentang Pemantauan dan Evaluasi Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2020 Nomor 994);

10. Peraturan Badan Siber dan Sandi Negara Nomor 8 tahun 2020 tentang Sistem Pengamanan dalam Penyelenggaraan Sistem Elektronik (Berita Negara Republik Indonesia Tahun 2020 Nomor 1375);

11. Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Sistem Informasi Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2021 Nomor 541);

12. Peraturan Bupati Katingan Nomor 50 Tahun 2022 tentang Pelaksanaan Persandian untuk Pengamanan Informasi di Pemerintah Daerah Kabupaten Katingan (Berita Daerah Kabupaten Katingan Tahun 2022 Nomor 700);

MEMUTUSKAN :

Menetapkan : PERATURAN BUPATI TENTANG SISTEM MANAJEMEN KEAMANAN INFORMASI DI LINGKUNGAN PEMERINTAH DAERAH KABUPATEN KATINGAN.

BAB I
KETENTUAN UMUM
Pasal 1

Dalam peraturan Bupati ini yang dimaksud dengan :

1. Daerah adalah Kabupaten Katingan;
2. Pemerintah Daerah adalah Bupati sebagai unsur penyelenggara Pemerintahan Daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan daerah otonom;
3. Bupati adalah Bupati Katingan;
4. Wakil Bupati adalah Wakil Bupati Katingan;
5. Sekretaris Daerah adalah Sekretaris Daerah Kabupaten Katingan;
6. Dinas Komunikasi Informatika, Statistik dan Persandian yang selanjutnya disebut Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan;
7. Perangkat Daerah Kabupaten Katingan yang selanjutnya disebut Perangkat Daerah adalah unsur pembantu Bupati dan Dewan Perwakilan Rakyat Daerah dalam penyelenggaraan unsur Pemerintahan yang menjadi kewenangan Daerah;
8. Sistem merupakan suatu kesatuan yang terdiri dari komponen atau elemen yang dihubungkan bersama yang bertujuan untuk memudahkan aliran informasi, materi atau energi demi mencapai suatu tujuan;
9. Informasi adalah keterangan, pernyataan, dan gagasan yang mengandung nilai, makna, dan pesan, baik data, fakta maupun penjelasannya yang dapat dilihat, didengar, dan dibaca yang disajikan dalam berbagai kemasan dan format sesuai dengan perkembangan teknologi informasi dan komunikasi secara elektronik ataupun nonelektronik;
10. Teknologi informasi adalah teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan/atau menyebarkan informasi;
11. Teknologi informasi dan komunikasi yang selanjutnya disingkat TIK adalah segala kegiatan yang terkait dengan pemrosesan, pengelolaan, dan pemindahan informasi antar media;

12. Komputer adalah alat untuk memproses data elektronik, mengetik, optik, atau sistem yang melaksanakan fungsi logika, aritmatika, serta penyimpanan;
13. Perangkat lunak diartikan sebagai satu atau sekumpulan program komputer, prosedur, dan/atau dokumentasi yang terkait dalam pengoperasian sistem elektronik;
14. Keamanan informasi adalah suatu kondisi dimana terjaganya aspek kerahasiaan, integritas dan ketersediaan dari data atau informasi;
15. Sistem manajemen keamanan informasi yang selanjutnya disingkat SMKI adalah sistem manajemen untuk membangun, mengimplementasikan, mengoperasikan, memonitor, meninjau, memelihara dan meningkatkan keamanan informasi berdasarkan pendekatan risiko;
16. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengidamkan, dan/atau menyebarkan informasi elektronik;
17. Penyelenggara Sistem Elektronik adalah setiap orang, perangkat daerah, badan usaha, dan masyarakat yang menyediakan, mengelola, dan/atau mengoperasikan Sistem Elektronik secara sendiri-sendiri maupun bersama-sama kepada pengguna Sistem Elektronik untuk keperluan dirinya dan/atau keperluan pihak lain;
18. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan layanan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada penggugat SPBE;
19. Aset informasi adalah unit informasi yang dapat dipahami, dibagi, dilindungi dan dimanfaatkan secara efektif;
20. Aset Pengolahan adalah suatu perangkat baik elektronik maupun non-elektronik yang dapat digunakan untuk membuat dan menyunting informasi;
21. Penyimpanan Informasi adalah suatu proses menyimpan informasi dengan menggunakan media baik elektronik maupun nonelektronik;
22. *Data Center*/Pusat Data adalah suatu fasilitas untuk menempatkan sistem komputer dan perangkat-perangkat terkait, seperti sistem komunikasi data dan penyimpanan data;
23. Risiko adalah kejadian atau kondisi yang tidak diinginkan, yang dapat menimbulkan dampak negatif terhadap pencapaian sasaran kinerja dari layanan Sistem Elektronik;
24. Badan Siber dan Sandi Negara yang selanjutnya disingkat BSSN adalah lembaga pemerintah yang menyelenggarakan tugas pemerintahan di bidang keamanan siber;
25. Sertifikat Sistem Manajemen Keamanan Informasi yang selanjutnya disebut Sertifikat SMKI adalah bukti tertulis yang diberikan oleh Lembaga Sertifikasi kepada Penyelenggara Sistem Elektronik yang telah memenuhi persyaratan;
26. Lembaga Sertifikasi Sistem Manajemen Keamanan Informasi yang selanjutnya disebut Lembaga Sertifikasi adalah lembaga audit Keamanan Informasi yang menerbitkan Sertifikat Sistem Manajemen Keamanan Informasi;

27. Penilaian Mandiri adalah mekanisme evaluasi yang dilakukan secara mandiri oleh Penyelenggara Sistem Elektronik berdasarkan kriteria tertentu;
28. Indeks Keamanan Informasi yang selanjutnya disebut Indeks KAMI adalah alat evaluasi untuk menganalisis tingkat kesiapan pengamanan informasi di organisasi;
29. Audit Internal adalah kegiatan evaluasi berupa pemeriksaan kepatuhan terhadap standar manajemen keamanan informasi yang digunakan oleh penyelenggara sistem elektronik.
30. Auditor Independen Keamanan Informasi adalah orang yang memiliki kompetensi untuk melakukan audit internal Keamanan Informasi.

Pasal 2

(1) Peraturan Bupati ini dimaksud sebagai pedoman pengelolaan Sistem Manajemen Keamanan Informasi (SMKI) secara terpadu untuk memastikan terjaganya kerahasiaan (confidentiality), keutuhan (integrity) dan ketersediaan (availability).
(2) Pengelolaan Sistem Manajemen Keamanan Informasi (SMKI) sebagaimana dimaksud pada ayat (1) meliputi infrastruktur komputer, jaringan, sistem informasi/aplikasi, dan sumber daya manusia.
(3) Tujuan ditetapkannya Peraturan Bupati ini sebagai acuan dan pedoman dalam mengelola sistem manajemen keamanan informasi secara terpadu serta untuk mengamankan aset informasi demi memastikan terjaganya aspek kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*) pada Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan.

BAB II
RUANG LINGKUP
Pasal 3

Ruang lingkup pengamanan informasi yang diatur dalam Peraturan Bupati ini meliputi :

a. Aset Informasi;
b. Aset Pengolahan Informasi;
c. Penyimpanan Informasi;
d. Kategorisasi Sistem Elektronik;

BAB III
ASET INFORMASI
Pasal 4

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

a. Fisik, meliputi informasi yang tercetak, tertulis dan tersimpan dalam bentuk fisik seperti :
   - kertas;
   - papan tulis;
   - spanduk; atau
   - di dalam buku dan dokumen.

b. Elektronik, meliputi informasi tercetak, tertulis dan tersimpan dalam bentuk elektronik seperti :
   - database dan file yang disimpan dalam komputer;
   - informasi yang ditampilkan pada website, layar komputer; dan
   - informasi yang dikirimkan melalui jaringan telekomunikasi.

BAB IV
ASET PENGOLAHAN INFORMASI
Pasal 5

Aset pengolahan informasi sebagaimana dimaksud dalam Pasal 3 huruf b berupa :
a. Peralatan mekanik yang digerakkan dengan tangan secara manual; dan
b. Peralatan elektronik yang bekerja secara elektronik penuh

BAB V
PENYIMPANAN INFORMASI
Pasal 6

Penyimpanan Informasi sebagaimana dimaksud dalam Pasal 3 huruf c menggunakan media :
a. Elektronik, meliputi antara lain :
   1. *server*;
   2. *hard disk*;
   3. *flash disk*; dan
   4. kartu memori, dan lain-lain.
b. Non-elektronik, meliputi antara lain :
   1. lemari;
   2. rak;
   3. laci; dan
   4. *filing cabinet*, dan lain-lain.

BAB VI
KATEGORISASI SISTEM ELEKTRONIK
Pasal 7

(1) Kategori Sistem Elektronik berdasarkan asas risiko terdiri atas :
   a. Sistem Elektronik Strategis;
   b. Sistem Elektronik Tinggi; dan
   c. Sistem Elektronik Rendah.
(2) Sistem Elektronik strategis sebagaimana dimaksud pada ayat (1) huruf a merupakan Sistem Elektronik yang berdampak serius terhadap kepentingan umum, pelayanan publik, kelancaran penyelenggaraan negara, atau pertahanan dan keamanan negara;
(3) Sistem Elektronik tinggi sebagaimana dimaksud pada ayat (1) huruf b merupakan Sistem Elektronik yang berdampak terbatas pada kepentingan sektor dan/atau daerah tertentu;
(4) Sistem Elektronik rendah sebagaimana dimaksud pada ayat (1) huruf c merupakan Sistem Elektronik lainnya yang tidak termasuk pada ayat (2) dan ayat (3).

BAB VII
SUMBER DAYA
Pasal 8

(1) Kepala Organisasi Perangkat Daerah menyediakan sumber daya yang dibutuhkan untuk membentuk, mengimplementasikan, memelihara, dan meningkatkan penerapan SMKI secara berkesinambungan.
(2) Uraian secara rinci SMKI sebagaimana dimaksud pada ayat (1) tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Peraturan Bupati ini.

BAB VIII
STANDAR DAN PROSEDUR PENGENDALIAN
Pasal 9

(1) Setiap Perangkat Daerah harus menyusun standar dan prosedur pengendalian kegiatan teknologi informasi yang memenuhi prasyarat keamanan informasi.
(2) Prasyarat keamanan informasi sebagaimana dimaksud pada ayat (1) digunakan untuk mengimplementasikan tindakan dalam mengelola Risiko yang meliputi aspek sebagai berikut :
    a. keamanan sumber daya manusia;
    b. pengelolaan aset;
    c. pengendalian akses;
    d. kriptografi;
    e. keamanan fisik dan lingkungan;
    f. keamanan operasional;
    g. keamanan komunikasi;
    h. keamanan dalam proses akuisisi, pengembangan dan pemeliharaan sistem informasi;
    i. hubungan kerja dengan pemasok (supplier);
    j. penanganan insiden keamanan informasi;
    k. kelangsungan usaha; dan
    l. kepatuhan.

