SALINAN

BUPATI LANDAK
PROVINSI KALIMANTAN BARAT

PERATURAN BUPATI LANDAK
NOMOR 24 TAHUN 2023

TENTANG

PEDOMAN PENYELENGGARAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI DI LINGKUNGAN PEMERINTAH KABUPATEN LANDAK

DENGAN RAHMAT TUHAN YANG MAHA ESA

BUPATI LANDAK,

Menimbang : a. bahwa berdasarkan Peraturan Kepala Lembaga Sandi Negara Nomor 7 Tahun 2017 tentang Pedoman Penyelenggaraan Persandian untuk Pengamanan Informasi di Lingkungan Pemerintah Daerah Provinsi, Kabupaten/Kota menegaskan perlunya upaya pengamanan informasi yang terintegrasi antara pusat, provinsi dan kabupaten/kota;

b. bahwa dalam rangka melindungi informasi di Pemerintah Kabupaten Landak perlu dilakukan upaya pengamanan informasi melalui penyelenggaraan persandian;

c. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b, perlu menetapkan Peraturan Bupati tentang Pedoman Penyelenggaraan Persandian untuk Pengamanan Informasi di Lingkungan Pemerintah Kabupaten Landak.

Mengingat : 1. Pasal 18 ayat (6) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;

2. Undang-Undang Republik Indonesia Nomor 55 Tahun 1999 tentang Pembentukan Kabupaten Landak (Lembaran Negara Republik Indonesia Tahun 1999 Nomor 183, Tambahan Lembaran Negara Republik Indonesia Nomor 3904) sebagaimana telah diubah dengan Undang-Undang Nomor 15 Tahun 2000 tentang Perubahan Atas

Undang-Undang Nomor 55 Tahun 1999 tentang Pembentukan Kabupaten Landak (Lembaran Negara Republik Indonesia Tahun 2000 Nomor 82, Tambahan Lembaran Negara Republik Indonesia Nomor 3970);

3. Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843);
4. Undang-Undang Republik Indonesia Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (Lembaran Negara Republik Indonesia. Tahun 2008 Nomor 61, Tambahan Lembaran Negara Republik Indonesia Nomor 4846);
5. Undang-Undang Republik Indonesia Nomor 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik Indonesia Nomor 5587) sebagaimana telah diubah beberapa kali dan yang terakhir dengan Undang-Undang Nomor 1 Tahun 2022 tentang Hubungan Keuangan Antara Pemerintah Pusat dan Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 4, Tambahan Lembaran Negara Republik Indonesia Nomor 6757);
6. Undang-Undang Republik Indonesia Nomor 30 Tahun 2014 tentang Administrasi Pemerintahan (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 292, Tambahan Lembaran Negara Republik Indonesia Nomor 5601);
7. Peraturan Pemerintah Nomor 61 Tahun 2010 tentang Pelaksanaan Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan lnformasi Publik (Lembaran Negara Republik Indonesia Tahun 2010 Nomor 99, Tambahan Lembaran Negara Republik Indonesia Nomor 5149);
8. Peraturan Pemerintah Nomor 12 Tahun 2017 tentang Pembinaan dan Pengawasan Penyelenggaraan Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2017 Nomor 73, Tambahan Lembaran

Negara Republik Indonesia Nomor 6041);Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 244, Tambahan Lembaran Negara Republik Indonesia Nomor 5587) sebagaimana telah diubah beberapa kali, terakhir dengan Undang-Undang Nomor 9 Tahun 2015 tentang Perubahan Kedua Atas Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2015 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 5679);

9. Peraturan Presiden Republik Indonesia Nomor 79 Tahun 2008 tentang Tunjangan Pengamanan Persandian;
10. Peraturan Presiden Republik Indonesia Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
11. Peraturan Presiden Republik Indonesia Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 129);
12. Peraturan Presiden Republik Indonesia Nomor 132 Tahun 2022 tentang Arsitektur Sistem Pemerintahan Berbasis Elektronik Nasional (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 233);
13. Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 8 Tahun 2019 tentang Penyelenggaraan Urusan Pemerintahan Konkuren Bidang Komunikasi dan Informatika (Berita Negara Republik Indonesia Tahun 2019 Nomor 1026);
14. Peraturan Kepala Badan Siber dan Sandi Negara Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian untuk Pengamanan Informasi di Pemerintah Daerah (Berita Negara Republik Indonesia Tahun 2019 Nomor 1054);
15. Peraturan Kepala Badan Siber dan Sandi Negara Nomor 8 Tahun 2020 tentang Sistem Pengamanan dalam