Pasal 10

(1) Setiap Perangkat Daerah bertanggung jawab dalam memastikan kegiatan operasional Teknologi Informasi yang stabil dan aman.
(2) Penyelenggaraan pemrosesan transaksi pada operasional teknologi informasi harus memenuhi prinsip kehati-hatian.
(3) Setiap Organisasi Perangkat Daerah penyelenggara 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 (lingkup) fisik dan lingkungan di area kerja dan Data Center;
    b. mengendalikan hak akses secara memadai sesuai kewenangan yang ditetapkan;
    c. menerapkan pengendalian terhadap informasi yang diproses;

d. memastikan ketersediaan dan kecukupan kapasitas layanan jaringan komunikasi baik yang dikelola secara internal maupun oleh pihak lain penyedia jasa;
e. melakukan pemantauan kegiatan operasional Teknologi Informasi termasuk audit trail/riwayat; dan
f. melakukan pemantauan terhadap aplikasi yang digunakan oleh PD maupun pengguna.

BAB IX
MANAJEMEN RISIKO
Pasal 11

(1) Setiap Perangkat Daerah penyelenggara Teknologi Informasi wajib melakukan proses manajemen risiko dalam menerapkan SMKI.
(2) Proses manajemen risiko sebagaimana dimaksud pada ayat (1) meliputi :
a. identifikasi;
b. pengukuran;
c. pemantauan; dan
d. pengendalian atas Risiko terkait penggunaan Teknologi Informasi.
(3) Manajemen risiko sebagaimana dimaksud pada ayat (2) meliputi :
a. pengembangan sistem;
b. operasional Teknologi Informasi;
c. jaringan komunikasi;
d. penggunaan perangkat komputer;
e. pengendalian terhadap informasi; dan
f. penggunaan pihak ketiga sebagai penyedia jasa Teknologi Informasi.
(4) Penerapan manajemen risiko harus dilakukan secara terintegrasi di setiap penggunaan operasional Teknologi Informasi pada sistem yang digunakan.

BAB X
MEKANISME PENYELENGGARAAN
Pasal 12

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

BAB XI
PELAKSANAAN AUDIT KEAMANAN INFORMASI
Pasal 13

(1) Setiap Organisasi Perangkat Daerah harus menerapkan prinsip pengendalian terhadap aktivitas Teknologi Informasi melalui proses evaluasi dan monitoring secara berkala.

(2) Setiap Organisasi Perangkat Daerah wajib melakukan kegiatan pemantauan dan tindakan koreksi penyimpangan terhadap kontrol keamanan informasi yang berada di bawah tanggung jawabnya meliputi :
   a. kegiatan pemantauan secara terus menerus; dan
   b. pelaksanaan fungsi Pemeriksaan internal yang efektif dan menyeluruh.

(3) Untuk menjamin efektifitaskegiatan pemantauan dan tindakan koreksi penyimpangan terhadap kontrol keamanan informasi, maka Organisasi Perangkat Daerah harus melaksanakan audit internal keamanan informasi minimal 1 (satu) kali dalam setahun.

(4) Pelaksanaan audit internal keamanan informasi oleh organisasi perangkat daerah dapat menunjuk auditor independent untuk menjamin obyektifitas dan efektifitas pelaksanaan audit internal dan melaporkan hasilnya kepada Kepala Daerah cq. Sekretaris Daerah.

Pasal 14

(1) Organisasi Perangkat Daerah Penyelenggara Teknologi Informasi berdasarkan hasil audit, umpan balik dan evaluasi terhadap pengendalian keamanan informasi yang dilakukan, wajib meningkatkan efektivitas SMKI secara berkesinambungan melalui perbaikan terhadap akibat penyimpangan kegiatan teknologi informasi.

(2) Hasil dari tindakan perbaikan dan peningkatan sebagaimana dimaksud pada ayat (3) harus didokumentasikan dan dilaporkan kepada Kepala Perangkat Daerah cq. Sekretaris Daerah.

BAB XI
PENANGGULANGAN INSIDEN KEAMANAN INFORMASI
Pasal 15

(1) Organisasi Perangkat Daerah diwajibkan melakukan simulasi insiden keamanan informasi dengan bekerjasama dengan Dinas Komunikasi, Informatika, Statistik, dan Persandian sebagai upaya penyadaran dan kesiapan dini dalam mengantisipasi terjadinya insiden keamanan informasi dalam lingkup internal / lokal, minimal 2 tahun sekali.

(2) Dinas Komunikasi, Informatika, Statistik, dan Persandian dapat merencanakan dan melaksanakan simulasi insiden keamanan informasi dalam lingkup internal / lokal dan antar Organisasi Perangkat Daerah minimal 1 (satu) kali dalam tiga tahun.

(3) Dinas Komunikasi, Informatika, Statistik, dan Persandiandiberikan kewenangan membentuk *task force*(tim khusus) apabila terjadi insiden keamanan informasi yang mempunyai dampak luas pada Perangkat Daerah terkait untuk penanggulangan insiden keamanan informasidan dapat menunjuk auditor independen untuk melakukan investigasi yang diperlukan.

(4) Tim khusus sebagaimana yang dimaksud pada ayat (3) wajib menyediakan akses kepada auditor independen untuk melakukan Pemeriksaan seluruh aspek terkait penyelenggaraan Teknologi Informasi.

organisasi pelaksana internal keamanan informasi dan menetapkannya dalam keputusan kepala perangkat daerah serta memberikan tembusan kepada Dinas Komunikasi Informatika, Statistik dan Persandian dan Sekretaris Daerah Kabupaten Katingan.

(2) Dinas Komunikasi Informatika, Statistik dan Persandian diwajibkan menyiapkan dan melaksanakan program peningkatan kompetensi aparatur sipil yang bertugas di masing-masing organisasi perangkat daerah setiap tahun untuk mendukung keberhasilan implementasi sistem manajemen keamanan informasi.

BAB XI
KETENTUAN PENUTUP
Pasal 16

Peraturan Bupati ini mulai berlaku pada tanggal diundangkan.

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

Ditetapkan di Katingan
pada tanggal 4 Desember 2023
Pj. BUPATI KATINGAN,

SAIFUL

Diundangkan di Katingan
pada tanggal 4 Desember 2023

SEKRETARIS DAERAH KABUPATEN KATINGAN,

PRANSANG

BERITA DAERAH KABUPATEN KATINGAN TAHUN 2023 NOMOR 762

LAMPIRAN
PERATURAN BUPATI KATINGAN
NOMOR 38 TAHUN 2023
TENTANG
SISTEM MANAJEMEN KEAMANAN INFORMASI DI LINGKUNGAN PEMERINTAH DAERAH KABUPATEN KATINGAN

A. Maksud dan Tujuan

Sebagai acuan dan pedoman dalam mengelola sistem manajemen keamanan informasi secara terpadu serta untuk mengamankan aset informasi demi memastikan terjaganya aspek kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*) pada Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan.

Pelaksanaan pengendalian keamanan informasi menjadi tanggung jawab Kepala Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan dan tanggung jawab seluruh pegawai serta pihak lain yang terkait. Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan berusaha dan berkomitmen untuk menetapkan kebijakan Information Security Management System (ISMS) sebagai langkah awal untuk melakukan langkah mitigasi serangan siber dan meningkatkan efektivitas kinerja operasional organisasi dalam aspek keamanan informasi.

B. Ruang Lingkup

Meliputi keamanan layanan, keamanan sumber daya manusia, dan seluruh aset informasi dan aset atau fasilitas pemrosesan informasi yang berada di bawah pengelolaan Pemerintah Daerah Kabupaten Katingan, beserta Perangkat Daerah Pemilik Aset terkait.

C. Definisi/Istilah

1. Access control : Pembatasan akses terhadap sumber daya di lingkungan Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan.
2. Aset informasi : Segala sumber IT yang bernilai Aset Informasi adalah segala sesuatu yang memiliki nilai bagi Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan baik dalam bentuk fisik ataupun dalam bentuk elektronik.
3. Ancaman : Ancaman atau peluang terjadinya kejadian yang tidak diinginkan dan menimbulkan kerugian bagi sistem Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan.
4. Backup : Proses penyalinan data/informasi yang dapat digunakan jika data asli hilang atau rusak.

5. Cyber Attack	:	Serangan di dunia maya yang menargetkan suatu organisasi, lembaga, atau individu untuk mengganggu, melumpuhkan, menghancurkan atau mengendalikan sistem teknologi informasi dan/atau menghancurkan integritas data atau mencuri informasi yang dikendalikan.
6. Cyber Security	:	Kemampuan untuk melindungi atau mempertahankan diri dari serangan di dunia maya.
7. Log	:	Catatan suatu peristiwa atau kejadian.
8. Malware	:	Perangkat lunak berbahaya yang digunakan untuk mengganggu pengoperasian komputer, mengumpulkan informasi sensitif, atau mendapatkan akses ke sistem komputer pribadi.
9. Perjanjian Non-Disclosure	:	Perjanjian untuk tidak mengungkapkan informasi rahasia yang telah atau akan dibagikan dalam suatu kerjasama.
10. Otentikasi	:	Mekanisme sistem untuk memverifikasi hak akses yang dimiliki oleh suatu entitas.
11. Sistem Manajemen Keamanan Informasi (SMKI)	:	Sistem manajemen yang mencakup pedoman atau kebijakan, perencanaan, penanggung jawab proses dan sumber daya yang mengacu pada pendekatan risiko bisnis untuk menetapkan, menerapkan, mengoperasikan, memantau, mengevaluasi, mengelola, dan meningkatkan keamanan informasi.
12. Teknologi Informasi	:	Teknologi yang dapat membantu membuat, memodifikasi,menyimpan, mengkomunikasikan dan/atau menyebarkan informasi.
13. Uninterruptible Power Supply (UPS)	:	Perangkat keras komputer yang berfungsi untuk memberikan suplai listrik pada saat tegangan primer (PLN) tidak bekerja, atau terjadi pemadaman listrik secara tiba-tiba.
14. VPN	:	Metode menggunakan enkripsi untuk menyediakan akses aman ke perangkat dari jarak jauh melalui internet.

15. Removable Media : Seperangkat penyimpanan yang dapat dilepas dan dihubungkan untuk memudahkan pemindahan informasi antar komputer misalnya hard drive eksternal, CD/DVD, pen drive, USB memory sticks, media card readers, backup cassettes, dan lain-lain.

D. Syarat dan Ketentuan

1. Umum

a. Sistem Manajemen Keamanan Informasi atau dapat disingkat SMKI, adalah kontrol keamanan yang memberikan serangkaian perlindungan dan tindakan pencegahan bagi Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan yang bergerak di bidang sistem teknologi informasi. Kontrol keamanan dirancang untuk memfasilitasi kepatuhan terhadap hukum yang berlaku, serta arahan dari pemangku kepentingan.

b. Kontrol keamanan ini dibuat dan disahkan sebagai bentuk perlindungan dan tindakan pencegahan dasar yang diperlukan untuk melindungi informasi selama pemrosesan, saat dalam penyimpanan, dan selama transmisi.

c. Kebijakan ini akan mengatur secara umum mencakup kegiatan untuk mengidentifikasi, melindungi, mendeteksi, merespons, dan memulihkan keamanan informasi atau proses siber terkait.

d. *Manajemen dan seluruh pegawai harus memiliki kesadaran dan* komitmen yang tinggi untuk menerapkan kebijakan ini sebagai bagian dari budaya kerja.

2. Spesifik

a. Kebijakan ini harus diperbarui apabila terdapat perubahan pada hal berikut :
   1) Perubahan standar atau kerangka kerja yang menjadi dasar acuan;
   2) Perubahan arah strategis organisasi (visi, misi, atau target);
   3) Perubahan peraturan perundang-undangan, anggaran dasar, dan proses bisnis;
   4) Adanya perbedaan yang ditemukan berdasarkan hasil pemeriksaan atau audit.

b. Apabila suatu ketentuan dalam kebijakan ini bertentangan dengan ketentuan lain yang telah diberlakukan sebelum diterbitkannya dokumen ini, maka ketentuan dalam kebijakan ini berlaku atau dapat disesuaikan dengan kebutuhan.

c. Dalam rangka perbaikan berkelanjutan, fungsi penanggung jawab kebijakan ini dan fungsi terkait melakukan penyempurnaan dokumen ini secara berkala atau berkala minimal 1 (satu) kali dalam 1 (satu) tahun untuk senantiasa menyesuaikan dengan perkembangan bisnis, organisasi, teknologi, dan peraturan yang berlaku.

d. Apabila terdapat perubahan aparatur yang mengakibatkan perbedaan nama jabatan, maka tugas dan tanggung jawab jabatan dalam kebijakan ini mengikuti jabatan aparatur yang baru.
e. Sosialisasi implementasi kebijakan di Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan akan dilakukan oleh Kepala Bidang Pengelolaan Informasi Publik dan Pengelolaan Komunikasi Publik.
f. Kebijakan ini mengatur :
   1) Aset Sistem Teknologi Informasi;
   2) Manajemen Peran dan Tanggung Jawab Keamanan;
   3) Manajemen Penggunaan Pihak Ketiga;
   4) Manajemen Identitas, Otentikasi, Akses Jarak Jauh, dan Hak Istimewa;
   5) Keamanan Jaringan Komunikasi;
   6) Organisasi dan Manajemen Keamanan Sumber Daya;
   7) Perlindungan Fisik dan Pengelolaan Lingkungan Kerja;
   8) Manajemen Kriptografi;
   9) Manajemen Keamanan Sistem Akuisisi, Pengembangan, dan Pemeliharaan;
   10) Manajemen *Backup;*
   11) Manajemen Kerentanan;
   12) Manajemen Insiden Keamanan Informasi atau Keamanan Siber;
   13) Manajemen Log;
   14) Ancaman *Intelligence;*
   15) Kesiapan TIK untuk kelangsungan bisnis;
   16) Keamanan informasi untuk penggunaan layanan cloud;
   17) Manajemen konfigurasi;
   18) Pencegahan kebocoran data;
   19) Pengkodean aman;
   20) Manajemen Keberlanjutan Aspek Keamanan Informasi atau *Cyber;*
   21) Manajemen Kepatuhan; dan
   22) Evaluasi dan Perbaikan Berkelanjutan.

E. Manajemen Aset Sistem Teknologi Informasi

Klasifikasi jenis aset sistem teknologi informasi harus disusun dan diterapkan, kemudian dimutakhirkan secara berkala sesuai dengan kebutuhan, kepentingan, dan dampak bisnis. Kepemilikan atau alokasi dan tanggung jawab aset juga harus dinyatakan dengan jelas. Manajemen aset sistem informasi harus menerapkan hal-hal berikut, diantaranya :

1. Memastikan segala peraturan dan perundangan yang berlaku terkait dengan keamanan informasi dipatuhi;
2. Memastikan bahwa manajemen SMKI dilakukan peninjauan, setidaknya dalam setiap tahun dilakukan satu kali;
3. Agar implementasi SMKI berlangsung secara efektif, maka disediakan sumber daya yang diperlukan;
4. Dilakukan assessment risiko keamanan informasi secara berkala;
5. Menyediakan dokumentasi sebagai pendukung yang diperlukan untuk mengimplementasikan bab-bab ketentuan keamanan informasi yang tertulis dalam dokumen ini;

6. Perangkat Daerah harus memastikan bahwa pertukaran atau transmisi informasi rahasia dan sejenisnya diterapkan sesuai prosedur atau kebijakan persyaratan keamanan yang telah disepakati;
7. Klasifikasi jenis aset sistem teknologi informasi harus disusun serta diterapkan, kemudian dimutakhirkan secara berkala, dan disesuaikan dengan kebutuhan, kepentingan, dan dampak bisnis. Kepemilikan atau alokasi dan tanggung jawab aset juga harus dinyatakan dengan jelas;
8. Informasi merupakan salah satu jenis aset organisasi yang memerlukan perlindungan sesuai dengan tingkat kepentingan organisasi, sehingga harus diklasifikasikan dan ditangani secara tepat sesuai klasifikasinya;
9. Mengklasifikasikan informasi dilakukan dengan mempertimbangkan regulasi yang ada di Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan, nilai yang terkandung dalam informasi tersebut, serta tingkat kekritisan dan kerahasiaannya;
10. Keamanan dalam pertukaran informasi atau data bertujuan untuk melindungi aset Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan agar terhindar dari berbagai ancaman dari dalam dan luar, baik sengaja maupun tidak sengaja, memberikan jaminan mengenai kerahasiaan, keutuhan, dan ketersediaan informasi untuk mendukung kelangsungan usaha organisasi;
11. Setiap pertukaran atau transmisi yang bersifat rahasia melalui jaringan publik harus menggunakan teknik kriptografi, password, atau enkripsi;
12. Fasilitas dan layanan sistem teknologi informasi yang dimiliki dan disediakan oleh Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan, yang tidak terbatas pada layanan email, file sharing, dan fasilitas lainnya, harus digunakan untuk kepentingan pekerjaan;
13. Jika media penyimpanan informasi Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan hilang, pengguna harus melaporkannya dan diketahui oleh Bagian Pengelola Resiko.

F. Manajemen Penggunaan Pihak Ketiga

Organisasi harus memastikan bahwa pihak ketiga di lingkungan Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan memahami tanggung jawabnya masing-masing, sadar atas ancaman keamanan informasi, serta mengetahui proses terkait keamanan informasi. Kepatuhan persyaratan manajemen penggunaan pihak ketiga dapat dijabarkan sebagai berikut :

1. Pemilik Aset Informasi harus melakukan pemeriksaan data pribadi pegawai baru ataupun pihak ketiga sesuai dengan ketentuan yang berlaku;

2. Seluruh persyaratan keamanan informasi harus disertakan sebagai bagian dari perjanjian dengan pihak ketiga mana pun yang dapat mengakses, memproses, menyimpan, mengomunikasikan, atau menyediakan komponen infrastruktur sistem teknologi informasi untuk Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan;
3. Perjanjian kontrak dengan pihak ketiga juga harus memuat persyaratan keamanan informasi dan mendukung proses manajemen risiko di Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan;
4. Kegiatan pemantauan, peninjauan, dan pemeriksaan pihak ketiga harus dilakukan secara berkala untuk memastikan bahwa semua persyaratan keamanan informasi dalam perjanjian telah diterapkan;
5. Permintaan perubahan dalam penyediaan layanan oleh pihak ketiga harus dikelola dengan mempertimbangkan kekritisan informasi bisnis, sistem, dan proses yang terlibat serta meninjau risiko yang terkait dengan keamanan informasi;
6. Permohonan penjaminan keamanan informasi kepada pihak ketiga dapat dilakukan dengan membuat dokumen *Non-Disclosure Agreement (NDA)* atau sejenisnya bagi personil yang bekerja dan/atau menggunakan informasi atau data;
7. Pihak ketiga diberikan sosialisasi untuk meningkatkan kepedulian terhadap keamanan informasi (jika diperlukan).

G. Manajemen Identitas, Otentikasi, Akses Jarak Jauh, dan Hak Istimewa

1. Manajemen Identitas

Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan akan mengidentifikasi, memilih, dan menentukan jenis penggunaan akun yang terkait dengan sistem teknologi informasi untuk mendukung misi atau fungsi proses bisnis yang ada. Untuk mendukung hal tersebut, Perangkat Daerah dapat melakukan hal-hal dibawah ini :

a. Pembatasan pemberian identitas atau tanda-tanda keberadaan aktivitas pengolahan informasi;
b. Pengajuan akun atau hak akses apapun yang terkait dengan *aset atau sistem teknologi informasi harus disetujui minimal* oleh Kepala Bidang Persandian dan Statistik dan/atau Supervisor Pengguna terkait kemudian setiap pengajuan harus didokumentasikan dengan baik;
c. Bagi pegawai baru, Kepala Sub Bagian Umum dan Kepegawaian akan berkoordinasi dengan Kepala Bidang Persandian dan Statistik untuk pembuatan akun atau hak akses;
d. User ID atau nama pengguna merupakan identitas unik yang diberikan kepada pengguna sistem teknologi informasi di Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan sebagai bukti kepemilikan hak akses;

e. Setiap pengguna diberi User ID atau username yang kemudian diberi kewenangan mengakses sistem teknologi informasi di Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan harus berkomitmen dan bertanggung jawab atas segala kegiatan yang dilakukan;
f. Pengguna tidak diperkenankan membagikan User ID atau username dan password kepada orang lain dalam keadaan apapun;
g. Seluruh pengguna di Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan tidak diperkenankan mengakses sistem teknologi informasi dengan menggunakan User ID atau username dan password yang bukan kewenangannya;
h. Ketentuan mengenai pembuatan User ID atau username, password, dan frekuensi perubahannya ditentukan oleh Bidang Persandian dan Statistik;
i. Setiap perubahan yang terkait dengan identitas atau penghapusan hak akses dalam sistem harus dicatat dan didokumentasikan dengan baik.