Penyelenggaraan Sistem Elektronik (Berita Negara Republik Indonesia Tahun 2020 Nomor 1375);

16. Peraturan Kepala Badan Siber dan Sandi Negara Nomor 10 Tahun 2020 tentang Tim Tanggap Insiden Siber (Berita Negara Republik Indonesia Tahun 2020 Nomor 1488);
17. Peraturan Kepala Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Managemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik (Berita Negara Republik Indonesia Tahun 2021 Nomor 541);

MEMUTUSKAN:

Menetapkan : PERATURAN BUPATI TENTANG PEDOMAN PENYELENGGARAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI DI LINGKUNGAN PEMERINTAH KABUPATEN LANDAK

BAB I
KETENTUAN UMUM

Bagian Kesatu
Pengertian

Pasal 1

Dalam Peraturan Bupati ini yang dimaksud dengan:

1. Daerah adalah Kabupaten Landak.
2. Pemerintah Daerah adalah Pemerintah Kabupaten Landak.
3. Bupati adalah Bupati Landak.
4. Pemerintahan Daerah adalah penyelenggaraan urusan pemerintahan Pemerintah Daerah dan DPRD menurut asas otonomi dan tugas pembantuan dengan prinsip otonomi seluas-luasnya dalam sistem dan prinsip Negara Kesatuan Republik Indonesia sebagaimana dimaksud dalam Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

5. Dinas Komunikasi dan Informatika yang selanjutnya disebut Dinas adalah dinas yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika, statistik dan persandian.
6. Persandian adalah kegiatan di bidang pengamanan data/informasi yang dilaksanakan dengan menerapkan konsep, teori, seni dan ilmu kripto beserta ilmu pendukung lainnya secara sistematis, metodologis dan konsisten serta terkait pada etika profesi sandi.
7. Penyelenggaraan persandian merupakan penjabaran atas pelaksanaan kebijakan, program dan kegiatan di bidang persandian.
8. Penyelenggara persandian untuk pengamanan informasi di lingkungan pemerintahan daerah kabupaten yang selanjutnya disebut sebagai penyelenggara persandian kabupaten terdiri atas bupati dibantu oleh Dinas.
9. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada pengguna SPBE.
10. Keamanan SPBE adalah pengendalian keamanan yang terpadu dalam SPBE.
11. Manajemen Keamanan SPBE adalah serangkaian proses untuk mencapai penerapan keamanan SPBE yang efektif, efisien dan berkesinambungan serta mendukung layanan SPBE yang berkualitas.
12. Layanan SPBE adalah keluaran yang dihasilkan oleh 1 (satu) atau beberapa fungsi aplikasi SPBE dan yang memiliki nilai manfaat.
13. Aplikasi SPBE adalah satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas atau fungsi Layanan SPBE.
14. Jaringan Intra adalah jaringan tertutup yang menghubungkan antar simpul jaringan dalam suatu organisasi.
15. Sistem Penghubung Layanan adalah perangkat integrase/penghubung untuk melakukan pertukaran Layanan SPBE.
16. Infrastruktur SPBE adalah semua perangkat keras, perangkat lunak, dan fasilitas yang menjadi penunjang utama untuk menjalankan sistem, aplikasi, komunikasi data, pengolahan dan penyimpanan data, perangkat integrasi/penghubung dan perangkat elektronik lainnya.
17. Jaring Komunikasi Sandi yang selanjutnya disingkat JKS adalah keterhubungan antar pengguna persandian melalui jaring telekomunikasi.