2. Otentikasi

a. Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan dapat menggunakan kata sandi *(password)*, token, atau biometrik dalam melakukan autentikasi proses dari identitas pengguna;
b. Akses ke sistem teknologi informasi di Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan didefinisikan sebagai :
   1) Akses lokal
      Setiap pengguna melakukan pengaksesan ke sistem informasi milik Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan, akses tersebut dapat diperoleh melalui koneksi langsung tanpa menggunakan jaringan.
   2) Akses jaringan
      Setiap pengguna melakukan pengaksesan ke sistem informasi milik Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan, akses tersebut diperoleh melalui koneksi jaringan (yaitu, akses non-lokal). Akses jarak jauh adalah jenis akses jaringan yang melibatkan komunikasi melalui jaringan eksternal (misalnya, internet). Jaringan internal meliputi jaringan area lokal dan jaringan area luas. Selain itu, penggunaan Virtual Private Network (VPN) untuk koneksi jaringan antara titik akhir yang dikendalikan Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan dan titik akhir yang dikontrol eksternal dapat diperlakukan sebagai jaringan internal dari perspektif melindungi kerahasiaan dan integritas informasi yang melintasi jaringan.

c. Bentuk otentikasi multifaktor harus menerapkan penggunaan dua atau lebih faktor yang berbeda (otentikasi dua faktor/otentikasi multifaktor). Faktor didefinisikan sebagai sesuatu yang diketahui (misalnya, Kata Sandi, Nomor Identifikasi Pribadi (PIN), sesuatu yang dimiliki (misalnya, perangkat identifikasi kriptografi, token keras/lunak), atau sesuatu tentang diri pribadi (misalnya, ID Pengguna, Biometrik);
d. Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan dapat menggunakan mekanisme identifikasi dan otentikasi di tingkat sistem informasi dan aplikasi;
e. Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan memiliki kewenangan penuh untuk menentukan kekuatan mekanisme otentikasi yang diperlukan berdasarkan kategori keamanan informasi;
f. Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan dapat menetapkan dan melaksanakan tata cara administrasi pendistribusian autentikator baru, hilang, atau rusak serta pencabutan autentikator;
g. Pegawai yang ingin menggunakan authenticator harus menjaga dan melindungi dari pihak yang tidak berwenang dengan tidak mengungkapkan atau meminjamkan password kepada orang lain. Kata sandi tidak boleh ditulis di media yang mudah terlihat *oleh orang lain;*
h. Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan berhak mengubah autentikator untuk akun atau peran grup saat keanggotaan akun tersebut berubah.

3. Hak Akses Istimewa

a. Instruksi, pendokumentasian, dan otorisasi pengelolaannya harus tersedia dan lengkap pada akun administrator / istimewa;
b. Hak akses khusus diberikan secara terpisah dari akun yang digunakan untuk kegiatan umum, seperti akun system administrator, database administrator, dan network administrator;
c. Proses pemutakhiran perangkat lunak operasional, aplikasi dan *library* program hanya boleh dilakukan oleh system administrator;
d. Kata sandi (*password*) untuk akun administrator/istimewa harus diubah apabila pengguna (yang mengetahui kata sandi tersebut) menjadi pegawai dan akun tidak lagi digunakan;
e. Harus terdapat prosedur escrow (mandat) dengan bertujuan untuk memberikan pengguna lain yang dikehendaki mengakses akun administrator dalam keadaan darurat;
f. Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan memberikan hak istimewa kepada pihak internal untuk menyelesaikan tugas sesuai tugas dan fungsi;

g. Pengelolaan proses otorisasi dan catatan dari seluruh hak akses khusus yang dialokasikan/diberikan kepada pengguna. Hak akses khusus tidak boleh diberikan sebelum proses otorisasi selesai;
h. Pengembangan dan penggunaan sistem rutin diutamakan untuk menghindari kebutuhan dalam memberikan hak akses khusus secara terus menerus kepada pengguna;
i. Hak istimewa yang rendah dapat digunakan untuk mengembangkan, mengimplementasikan, dan mengoperasikan sistem teknologi informasi di Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan;
j. Akun hak istimewa, termasuk akun root, pengguna super, dan sejenisnya, disertakan, biasanya bertindak sebagai administrator sistem untuk berbagai jenis sistem yang tersedia. Membatasi akun istimewa untuk personel atau pemisahan dari peran tertentu dapat efektif mencegah pengaksesan informasi atau fungsi rahasia;
k. Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan dapat membedakan dalam menerapkan peningkatan kontrol tersebut antara hak istimewa yang diizinkan untuk akun lokal dan akun domain asalkan dapat menerapkan kontrol keamanan yang memadai;
l. Penunjukan peran administrator dan sejenisnya pada sistem operasi, aplikasi, atau database diketahui oleh Kepala Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan. Akun harus menggunakan nama pengguna unik yang dibuat untuk setiap layanan jika memungkinkan;
m. Semua akun dengan hak akses istimewa harus dilindungi oleh mekanisme keamanan yang memadai;
n. Hak akses istimewa seperti super user atau administrator dan sejenisnya harus diperhatikan bahwa tidak ada yang dapat mengakses, mengubah atau menggunakan akses tanpa izin atau tidak terdeteksi sama sekali;
o. Hak akses khusus yang dikelola oleh pegawai harus ditinjau secara berkala, dan ketika pegawai tersebut tidak lagi bekerja, akses tersebut harus dicabut.

4. Akses Jarak Jauh

a. Menjaga area aman dengan cara dikunci, sesuai pada inspeksi berkala, dan / atau dipantau dari jarak jauh yang sesuai dengan teknologi lainnya;
b. Akses jarak jauh harus dibuat sesuai dengan kebijakan teleworking / remote access dengan menggunakan enkripsi data dan otentikasi multi-faktor bagi semua koneksi jaringan Perangkat Daerah;
c. Akses jarak jauh adalah akses ke sistem informasi Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan oleh pengguna (atau proses yang bertindak atas nama pengguna) berkomunikasi melalui jaringan eksternal (misalnya, internet);

d. Metode akses jarak jauh termasuk *dial-up, broadband*, dan nirkabel milik Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan harus menggunakan *Virtual Private Network* (VPN) terenkripsi untuk meningkatkan kerahasiaan dan integritas melalui koneksi jarak jauh;
e. Penggunaan VPN, bila dilengkapi dengan kontrol keamanan yang memadai (misalnya, menggunakan teknik enkripsi untuk perlindungan kerahasiaan dan integritas), dapat memberikan jaminan yang memadai bagi Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan. Namun, tidak dapat disangkal bahwa masih ada potensi risiko;
f. Hak akses jarak jauh hanya diberikan kepada pegawai Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan untuk keperluan operasional Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan dengan persetujuan dari Bidang terkait;
g. Kegiatan bekerja secara jarak jauh tidak boleh dilakukan oleh aparatur Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan tanpa adanya penugasan secara langsung dari atasan terkait.

H. Manajemen Keamanan Jaringan Komunikasi

1. Pemasangan kabel jaringan harus terlindungi dari penyusupan yang *tidak sah atau kerusakan dapat dilakukan dengan menggunakan* conduit atau menghindari rute area publik;
2. Penerapan pemisahan antara kabel sumber daya listrik dengan kabel jaringan telekomunikasi bertujuan untuk mencegah interferensi;
3. Penyediaan perangkat jaringan komunikasi menjadi tanggung jawab Bidang Infrastruktur TIK dan Persandian. Perangkat harus memiliki perlindungan yang memadai terkait praktik terbaik atau praktik yang baik di industri;
4. Fasilitas session *time-out* harus diaktifkan untuk menutup dan mengunci layar komputer, aplikasi, dan koneksi jaringan apabila tidak ada aktivitas pengguna setelah periode tertentu;
5. Mengidentifikasi fitur keamanan layanan, tingkat layanan, dan kebutuhan pengelolaan serta mencantumkannya dalam kesepakatan penyediaan layanan jaringan termasuk layanan jaringan yang disediakan oleh pihak ketiga;
6. Koneksi dari dalam jaringan Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan ke eksternal dan sebaliknya dilindungi oleh *firewall*;
7. Pengguna tidak diperkenankan memasang peralatan jaringan komunikasi tanpa persetujuan Kepala Dinas Komunikasi Informatika, Statistik dan Persandian, seperti *switch, access point, router,* dan lain-lain di lingkup Instansi Pemerintah Kabupaten Katingan;

8. Perseroan menerapkan proses segmentasi jaringan dengan mengkonfigurasi *Virtual Local Area Network* (VLAN) dan sejenisnya;
9. Perangkat jaringan komunikasi ditempatkan dengan aman, dan hanya pihak tertentu yang dapat mengakses perangkat tersebut sesuai dengan kewenangannya;
10. Setiap perangkat jaringan komunikasi yang tidak digunakan lagi karena kerusakan, modernisasi, atau berakhirnya masa sewa harus dipastikan tidak mengandung informasi dalam bentuk apapun terkait konfigurasi jaringan sebelumnya;
11. Setiap perangkat yang terhubung dengan sistem jaringan komunikasi Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan harus dilengkapi dengan sistem keamanan, seperti memiliki keamanan *endpoint* (antivirus, anti-malware);
12. Untuk menjaga keandalan peralatan jaringan komunikasi, diperlukan pemeliharaan terjadwal oleh Bidang Infrastruktur TIK dan Persandian. Hal ini dilakukan sebagai bentuk pemeliharaan preventif.

I. Organisasi dan Manajemen Keamanan Sumber Daya Manusia

1. Organisasi

   Pengelolaan SDM dilakukan dengan melakukan koordinasi dengan semua pihak yang memanfaatkan sistem teknologi informasi. Kemudian, organisasi menetapkan proses perencanaan, prosedur, standar, proses review, dan upaya peningkatan keamanan informasi atau *cyber* di Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katinga. Upaya peningkatan keamanan tersebut dapat dilakukan dengan hal berikut ini :

   a. Memahami tanggung jawab Tim Keamanan Informasi yang diuraikan dalam standar organisasi keamanan informasi;
   b. Menjalin kerja sama dengan pihak-pihak di luar Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan yang terkait dengan keamanan informasi;
   c. Menjalin kerja sama dengan komunitas keamanan informasi di luar Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan melalui pelatihan, seminar, atau forum lain yang relevan dengan keamanan informasi;
   d. Menerapkan pengendalian keamanan informasi terhadap penggunaan perangkat komunikasi;
   e. Pengelolaan SDM dilakukan dengan melakukan koordinasi dengan semua pihak yang memanfaatkan sistem teknologi informasi. Kemudian, menetapkan proses perencanaan, prosedur, standar, proses review, dan upaya peningkatan keamanan informasi atau *cyber* di Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan;
   f. Jika ditemukan pelanggaran atau ancaman keamanan Informasi wajib dilaporkan kepada Kepala Bidang Persandian dan Statistik untuk ditindaklanjuti;

g. Pemisahan tugas dan tanggung jawab dilakukan untuk mengurangi risiko terjadinya tindak pidana atau penyalahgunaan hak istimewa. Pemisahan tanggung jawab meliputi, pembagian misi dan fungsi pendukung sistem teknologi informasi di antara individu dan/atau peran yang berbeda, menjalankan fungsi pendukung sistem teknologi informasi dengan individu yang berbeda (misalnya, membagi pembagian antara Tim Infrastruktur, *Front- End Team, Back-end Team, Quality Assurance Team, Information Security Team*);

h. Seluruh kontak dengan kelompok kepentingan khusus atau asosiasi profesi dan/atau komunitas yang terkait dengan informasi atau keamanan siber harus dikelola dengan baik untuk mendapatkan informasi terupdate terkait informasi atau *cyber security*;

i. Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan dapat bergabung dengan komunitas informasi atau keamanan siber untuk mengetahui kondisi terkini terkait praktik, teknik, dan teknologi keamanan yang direkomendasikan serta berbagi informasi terkait informasi atau ancaman keamanan siber, kerentanan, dan insiden;

j. Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan juga dapat memberikan arahan kepada pegawai untuk mengikuti portal berita yang khusus membahas *keamanan informasi untuk mengetahui informasi terkini* atau trend keamanan siber.

2. Sumber Daya Manusia

a. Seluruh pegawai bertanggung jawab untuk menjaga keamanan informasi Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan sesuai tugas dan fungsinya;

b. Seluruh pegawai mendapatkan pendidikan/pelatihan/ sosialisasi keamanan sistem informasi secara berkala sesuai tingkat tanggung jawabnya;

c. Kepatuhan pegawai terhadap kebijakan dan standar SMKI di lingkungan Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan diawasi oleh atasan masing-masing;

d. Screening atau pemeriksaan latar belakang dilakukan untuk setiap kandidat yang akan bekerja di Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan tersebut. Informasi tersebut dikumpulkan dan ditangani oleh People Operation Team atau pihak terkait;

e. Proses background check harus disesuaikan dengan hukum atau peraturan yang berlaku di Indonesia;

f. Setiap pegawai, calon pegawai, dan pihak ketiga harus menyetujui dan menandatangani syarat dan ketentuan kontrak kerja untuk memastikan bahwa tanggung jawab atas proses keamanan informasi dalam fungsi kerja yang relevan dipahami;

g. Proses penyampaian sosialisasi mengenai informasi atau *keamanan siber terkait dengan pihak ketiga dapat diberikan* secara eksplisit atau saat pekerjaan akan dimulai;

h. Peran dan tanggung jawab pegawai dan pihak ketiga terhadap keamanan informasi didefinisikan, diterapkan, dan dikomunikasikan kepada yang bersangkutan;

i. Penerapan pengendalian lain yang terkait dengan pihak ketiga dapat dilakukan dengan membuat dokumen *Non-Disclosure Agreement* (NDA) atau sejenisnya bagi individu yang bekerja dan/atau menggunakan informasi atau data di Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan;

j. Dokumen NDA berlaku selama pihak yang berkepentingan tersebut melakukan kegiatan di Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan dan beberapa kali setelah menyelesaikan kegiatan pekerjaan sesuai dengan ketentuan perjanjian;

k. Pada saat pegawai suatu instansi dimutasi, harus dipastikan bahwa semua akses sistem teknologi informasi terkait perubahan status pegawai telah disesuaikan dengan peraturan yang berlaku dan pengembalian fasilitas kantor dilakukan secara formal dan didokumentasikan dengan peraturan yang berlaku;

l. Pada saat pemutusan hubungan kerja, harus dipastikan bahwa :
   1) Pegawai yang hubungan kerjanya berakhir, atau berakhir masa kerja wajib mengisi formulir *exit clearance* atau *formulir pengembalian aset atau barang yang telah* ditetapkan Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan;
   2) Semua akses ke sistem informasi disesuaikan dan atau dicabut (*Electronic Mail, User Account,* dan layanan lainnya);
   3) Mengembalikan informasi, perangkat lunak, perangkat keras, dan semua fasilitas milik organisasi sesuai ketentuan yang berlaku; dan
   4) Penyesuaian hak akses terkait perubahan status pegawai dilakukan dengan ketentuan yang berlaku.

J. Pengelolaan Perlindungan Fisik dan Lingkungan Kerja

1. Pengamanan area

   Seluruh pegawai, pihak ketiga, dan tamu yang memasuki lingkungan area Pusat Data/Ruang Server Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan harus mematuhi aturan yang berlaku. Ketentuan rinci tentang pengamanan area lingkungan kerja Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan diuraikan dalam standar keamanan fisik dan lingkungan.

2. Pengamanan perangkat
   a. Perangkat pengolah informasi dan perangkat pendukung ditempatkan di lokasi yang aman dan diposisikan sedemikian rupa untuk mengurangi risiko aset informasi dapat diakses oleh pihak yang tidak berwenang;

b. Perangkat pendukung dipasang untuk menjamin beroperasinya perangkat pengolah informasi dan diperiksa dan diuji ulang kinerjanya secara berkala;
c. Perangkat pengolah informasi dipelihara secara berkala untuk menjamin ketersediaan, keutuhan, dan fungsinya;
d. Penggunaan perangkat yang dibawa ke luar dari lingkungan Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan disetujui oleh Pejabat yang berwenang.

3. Parameter keamanan harus ditetapkan dan digunakan untuk melindungi daerah-daerah yang berisi informasi dan fasilitas pengolahan informasi yang sensitif atau kritis.
4. Area aman harus dilindungi oleh pengendalian masuk yang tepat untuk menjamin bahwa hanya personil berwenang yang diperbolehkan untuk mengakses.
5. Penerapan perlindungan fisik dan lingkungan berlaku bagi pegawai dan pihak ketiga yang bekerja di Kantor Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan.
6. Perlindungan fisik terhadap bencana alam, serangan berbahaya atau kecelakaan harus dirancang dan diterapkan.
7. Setiap pegawai dan pihak ketiga yang ingin mengakses secara fisik fasilitas pemrosesan sistem teknologi informasi dan sejenisnya harus memperoleh izin tertulis dari penanggung jawab yang menangani.
8. Peralatan harus diletakkan dan dilindungi untuk mengurangi risiko dari ancaman lingkungan dan bahaya, dan kesempatan terhadap akses oleh yang tidak berwenang.
9. Proteksi yang memadai seperti sistem akses pintu elektronik, alarm kebakaran, *Closed Circuit Television (CCTV),* detektor asap atau api, alat pemadam kebakaran, *Uninterruptible Power Supply (UPS),* genset, dan peralatan lainnya di kantor yang dikelola oleh penyedia layanan.
10. Peralatan harus dilindungi dari gangguan listrik dan gangguan lain yang disebabkan oleh kegagalan dalam fasilitas pendukung.
11. Peralatan harus dipelihara dengan benar untuk memastikan aspek ketersediaan dan integritas.
12. Semua keamanan fisik menjadi tanggung jawab penyedia layanan *Cloud Computing.*
13. Di ruang kerja dilarang makan, minum, merokok, dan kegiatan lain yang dapat melemahkan keamanan informasi, termasuk bahaya korsleting listrik, kebakaran, dan gangguan teknis lainnya.
14. Pihak ketiga (vendor) atau tamu yang memasuki area kerja yang mengandung informasi sensitif harus mengikuti aturan, seperti :
    a. Didampingi oleh personel terkait; dan
    b. Perangkat elektronik yang berfungsi untuk mengambil gambar, video, audio seperti kamera dan perangkat mobile tidak diperbolehkan kecuali mendapat izin dari otoritas terkait.
15. Setiap pegawai wajib melindungi peralatan komputer yang tertinggal, baik dengan mengunci komputer atau ruangannya, mematikannya, dan menyimpannya di lemari yang terkunci. Setiap pegawai harus mengaktifkan batas waktu screen saver dan memberikan kata sandi *dan/atau membiarkan komputer dalam keadaan tidak aktif,* dan sistem operasi harus dikunci.

16. Setiap pegawai tidak boleh menyimpan atau meninggalkan informasi rahasia di atas meja tanpa pengawasan atau pada perangkat lain, seperti PC, notebook, media yang dapat dipindahkan, printer, dan pemindai. Hindari bertemu tamu, vendor, atau pihak ketiga lainnya di depan mejanya tanpa mengamankan informasi rahasia sehingga tidak mudah terbaca.

K. Manajemen Kriptografi

1. Mengembangkan dan menerapkan sistem kriptografi untuk perlindungan informasi dan membuat rekomendasi yang tepat bagi penerapannya.
2. Sistem kriptografi digunakan untuk melindungi aset informasi yang memiliki klasifikasi sangat rahasia, rahasia, dan terbatas.
3. Pengendalian dan Penggunaan Kriptografi untuk perlindungan informasi mempertimbangkan :
   a. Kondisi dari suatu kegiatan yang menentukan bahwa informasi harus dilindungi, seperti risiko kegiatan, media pengiriman informasi, tingkat perlindungan yang dibutuhkan;
   b. Tingkat perlindungan yang dibutuhkan diidentifikasi berdasarkan penilaian risiko, antara lain jenis, kekuatan, dan kualitas dari alogoritma enkripsi yang akan digunakan;
   c. Keperluan enkripsi untuk perlindungan informasi kategori sangat rahasia, rahasia, dan terbatas yang melalui perangkat mobile computing, removable media atau jalur komunikasi.
4. Pengelolaan teknik kriptografi dapat disesuaikan dengan kebutuhan Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan namun tetap dari segi regulasi dan keamanan informasi, terutama pada komponen kerahasiaan, integritas, non-repudiation, dan otentikasi.
5. Perangkat Daerah dapat memproduksi, mengontrol, dan mendistribusikan kunci kriptografi simetris atau asimetris menggunakan teknologi dan proses manajemen kunci.
6. Proses kriptografi diterapkan untuk memastikan keamanan saat pertukaran dilakukan pada sistem aplikasi, jaringan komunikasi, email, dan sistem teknologi informasi lainnya.
7. Jika dilihat dari sisi sistem aplikasi yang dikembangkan oleh pihak internal dan eksternal, file seperti "*connection string*", " *load- sikureto - env*", atau konfigurasi yang berfungsi sebagai penghubung aplikasi ke database engine harus dilindungi oleh teknik kriptografi, setidaknya pada informasi *username* dan *password* bukan *plaintext*.
8. Tidak disarankan untuk menggunakan metode kriptografi yang dibuat oleh pengembang sistem aplikasi pihak ketiga jika metode tersebut belum diuji keandalannya.
9. Ketika proses kriptografi belum diterapkan dengan tepat, disarankan agar setidaknya kontrol tambahan menggunakan protokol komunikasi yang aman seperti HTTPS/SSL/TLS dan sejenisnya.

10. Ketentuan untuk kunci kriptografi dapat mengadopsi hal-hal berikut :
    a. Jika memungkinkan, dapat diimplementasikan secara terpusat, dan ketika terpusat, harus menerapkan proses otentikasi, otorisasi, dan audit yang andal untuk menghindari akses ilegal atau modifikasi kunci;
    b. Jika terjadi pelanggaran keamanan terkait seperti hilangnya kunci kriptografi atau terjadinya pencurian metode kunci kriptografi, maka harus segera diganti;
    c. Pembuatan, penyimpanan, dan pemusnahan kunci kriptografi harus didokumentasikan dan dilakukan oleh personel yang berwenang di Tim Teknologi;
    d. Ketika pihak ketiga melakukan pengembangan sistem aplikasi, kunci kriptografi harus diserahkan kepada Tim Teknologi; dan
    e. Itu harus dievaluasi untuk jangka waktu tertentu, setidaknya setahun sekali, untuk meminimalkan risiko kebocoran kunci kriptografi.