18. Informasi adalah keterangan, pernyataan, gagasan dan tanda-tanda yang mengandung nilai, makna dan pesan baik data, fakta, maupun penjelasannya yang dapat dilihat, didengar dan dibaca yang disajikan dalam berbagai kemasan dan format sesuai dengan perkembangan teknologi informasi dan komunikasi secara elektronik ataupun nonelektronik.
19. Informasi publik adalah Informasi yang dihasilkan, disimpan, dikelola, dikirim dan/atau diterima oleh suatu badan publik yang berkaitan dengan penyelenggara dan pelenggaraan negara dan/atau penyelenggara badan publik lainnya yang sesuai dengan Undang-Undang serta informasi lain yang berkaitan dengan kepentingan publik.
20. Informasi berklasifikasi adalah informasi publik yang dikecualikan menurut ketentuan peraturan perundang-undangan.
21. Keamanan Informasi adalah terjaganya kerahasiaan, keaslian, keutuhan, ketersediaan dan kenirsangkalan Informasi.
22. Pengamanan Informasi adalah segala upaya, kegiatan dan tindakan untuk mewujudkan Keamanan Informasi.
23. Materiil Sandi yang selanjutnya disingkat matsan adalah barang atau benda dalam penyelenggaraan persandian.
24. Sumber daya manusia adalah sumber daya manusia aparatur Pemerintah Daerah.
25. Insiden Siber adalah satu atau serangkaian kejadian yang mengganggu atau mengancam berjalannya Sistem Elektronik.
26. Tim Tanggap Insiden Siber adalah sekelompok orang yang bertanggung jawab menangani Insiden Siber dalam ruang lingkup yang ditentukan terhadapnya.
27. Badan Siber dan Sandi Negara yang selanjutnya disingkat BSSN adalah lembaga pemerintah non Kementerian.
28. Tunjangan Pengamanan Persandian yang selanjutnya di singkat TPP adalah tunjangan khusus yang diberikan kepada Pegawai Negeri yang diangkat dan ditugaskan secara penuh sesuai dengan ketentuan peraturan perundang-undangan sebagai pengelola pengamanan persandian di lingkungan instansi pemerintah pusat dan daerah, sebagai bentuk kompensasi atas tanggung jawab dalam melaksanakan tugas di bidang penyelenggaraan pengamanan persandian.
29. Operasi Siaga Kontra Penginderaan yang selanjutnya disebut Kontra Penginderaan adalah kegiatan yang dibatas waktu untuk melakukan

pencegahan terhadap pengawasan pihak lain, termasuk metode-metode yang melibatkan peralatan elektronik seperti *bugsweeping* dan mendeteksi adanya peralatan pengawasan (*surveillance*).

30. *Penetration Test* yang selanjutnya disingkat PENTEST adalah pengujian keamanan informasi dimana seorang asesor meniru serangan yang biasa sering terjadi untuk mengidentifikasi metode peretasan fitur keamanan aplikasi, sistem, atau jaringan.
31. *Security Operation Center* yang selanjutnya disingkat SOC adalah kegiatan Pengamanan Informasi dengan melakukan proses pengawasan, pelindungan dan penanggulangan insiden keamanan informasi dengan memperhatikan aspek personil, proses pelaksanaan dan ketersediaan teknologi.
32. *Assessment* adalah suatu proses untuk mengetahui kemampuan seseorang, terhadap suatu kompetensi, berdasarkan bukti-bukti.
33. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan dan/atau menyebarkan informasi elektronik.
34. Sertifikat Elektronik adalah sertifikat yang bersifat elektronik yang memuat tanda tangan elektronik dan identitas yang menunjukkan status subjek hukum para pihak dalam transaksi elektronik yang dikeluarkan oleh penyelenggara sertifikasi elektronik.
35. Layanan Keamanan Informasi adalah keluaran dari pelaksanaan 1 (satu) atau beberapa kegiatan penyelenggaraan Urusan Pemerintahan bidang Persandian dan yang memiliki nilai manfaat.
36. Pengguna Layanan Keamanan Informasi yang selanjutnya disebut Pengguna Layanan adalah para pihak yang memanfaatkan Layanan Keamanan Informasi.
37. *Application Programming Interface* yang selanjutnya disingkat API adalah sekumpulan perintah, fungsi serta protokol yang mengintegrasikan dua bagian dari aplikasi atau dengan aplikasi yang berbeda secara bersamaan.
38. Pusat Data adalah fasilitas yang digunakan untuk penempatan sistem elektronik dan komponen terkait lainnya untuk keperluan penempatan, penyimpanan dan pengolahan data serta pemulihan data.
39. Pusat Data Nasional adalah sekumpulan Pusat Data yang digunakan secara bagi pakai oleh Instansi Pusat dan Pemerintah Daerah yang saling terhubung.