L. Akuisisi, Pengembangan, dan Pemeliharaan Sistem Manajemen Keamanan

1. Pengendalian keamanan Informasi dalam akuisisi, pengembangan, dan pemeliharaan sistem informasi terdiri dari :
    a. Persyaratan keamanan pada Sistem Informasi;
    b. Keamanan dalam proses pengembangan dan pendukung;
    c. Data pengujian.
2. Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan menetapkan dan mendokumentasikan persyaratan keamanan informasi yang relevan sebelum pengembangan Sistem Informasi.
3. Persyaratan keamanan informasi yang harus disusun juga termasuk vulnerability point atas Sistem Informasi yang akan dikembangkan.
4. Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan harus mengidentifikasi risiko dari setiap vulnerability point dan menentukan mitigasi yang harus diterapkan dalam pengembangan Sistem Informasi.
5. Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan harus melakukan pemeliharaan yang tepat terhadap Fasilitas Pengolah Informasi untuk menjamin keutuhan dan ketersediaan Fasilitas Pengolah Informasi.
6. Pengadaan sistem teknologi informasi baru atau yang sudah ada, Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan membentuk tim yang bertugas menentukan spesifikasi teknis sesuai kebutuhan pengguna dan memenuhi persyaratan keamanan informasi yang relevan.
7. Persyaratan keamanan informasi atau cyber merupakan bagian integral dari persyaratan lainnya. Semua perangkat lunak berupa sistem aplikasi yang dikembangkan dapat menerapkan metode pengembangan seperti Secure System Development Life Cycle, Scrum, DevSecOps , dan lain-lain.

8. Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan memisahkan lingkungan antara sistem produksi dan sistem pengembangan dan pengujian, minimal, dengan memastikan bahwa individu yang bertanggung jawab untuk pengembangan dan pengujian tidak diperbolehkan memiliki akses ke sistem lingkungan produksi tanpa persetujuan.
9. Hak akses dari application tier ke database tier menggunakan otorisasi tidak melebihi persyaratan sesuai dengan tugas dan tanggung jawabnya (lebih rendah dari pemilik DB, root, system administrator, dan sejenisnya).
10. Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan tidak merekomendasikan pengaturan (membuat, mengubah, dan menghapus) User ID dan password untuk akses ke aplikasi hard-coded.
11. Bentuk otentikasi untuk mengakses aplikasi setidaknya harus memenuhi aspek keamanan seperti penerapan fitur captcha pada saat login, lupa User ID/password dan/atau update password, dan penerapan pengendalian lainnya.
12. Aplikasi harus menangani baik dari segi batasan ukuran file hingga ekstensi yang akan diunggah melalui fitur menu di aplikasi.
13. Aplikasi harus mencegah upaya serangan injeksi yang dilakukan oleh pihak tertentu dengan mengatur baik itu source code aplikasi, web service engine, atau dengan bantuan teknologi seperti Web *Application Firewall* (WAF) atau sejenisnya.
14. Sistem operasi dan aplikasi server hanya dapat diimplementasikan setelah serangkaian pengujian, dan pengoperasiannya di lingkungan produksi harus disetujui.
15. Instalasi atau pemutakhiran semua perangkat lunak operasional, sistem aplikasi, dan program perpustakaan hanya dapat dilakukan oleh personel yang ditunjuk.
16. Konfigurasi sistem operasi tidak dapat diubah tanpa melalui proses manajemen perubahan yang ditentukan.
17. Data pengujian harus disimpan di lokasi yang aman dan tidak boleh diakses oleh pengguna kecuali pihak yang berwenang. Jika Pengembang atau Insinyur memerlukan akses ke sistem produksi untuk menguji atau mengembangkan sistem baru, hanya akses "baca" dan "salin" yang diberikan. Akses ini hanya diizinkan selama pengujian dan aktivitas pengembangan terkait dan harus dicabut segera setelah aktivitas berhasil diselesaikan.
18. Pengembangan aplikasi yang dilakukan oleh Pihak Ketiga mengikuti persyaratan keamanan informasi dan harus didefinisikan secara jelas dalam setiap kontrak yang dilaksanakan oleh pihak ketiga. Perjanjian tersebut harus menetapkan, antara lain, tetapi tidak terbatas pada :
    a. Syarat dan ketentuan untuk memastikan bahwa semua pihak yang terlibat bertanggung jawab atas keamanan informasi;
    b. Bagaimana menjaga kerahasiaan, integritas, dan ketersediaan aset dan informasi terkait dipelihara dan diuji;
    c. Bagaimana mematuhi hukum dan peraturan yang berlaku;

d. Pengendalian fisik dan logis yang harus dilaksanakan untuk memastikan bahwa akses informasi Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan hanya dapat dilakukan oleh pihak yang berwenang
e. Bagaimana mempertahankan layanan jika terjadi bencana;
f. Hak untuk mengaudit pihak ketiga;
g. Jika sistem aplikasi berbasis website, setidaknya harus mengadopsi Open Web Application Security Project (OWASP) atau Common Weakness Enumeration (CWE) dan sejenisnya, dan model ini juga dapat diterapkan ketika pengembangan dilakukan secara internal.

19. Sebelum aplikasi memasuki lingkungan produksi, harus diuji oleh Quality Assurance dengan melampirkan informasi seperti masalah yang diketahui, perencanaan pengujian, dan hasil pengujian akhir. Proses pengujian terkait keamanan informasi dapat dilakukan pada proses ini atau setelahnya dengan mengukur kompleksitas dan kebutuhan bisnis Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan.
20. Dalam proses rilis, perlu untuk mengisi daftar periksa yang memberikan informasi tentang versi rilis, fitur yang ditambahkan atau diperbarui, tim yang terlibat, langkah-langkah untuk penyebaran, dan informasi penting lainnya.
21. Semua proses perekaman ini dapat menggunakan alat aplikasi untuk *mendukung metode pengembangan seperti* Siklus Hidup Pengembangan Sistem Aman, Scrum, DevSecOps , dan lainnya.

M. Manajemen Pencadangan

1. Sistem pencadangan dapat dilakukan secara otomatis, dan perlu untuk memeriksa secara teratur mengenai prosesnya.
2. Proses backup dilakukan secara berkala sesuai dengan kekritisan informasi terkini dan untuk masa retensi sesuai kebutuhan internal Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan.
3. Media cadangan seperti hard drive dan media yang dapat dipindahkan lainnya harus disimpan di lokasi di luar lokasi yang dapat melindunginya dari kerusakan akibat faktor lingkungan atau risiko kehilangan.
4. Tim Teknologi bertanggung jawab untuk memastikan bahwa hasil pencadangan tersedia saat dibutuhkan.
5. Semua informasi sensitif atau kritis di Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan, terutama yang disimpan di cloud, harus memiliki cadangan.
6. Pengujian hasil backup akan dilakukan secara berkala, baik secara sampling maupun secara keseluruhan, untuk memastikan validitas dan ketersediaan hasil backup sehingga proses restore dapat dilakukan dengan benar.
7. Pencadangan informasi Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan yang sensitif dan kritis yang masih *tersimpan di laptop atau komputer personel dan tidak terhubung ke* jaringan menjadi tanggung jawab masing-masing pengguna.

N. Manajemen Kerentanan

1. Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan secara berkala melakukan penilaian terhadap kerentanan terkait sistem informasi yang digunakan.
2. Paparan terhadap kerentanan harus dievaluasi dan memberikan bentuk tindak lanjut yang tepat untuk mengurangi risiko ini.
3. Jika memungkinkan, Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan dapat memeriksa ancaman teknis di dunia dengan mengakses MITER ATT&CK. MITER ATT&CK adalah basis pengetahuan taktik dan teknik musuh yang dapat diakses secara global berdasarkan pengamatan dunia nyata. Basis pengetahuan ATT&CK digunakan untuk mengembangkan model dan metodologi ancaman di berbagai sektor industri.
4. Alat keamanan titik akhir seperti antivirus atau anti-malware harus diinstal, diperbarui, dan tanda tangan diperbarui secara berkala untuk mencegah dan mendeteksi virus di lingkungan Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan.
5. Setiap perangkat yang terdeteksi atau terinfeksi virus harus segera diisolasi atau terputus dari jaringan komunikasi, atau perangkat keamanan titik akhir harus melakukan proses seperti sandbox atau sejenisnya.
6. Pengguna harus melaporkan saat mendeteksi virus atau malware, *mengalami, atau melihat perubahan konfigurasi mendadak*, atau aplikasi atau perilaku komputer yang tidak normal .
7. Untuk dapat membangun proses manajemen penilaian kerentanan yang efektif, hal-hal seperti :
   a. Menentukan dan menetapkan peran dan tanggung jawab yang terkait dengan manajemen kerentanan teknis, penilaian risiko kerentanan, dan hal- hal lain yang diperlukan;
   b. Sumber informasi yang digunakan dalam mengidentifikasi kerentanan baik dari segi perangkat lunak maupun teknologi lainnya;
   c. Tetapkan garis waktu untuk mengambil tindakan untuk memberi tahu semua bentuk kerentanan atau potensi yang relevan;
   d. Melakukan aktivitas minimal seperti pemindaian kerentanan (menggunakan pemindai kerentanan) dalam hal aplikasi dan infrastruktur (server, perangkat komunikasi jaringan, perangkat keamanan seperti firewall, dan lain-lain). Ketika sebuah Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan melakukan pengujian penetrasi, itu harus dikombinasikan dengan metode Black Box, grey box, atau White box dengan skor akhir untuk setiap temuan. Bentuk penilaian dapat menggunakan "The Common Vulnerability Scoring System" atau yang lebih dikenal dengan CVSS minimal versi 3.0;
   e. Ketika ada kerentanan, dan sifatnya membutuhkan tindakan cepat, mereka tetap harus melalui mekanisme manajemen perubahan;
   f. *Patch untuk sistem yang digunakan harus dari sumber* terpercaya. Misalnya ada kerentanan MS17-010 (SMB Server

Remote Code Execution Vulnerability) atau CVE-2021-26855 (Microsoft Exchange Server Remote Code Execution Vulnerability), maka patch harus diunduh dari Microsoft, bukan dari sumber lain;

g. Instalasi atau patching harus dinilai (risiko yang akan ditimbulkan oleh kerentanan dibandingkan dengan risiko menginstal patch). Tambalan harus diuji dan dievaluasi sebelum pemasangan untuk memastikan bahwa tambalan digunakan secara efektif dan tidak ada dampak signifikan; dan
h. Ketika tidak ada patch dan ditemukan kerentanan 0-day (zero-day), maka harus ada kontrol lain yang perlu dipertimbangkan, seperti :
   1) Mematikan atau menonaktifkan layanan yang memiliki kerentanan jika sistem tidak digunakan atau tidak mempengaruhi bisnis atau operasional Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan;
   2) Menyesuaikan atau menambahkan kontrol akses seperti penggunaan firewall atau WAF dan lainnya;
   3) Meningkatkan pemantauan untuk mendeteksi serangan yang sebenarnya; dan
   4) Meningkatkan rasa kepedulian atau kepedulian seluruh SDM terhadap kerentanan tersebut.

O. Manajemen Informasi atau Insiden Keamanan *Cyber*

1. Manajemen insiden dilakukan untuk memulihkan ketersediaan layanan sistem teknologi informasi sesegera mungkin dengan menerapkan solusi sementara atau permanen untuk mengurangi hilangnya produktivitas pengguna akibat insiden tersebut.
2. Proses penanganan insiden keamanan informasi masih mengacu pada standar pengelolaan insiden di Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan.
3. Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan harus menerapkan program ancaman orang dalam yang mencakup tim penanganan insiden atau Tim Respons Insiden Keamanan Komputer (CSIRT).
4. Program dari ancaman orang dalam mencakup keamanan informasi atau kontrol siber untuk mendeteksi dan mencegah aktivitas tersebut melalui integrasi terpusat dan analisis informasi teknis dan non-teknis untuk mengidentifikasi potensi masalah.
5. Program tersebut harus dilaksanakan dan dipantau secara berkala.
6. Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan memberikan pelatihan penanganan insiden atau respons insiden terkait peran dan tanggung jawab personel yang ditugaskan. Misalnya, pengguna biasa mungkin hanya perlu mengetahui siapa yang harus dihubungi atau mengidentifikasi insiden dalam sistem teknologi informasi. Sementara itu, administrator sistem mungkin memerlukan pelatihan tambahan tentang cara menangani atau memperbaiki insiden. Kemudian penanggap insiden dapat menerima pelatihan yang lebih spesifik tentang forensik, pelaporan, pemulihan, dan pengembalian sistem ke kondisi normal. Pelatihan penanggap

insiden mencakup pelatihan pengguna dalam mengidentifikasi dan melaporkan aktivitas mencurigakan dari sumber eksternal dan internal.

7. Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan menguji kapabilitas respons insiden untuk menentukan efektivitas kapabilitas secara keseluruhan dan mengidentifikasi potensi kelemahan atau kekurangan.
8. Pengujian respons insiden mencakup, misalnya, penggunaan daftar periksa, latihan berjalan atau latihan meja, simulasi paralel dan/atau latihan komprehensif.
9. Perseroan menyadari bahwa kemampuan respon insiden tergantung pada kemampuan sistem teknologi informasi dan misi atau proses bisnis yang didukung oleh sistem tersebut.
10. Informasi terkait insiden dapat diperoleh dari berbagai sumber, seperti pemantauan audit, pemantauan jaringan, pemantauan akses fisik, laporan pengguna/administrator, dan peristiwa rantai pasokan yang dilaporkan.
11. Kemampuan penanganan insiden yang efektif mencakup koordinasi di antara banyak entitas, termasuk, misalnya, pemilik layanan bisnis, pemilik sistem teknologi informasi, otoritas pengatur, dan departemen lain.
12. Penanganan dan penyelesaian insiden harus dilakukan berdasarkan prioritas insiden yang ditentukan berdasarkan kombinasi dampak insiden dan urgensi insiden. Namun, harus dibedakan antara insiden keamanan informasi dan insiden operasional (non-keamanan informasi).
13. Dalam menyelesaikan tiket insiden terkait bug yang diverifikasi, dibagi menjadi beberapa prioritas sebagai berikut :
    a. Prioritas 0 adalah hal utama yang harus segera diperbaiki karena dapat memblokir aktivitas lain, dan pembaruan status informasi tiket dilakukan setiap 30 menit. Kemudian untuk Service Level Agreement (SLA), resolusi bug adalah 4 jam;
    b. Prioritas 1 adalah memperbaiki bug dan mengarah ke pengalaman pengguna yang buruk dan pembaruan status informasi tiket setiap 2 jam. Kemudian untuk Service Level Agreement (SLA), resolusi bug adalah 1 hari (24 jam);
    c. Prioritas 2 adalah bahwa bug harus diperbaiki tetapi perlu dilihat dari sudut pandang waktu dan sumber daya yang diharapkan. Update status informasi tiket dilakukan setiap 1 hari (24 jam). Kemudian untuk Service Level Agreement (SLA), resolusi bug adalah 1 minggu (7 hari);
    d. Prioritas 3 adalah bug dapat diperbaiki pada aktivitas pengembangan atau sprint berikutnya, dan pembaruan status informasi tiket dilakukan setiap 1 minggu (7 hari). Kemudian untuk Service Level Agreement (SLA), resolusi bug adalah 3 minggu; dan
    e. Prioritas 4 selangkah lagi dari lubang hitam. Perbaikan jika memungkinkan ditempatkan di product backlog, dan update status informasi tiket dilakukan setiap 1 bulan sekali. Kemudian untuk

waktu Service Level Agreement (SLA), resolusi bug bersifat fleksibel.

14. Tingkat prioritas dan resolusi bug akan ditambahkan dalam insiden atau tiket bug yang dihasilkan oleh Tim Teknologi.
15. Mendokumentasikan insiden keamanan informasi, misalnya, memelihara catatan setiap insiden, status insiden, dan informasi relevan lainnya yang diperlukan untuk forensik, mengevaluasi detail insiden, tren, dan penanganan.
16. Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan diperbolehkan untuk mengembangkan rencana untuk menangani keamanan informasi atau insiden siber seperti :
    a. Menyediakan peta jalan untuk menerapkan kemampuan respons insiden;
    b. Menjelaskan struktur organisasi kemampuan respon insiden;
    c. Memberikan pendekatan tingkat tinggi tentang bagaimana kapabilitas respons insiden cocok secara keseluruhan;
    d. Memenuhi persyaratan unik yang terkait dengan misi, ukuran, struktur, dan fungsi;
    e. Mendefinisikan insiden yang dapat dilaporkan;
    f. Menyediakan metrik untuk mengukur kemampuan penanganan insiden;
    g. Menentukan sumber daya dan dukungan manajemen yang diperlukan untuk memelihara dan mengembangkan kemampuan *respons insiden secara efektif; dan*
    h. Ditinjau dan disetujui oleh manajemen mengenai hal ini.

P. Manajemen Log

1. Log audit pemantauan aktivitas untuk sistem aplikasi kritis dan infrastruktur server harus diaktifkan dan hasilnya dipertahankan selama periode tertentu sebagai bukti atau catatan penggunaan.
2. Aktivitas pengguna super, administrator sistem, dan operator juga harus dicatat.
3. Administrator sistem atau hak akses istimewa dilarang menghapus atau menonaktifkan log aktivitas mereka tanpa persetujuan pemimpin tertinggi di Tim Teknologi.
4. Informasi log aktivitas harus diakses dan disimpan secara aman dengan memberikan kata sandi atau enkripsi.
5. Pemantauan penggunaan sistem pemrosesan informasi harus dilakukan secara berkala untuk memastikan tidak terjadi aktivitas yang tidak sah. Kegiatan ini harus memastikan pemeriksaan untuk kegagalan akses, alokasi dan penggunaan kemampuan akses istimewa, pelacakan transaksi tertentu, dan penggunaan sumber daya sensitif.
6. Kemudian, sinkronisasi waktu semua perangkat dilakukan secara berkala dengan mengacu pada referensi waktu tertentu yang telah ditetapkan oleh Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan.

7. Infrastruktur manajemen log harus terdiri dari tiga level berikut :
   a. Pembuatan log adalah tingkat pertama yang berisi host yang menghasilkan data log. Beberapa host menjalankan log aplikasi atau layanan yang membuat data tersebut tersedia melalui jaringan ke server log tingkat kedua;
   b. Analisis dan penyimpanan log, tingkat kedua terdiri dari satu atau lebih server log yang menerima data log atau salinan dari host di tingkat pertama. Data ditransfer ke server baik secara real-time atau mendekati real-time atau dalam batch sesekali berdasarkan jadwal atau jumlah log yang menunggu untuk ditransfer; dan
   c. Pemantauan log, tingkat ketiga berisi konsol yang dapat secara otomatis memantau dan meninjau log dan hasil analisis. Konsol pemantauan log juga dapat digunakan untuk membuat laporan. Dalam beberapa infrastruktur manajemen log, konsol juga dapat menyediakan Manajemen untuk log server dan klien.
8. Manajemen log harus didasarkan pada sumber terpercaya. Isinya konsisten, konsisten dalam stempel waktu, dan konsisten dalam format.
9. Log audit harus mencatat rincian termasuk namun tidak terbatas pada ID pengguna, tanggal, dan waktu log-on dan log-off, aktivitas yang dilakukan, dan informasi lainnya.

Q. Ancaman Intelligence

1. *Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten* Katingan dapat melakukan penilaian security intelligence secara holistic dan komprehensif.
2. Setiap adanya temuan ancaman keamanan informasi maka harus langsung didokumentasikan.
3. Setelah semua ancaman dan kerentanan didaftar dan diprioritaskan, organisasi dapat melanjutkan dengan mengelola teknologi dan alat keamanan.
4. Organisasi dapat menerapkan security intelijen yang terfokus pada wawasan berbasis bukti, termasuk mekanisme, indikator, implikasi, dan rekomendasi yang dapat ditindaklanjuti tentang ancaman atau bahaya yang ada atau dapat muncul terhadap aset organisasi.
5. Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan dapat memperluas dan meningkatkan kemampuan manajemen ancaman yang tersedia.

R. Kesiapan TIK Untuk Keberlangsungan Bisnis

1. Kesiapan TIK harus direncanakan, dilaksanakan, dipelihara dan diuji berdasarkan tujuan kelangsungan bisnis dan persyaratan kelangsungan TIK.
2. Instansi harus mengidentifikasi dan memilih strategi kesinambungan TIK yangmempertimbangkan opsi sebelum, selama, dan setelah gangguan.
3. Berdasarkan strategi, rencana harus dikembangkan, diimplementasikan dan diuji untuk memenuhi tingkat ketersediaan *layanan TIK yang diperlukan dan dalam kerangka waktu yang* diperlukan setelah gangguan, atau kegagalan, proses kritis.

4. Instansi harus memastikan bahwa terdapat struktur organisasi yang memadai untuk mempersiapkan, mengurangi, dan menangani gangguan yang didukung oleh personel dengan tanggung jawab, wewenang, dan kompetensi yang diperlukan.
5. Rencana kesinambungan TIK, termasuk prosedur respons dan pemulihan yang merinci proses evaluasi secara berkala melalui latihan dan tes dan mendapat persetujuan dari pimpinan Instansi.