Bagian Kedua

Maksud, Tujuan dan Ruang Lingkup

Pasal 2

Peraturan Bupati ini dimaksudkan untuk memberikan pedoman dalam melaksanakan kebijakan, program dan kegiatan penyelenggaraan persandian untuk Pengamanan Informasi di lingkungan Pemerintah Daerah.

Pasal 3

Pelaksanaan persandian untuk pengamanan informasi di lingkungan Pemerintah Daerah bertujuan untuk:

a. menciptakan harmonisasi dalam pembagian urusan pemerintahan di bidang persandian;
b. memfasilitasi pemerintah kabupaten dalam melaksanakan penyelenggaraan persandian untuk pengamanan informasi;
c. meningkatkan efektivitas pelaksanaan kebijakan, program dan kegiatan penyelenggaraan persandian untuk pengamanan informasi;
d. memberikan pedoman bagi Pemerintah Daerah dalam menetapkan pola hubungan komunikasi sandi antar perangkat daerah;
e. memberikan pedoman manajemen keamanan informasi SPBE bagi Pemerintah Daerah; dan
f. sebagai standar teknis dan prosedur keamanan SPBE.

Pasal 4

Ruang lingkup Peraturan Bupati ini meliputi:

a. Perencanaan;
b. Pelaksanaan;
c. Operasional dukungan persandian;
d. Pemantauan, evaluasi dan pelaporan;
e. Koordinasi dan konsultasi; dan
f. Pembiayaan.

BAB II

PERENCANAAN

Pasal 5

(1) Perencanaan Persandian untuk Pengamanan Informasi di lingkungan Pemerintah Kabupaten Landak dituangkan dalam bentuk Rencana Strategis Pengamanan Informasi.

(2) Rencana Strategis Pengamanan Informasi sebagaimana dimaksud pada ayat (1) disusun oleh Dinas dan dikoordinasikan dengan perangkat daerah yang membidangi perencanaan pembangunan daerah.

(3) Rencana strategis sebagaimana dimaksud pada ayat (1) terdiri atas:
   a. tujuan, sasaran, program, kegiatan dan target pelaksanaan Pengamanan Informasi setiap tahun untuk jangka waktu 5 (lima) tahun; dan
   b. peta rencana penyelenggaraan Pengamanan Informasi yang merupakan penjabaran dari tahapan rencana strategis yang akan dicapai setiap tahun untuk jangka waktu 5 (lima) tahun.

(4) Rencana Strategis Pengamanan Informasi sebagaimana dimaksud pada ayat (1) ditetapkan dengan Keputusan Bupati.

Pasal 6

(1) Rencana Strategis Pengamanan Informasi yang telah disusun sebagaimana dimaksud dalam Pasal 5 ayat (1) diintegrasikan ke dalam Rencana Pembangunan Jangka Menengah Daerah (RPJMD).

(2) Penyusunan rencana strategis sebagaimana dimaksud pada ayat (1) dikoordinasikan dan dikonsultasikan oleh Dinas kepada BSSN.

BAB III

PELAKSANAAN

Bagian Kesatu

Umum

Pasal 7

(1) Pelaksanaan Persandian untuk Pengamanan Informasi di Lingkungan Pemerintah Daerah meliputi:
   a. penyelenggaraan persandian untuk pengamanan informasi;
   b. penetapan pola hubungan komunikasi sandi antar Perangkat Daerah;

c. penyelenggaraan Sertifikat Elektronik di lingkungan Pemerintah Daerah untuk mendukung SPBE; dan
d. penyelenggaraan manajemen keamanan informasi SPBE;

(2) Pelaksanaan Persandian untuk Pengamanan Informasi sebagaimana dimaksud pada ayat (1) dilaksanakan oleh Bupati melalui:
a. penguatan kapasitas kelembagaan, sumber daya manusia dan sarana prasarana;
b. mengoordinasikan kegiatan antar Perangkat Daerah; dan
c. kerjasama dengan kabupaten/kota, provinsi lain dan/atau kabupaten/kota di provinsi lain.