S. Keamanan Informasi Untuk Penggunaan Layanan Cloud

1. Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan harus menetapkan dan mengomunikasikan kebijakan topik khusus tentang penggunaan layanan cloud kepada semua pihak berkepentingan yang relevan.
2. Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan harus mendefinisikan dan mengomunikasikan pengelolaan risiko keamanan informasi yang terkait dengan penggunaan layanan cloud.
3. Penggunaan layanan cloud dapat melibatkan tanggung jawab bersama untuk keamanan informasi dan upaya kolaboratif antara penyedia layanan cloud dan organisasi yang bertindak sebagai pelanggan layanan cloud. Adalah penting bahwa tanggung jawab untuk penyedia layanan cloud dan instansi, yang bertindak sebagai pelanggan layanan cloud, didefinisikan dan diterapkan dengan tepat.
4. *Dinas Komunikasi, Informatika, Statistik, dan Persandian Kabupaten* Katingan harus mendefinisikan semua persyaratan keamanan informasi terkait yang terkait dengan :
   a. Penggunaan layanan cloud, kriteria pemilihan layanan cloud dan cakupan penggunaan layanan cloud;
   b. Peran dan tanggung jawab yang terkait dengan penggunaan dan pengelolaan layanan cloud;
   c. Kontrol keamanan informasi mana yang dikelola oleh penyedia layanan cloud dan mana yang dikelola oleh instansi sebagai pelanggan layanan cloud;

T. Manajemen Konfigurasi

1. Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan harus mendefinisikan dan menerapkan proses dan alat untuk menegakkan konfigurasi yang ditentukan (termasuk konfigurasi keamanan) untuk perangkat keras, perangkat lunak, layanan (misalnya layanan cloud) dan jaringan, untuk sistem yang baru diinstal serta untuk sistem operasional selama masa pakainya.
2. Peran, tanggung jawab dan prosedur harus ada untuk memastikan kontrol yang memuaskan dari semua perubahan konfigurasi.
3. Perubahan konfigurasi harus mengikuti proses manajemen perubahan. Catatan konfigurasi dapat berisi pemilik terkini atau informasi kontak untuk aset tersebut, tanggal perubahan konfigurasi terakhir, dan kaitannya dengan konfigurasi aset lainnya.

4. Konfigurasi harus dipantau dengan seperangkat alat manajemen sistem yang komprehensif (misalnya utilitas pemeliharaan, dukungan jarak jauh, alat manajemen organisasi, perangkat lunak pencadangan dan pemulihan) dan harus ditinjau secara teratur untuk memverifikasi pengaturan konfigurasi, mengevaluasi kekuatan kata sandi, dan menilai aktivitas yang dilakukan.

U. Pencegahan Kebocoran Data

1. Mengidentifikasi dan mengklasifikasikan informasi untuk melindungi dari kebocoran (misalnya informasi pribadi, model harga dan desain produk).
2. Memantau saluran kebocoran data (misalnya email, transfer file, perangkat seluler, dan perangkat penyimpanan portabel).
3. Mengidentifikasi dan memantau informasi sensitif dengan risiko pengungkapan yang tidak sah (misalnya, dalam data tidak terstruktur pada sistem pengguna).
4. Mendeteksi pengungkapan informasi sensitif (misalnya ketika informasi diunggah ke layanan cloud pihak ketiga yang tidak tepercaya atau dikirim melalui email).
5. Jika ekspor data diperlukan, pemilik data harus diizinkan untuk menyetujui ekspor dan meminta pertanggungjawaban pengguna atas tindakan yang dilakukan.

V. Pengkodean Aman

1. Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan dapat mengelola akses ke kode sumber program dan *libraries* sumber program sesuai dengan prosedur yang ditetapkan;
2. Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan dapat memberikan akses baca dan tulis ke kode sumber berdasarkan kebutuhan bisnis dan dikelola untuk mengatasi risiko perubahan atau penyalahgunaan dan sesuai dengan prosedur yang ditetapkan;
3. Pemutakhiran source code dan item terkait dan pemberian akses ke kode sumber sesuai dengan prosedur pengendalian perubahan dan hanya melaksanakannya setelah otorisasi yang sesuai telah diterima;
4. Tidak memberikan pengembang akses langsung ke repositori kode sumber, tetapi melalui alat pengembang yang mengontrol aktivitas dan otorisasi pada kode sumber;
5. Menyimpan daftar program di lingkungan yang aman, di mana akses baca dan tulis harus dikelola dan ditetapkan dengan tepat;
6. Memelihara log audit dari semua akses dan semua perubahan kode sumber.

W. Manajemen Keberlanjutan Keamanan Informasi atau *Cyber*

1. Tim Teknologi diperbolehkan untuk mengembangkan kerangka kerja terkait dengan keberlanjutan sistem teknologi informasi untuk memastikan kelangsungan operasional. Kerangka kerja dapat diatur dalam dokumen terpisah dari kebijakan ini.

2. Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan mengidentifikasi kebutuhan bisnis untuk ketersediaan sistem informasi dan menentukan sistem aplikasi utama yang harus dipelihara dari sisi ketersediaan.
3. Proses kontinuitas dan kontrol yang terkait dengan keamanan informasi dapat ditinjau setelah menyelesaikan IT Disaster Recovery Plan (DRP) atau proses pengujian serupa.
4. Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan melakukan verifikasi Manajemen kelangsungan layanan dalam aspek keamanan informasi dengan cara :
   a. Menerapkan dan menguji fungsionalitas proses, prosedur, dan kontrol keamanan informasi untuk memastikan bahwa semuanya konsisten dengan tujuan kelangsungan keamanan informasi;
   b. Menguji pengetahuan pegawai Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan yang terlibat untuk mengoperasikan proses, prosedur, dan kontrol keamanan informasi untuk memastikan bahwa kinerja dilakukan secara konsisten dengan tujuan kelangsungan keamanan informasi; dan
   c. Meninjau keabsahan dan efektivitas langkah-langkah kelangsungan keamanan informasi, proses keamanan informasi, prosedur dan kontrol, dan solusi ketika gangguan atau bencana terjadi.
5. Untuk mendukung proses kontinuitas layanan, Dinas Komunikasi *Informatika, Statistik dan Persandian Kabupaten Katingan berhak* untuk membuat sistem cadangan menggunakan penyedia layanan cloud yang berbeda, atau setidaknya menerapkan sistem cadangan di wilayah yang berbeda jika memungkinkan.

X. Manajemen Kepatuhan

1. Semua pengguna sistem teknologi informasi Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan, termasuk pihak ketiga lainnya, harus mematuhi kebijakan ini, mematuhi undang-undang dan peraturan terkait serta perjanjian lisensi, termasuk persyaratan kontrak.
2. Hukum, kontrak, kebijakan dan peraturan (hukum) yang terkait dengan informasi, penyampaian layanan informasi (termasuk layanan yang disediakan oleh pihak lain), proses, dan infrastruktur harus diidentifikasi. Identifikasi ini mencakup aliran data, privasi, kontrol internal, pelaporan keuangan, peraturan khusus industri, penyalinan, hak kekayaan intelektual, dan keamanan.
3. Pengawasan dan pengendalian informasi atau keamanan siber harus diuji pada waktu-waktu tertentu untuk memastikan bahwa tingkat keamanan yang disepakati dan disepakati terpenuhi.
4. Hasil pengujian atau evaluasi dapat disesuaikan berdasarkan kebutuhan bisnis baru atau perubahan peraturan perundang-undangan yang berlaku.

5. Hal-hal yang berkaitan dengan Hak Kekayaan Intelektual (HAKI), peraturan dan undang-undang, dan informasi serupa lainnya, termasuk menjaga kerahasiaan Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan, harus disebarluaskan kepada semua Pengguna.
6. Kebijakan data di Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan untuk melindungi informasi pribadi dan privasi harus diterapkan dan dikembangkan bersama antara pihak internal dan eksternal dan dikomunikasikan kepada semua pihak yang terlibat dalam pemrosesan informasi. Selain itu juga harus dilihat dari peraturan perundang-undangan yang relevan di negara ini mengenai perlindungan data privasi.
7. Audit sistem harus dilakukan secara berkala pada aspek kepatuhan, terutama audit perizinan dan penggunaan.
8. Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan menjamin bahwa perangkat lunak yang diinstal pada sistem komputer Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan telah sesuai dengan ketentuan lisensi secara sah dan memadai, dan pegawai dilarang memasang perangkat lunak yang tidak sah (ilegal).
9. Pihak ketiga yang mengakses fasilitas informasi Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan harus memiliki kompetensi yang memadai, memahami, dan mematuhi kebijakan ini.
10. Pemeriksaan teknis sistem layanan aplikasi, infrastruktur peralatan jaringan komunikasi, server, dan hal-hal lain dilakukan untuk menilai penerapan informasi atau keamanan siber Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan. Kegiatan ini dilakukan secara berkala. Rencana inspeksi teknis harus dikomunikasikan dan disetujui oleh Tim Teknologi. Akses ke alat inspeksi atau pengujian keamanan tidak boleh diberikan kecuali kepada personel yang kompeten dan berwenang untuk mencegah risiko gangguan sistem atau kemungkinan penyalahgunaan.
11. Tinjauan kepatuhan juga dapat mencakup kegiatan seperti pengujian penetrasi dan penilaian kerentanan yang dapat dilakukan oleh pihak internal atau independen dengan kontrak khusus dengan tujuan utama, yaitu deteksi dini kerentanan dalam sistem Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan dan memeriksa seberapa memadai kontrol dalam mencegah akses tidak sah yang disebabkan oleh kerentanan.
12. Kegiatan pengujian penetrasi dan penilaian kerentanan memberikan hasil tentang sistem Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan dalam keadaan dan waktu tertentu. Hasilnya terbatas pada bagian sistem yang menjadi cakupannya, sehingga tidak dapat menggantikan penilaian risiko yang menyeluruh.

Y. Evaluasi dan Perbaikan Berkelanjutan

1. Pemeriksaan internal atas pelaksanaan informasi atau keamanan siber :
   a. Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan harus melakukan pemeriksaan internal dalam jangka waktu yang direncanakan untuk menentukan tingkat kepatuhan dan efektivitas Sistem Manajemen Keamanan Informasi.
   b. Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan akan merencanakan, menetapkan, menerapkan dan memelihara program audit internal, termasuk frekuensi, metode, tanggung jawab, perencanaan, dan persyaratan pelaporan. Program audit internal harus mempertimbangkan pentingnya proses yang terlibat dan hasil audit sebelumnya.
   c. Tetapkan kriteria dan ruang lingkup untuk setiap pemeriksaan.
   d. Dinas Komunikasi Informatika, Statistik dan Persandian Kabupaten Katingan memilih tim audit internal yang memastikan objektivitas dan ketidakberpihakan proses audit.
   e. Memastikan bahwa hasil inspeksi dilaporkan kepada Bupati Katingan dan menyimpan informasi terdokumentasi sebagai bukti bahwa audit internal telah dilakukan.
2. Tinjauan manajemen atas penerapan keamanan informasi atau cyber :
   a. Rapat tinjauan manajemen adalah mekanisme untuk memeriksa implementasi dan perbaikan berkelanjutan SMKI. Pelaksanaan dilakukan minimal setahun sekali yang dapat dilakukan melalui rapat internal.
   b. Bentuk kegiatan yang harus dicakup dan dipertimbangkan selama tinjauan manajemen adalah sebagai berikut :
      1) Status tindakan dari tinjauan manajemen sebelumnya;
      2) Perubahan pada isu internal dan eksternal yang relevan;
      3) Meliputi kinerja keamanan informasi, termasuk tren ketidaksesuaian dan tindakan korektif, hasil pemantauan dan pengukuran, dan hasil audit internal atau audit eksternal;
      4) Pemenuhan tujuan keamanan informasi;
      5) Masukan dari pihak yang berkepentingan;
      6) Hasil kegiatan penilaian risiko dan status rencana penanganan risiko; dan
      7) Peluang untuk perbaikan terus-menerus.
   c. Dokumen hasil diskusi harus didokumentasikan secara tertib.

Pj. BUPATI KATINGAN,

SAIFUL