Pasal 8

(1) Pelaksanaan persandian untuk Pengamanan Informasi sebagaimana dimaksud meliputi:
a. penyediaan analisis kebutuhan penyelenggaraan persandian untuk Pengamanan Informasi;
b. penyediaan kebijakan penyelenggaraan persandian untuk Pengamanan Informasi;
c. pengelolaan dan pelindungan informasi;
d. pengelolaan sumber daya persandian meliputi sumber daya manusia, matsan dan JKS serta anggaran;
e. penyelenggaraan operasional dukungan Persandian untuk Pengamanan Informasi;
f. pengawasan dan evaluasi penyelenggaraan Pengamanan Informasi melalui persandian di seluruh Perangkat Daerah; dan
g. koordinasi dan konsultasi penyelenggaraan persandian untuk Pengamanan Informasi.

(2) Pengamanan Informasi sebagaimana dimaksud pada ayat (1) mencakup pengamanan fisik, pengamanan logis dan pelindungan secara administrasi.

Bagian Kedua

Penyelenggaraan Persandian untuk Pengamanan Informasi

Paragraf 1

Umum

Pasal 9

Penyelenggaraan persandian untuk Pengamanan Informasi dilaksanakan melalui:

a. penyusunan kebijakan Pengamanan Informasi;
b. pengelolaan Sumber Daya Keamanan Informasi;
c. pengamanan sistem elektronik dan pengamanan informasi nonelektronik; dan
d. penyediaan Layanan Keamanan Informasi.

Paragraf 2

Penyusunan Kebijakan Pengamanan Informasi

Pasal 10

Penyusunan kebijakan Pengamanan Informasi sebagaimana dimaksud dalam Pasal 9 huruf a dilaksanakan dengan:

a. menyusun rencana strategis Pengamanan Informasi;
b. menetapkan arsitektur Keamanan Informasi; dan
c. menetapkan aturan mengenai tata kelola Keamanan Informasi.

Pasal 11

Penyusunan Rencana Strategis Pengamanan Informasi sebagaimana dimaksud dalam Pasal 10 huruf a dilaksanakan sesuai ketentuan Pasal 5 dan Pasal 6 Peraturan Bupati ini.

Pasal 12

(1) Arsitektur Keamanan Informasi sebagaimana dimaksud dalam Pasal 10 huruf b disusun oleh Dinas.
(2) Arsitektur Keamanan Informasi sebagaimana dimaksud pada ayat (1) memuat:
    a. infrastruktur teknologi informasi;
    b. desain keamanan perangkat teknologi informasi dan keamanan jaringan; dan

c. aplikasi keamanan perangkat teknologi informasi dan keamanan jaringan.

(3) Penyusunan Arsitektur Keamanan Informasi sebagaimana dimaksud pada ayat (1) dikoordinasikan dan dikonsultasikan oleh Dinas kepada BSSN.

(4) Arsitektur Keamanan Informasi yang telah disusun dan ditetapkan sebagaimana dimaksud pada ayat (1) berlaku untuk jangka waktu 5 (lima) tahun.

(5) Arsitektur Keamanan Informasi dilakukan evaluasi pada paruh waktu dan tahun terakhir pelaksanaan atau sewaktu waktu sesuai dengan kebutuhan.

Pasal 13

(1) Aturan mengenai tata kelola Keamanan Informasi sebagaimana dimaksud dalam Pasal 10 huruf c dituangkan dalam Standar Operasional Prosedur yang ditetapkan dengan Keputusan Kepala Dinas.

(2) Aturan mengenai tata kelola Keamanan Informasi sebagaimana dimaksud pada ayat (1) paling sedikit terdiri atas:
   a. keamanan sumber daya teknologi informasi;
   b. keamanan akses kontrol;
   c. keamanan data dan informasi;
   d. keamanan sumber daya manusia;
   e. keamanan jaringan;
   f. keamanan surat elektronik;
   g. keamanan pusat data; dan/atau
   h. keamanan komunikasi.

(3) Penyusunan aturan mengenai tata kelola Keamanan Informasi dilaksanakan oleh Dinas dan dikoordinasikan kepada Unit Kerja Perangkat Daerah yang membidangi urusan pemerintahan dibidang hukum.

(4) Penyusunan aturan mengenai tata kelola Keamanan Informasi sebagaimana dimaksud pada ayat (1) dikoordinasikan dan dikonsultasikan oleh Dinas kepada BSSN.

Paragraf 3

Pengelolaan Sumber Daya Keamanan Informasi

Pasal 14

(1) Pengelolaan sumber daya Keamanan Informasi sebagaimana dimaksud dalam Pasal 9 huruf b dilaksanakan oleh Perangkat Daerah terkait.

(2) Pengelolaan sumber daya Keamanan Informasi sebagaimana dimaksud pada ayat (1) terdiri atas:

a. pengelolaan aset keamanan teknologi informasi dan komunikasi;

b. pengelolaan sumber daya manusia; dan

c. manajemen pengetahuan.

Pasal 15

(1) Pengelolaan aset keamanan teknologi informasi dan komunikasi sebagaimana dimaksud dalam Pasal 14 ayat (2) huruf a dilakukan oleh Dinas dan berkoordinasi dengan Perangkat Daerah yang membidangi urusan aset daerah.

(2) Pengelolaan aset keamanan teknologi Informasi dan komunikasi dilakukan melalui perencanaan, pengadaan, pemanfaatan dan penghapusan terhadap aset keamanan teknologi informasi dan komunikasi sesuai dengan ketentuan peraturan perundang-undangan.

(3) Aset keamanan teknologi informasi dan komunikasi sebagaimana dimaksud pada ayat (1) merupakan perangkat yang digunakan untuk mengidentifikasi, mendeteksi, memproteksi, menganalisis, menanggulangi dan/atau memulihkan insiden Keamanan Informasi dalam Sistem Elektronik.

Pasal 16

(1) Pengelolaan sumber daya manusia sebagaimana dimaksud dalam Pasal 14 ayat (2) huruf b dilakukan oleh Dinas dan berkoordinasi dengan Perangkat Daerah yang membidangi urusan kepegawaian dan Perangkat Daerah yang membidangi urusan pengembangan sumber daya manusia.

(2) Pengelolaan sumber daya manusia sebagaimana dimaksud pada ayat (1) dilakukan melalui serangkaian proses sebagai berikut:

a. pengembangan kompetensi;

b. pembinaan karir;

c. pendayagunaan; dan

d. pemberian TPP.

Pasal 17

(1) Pengembangan kompetensi sebagaimana dimaksud dalam Pasal 16 ayat (2) huruf a dilaksanakan dengan ketentuan:
   a. melalui tugas belajar, pendidikan dan pelatihan pembentukan dan penjenjangan fungsional, pendidikan dan pelatihan teknis, bimbingan teknis, asistensi, workshop, seminar dan kegiatan lainnya yang terkait pengembangan kompetensi sumber daya manusia di bidang Keamanan Informasi;
   b. mengikuti berbagai kegiatan pengembangan kompetensi yang dilaksanakan oleh BSSN, pihak lainnya, atau Pemerintah Daerah masing-masing; dan
   c. memenuhi jumlah waktu minimal seorang pegawai untuk meningkatkan kompetensi di bidang Keamanan Informasi.

(2) Pembinaan karir sebagaimana dimaksud dalam Pasal 16 ayat (2) huruf b dilaksanakan dengan ketentuan:
   a. pembinaan jabatan fungsional di bidang Keamanan Informasi; dan
   b. pengisian formasi jabatan pimpinan tinggi, jabatan administrator dan jabatan pengawas sesuai dengan standar kompetensi yang ditetapkan.

(3) Pendayagunaan sebagaimana dimaksud dalam Pasal 16 ayat (2) huruf c dilaksanakan agar seluruh sumber daya manusia yang bertugas di bidang Keamanan Informasi melaksanakan tugasnya sesuai dengan sasaran kinerja pegawai dan standar kompetensi kerja pegawai yang ditetapkan; dan

(4) Pemberian TPP sebagaimana dimaksud dalam Pasal 16 ayat (2) huruf d dilaksanakan dengan ketentuan:
   a. pengelola persandian di lingkungan Pemerintah Daerah berhak menerima TPP dengan besaran sesuai ketentuan peraturan perundang-undangan;
   b. TPP dianggarkan secara berkala setiap tahun sebelum tahun anggaran berjalan; dan
   c. pengelola persandian yang berhak menerima TPP ditetapkan dengan Keputusan Bupati.

Pasal 18

(1) Manajemen pengetahuan sebagaimana dimaksud dalam Pasal 14 ayat (2) huruf c dilakukan untuk meningkatkan kualitas Layanan Keamanan Informasi dan mendukung proses pengambilan keputusan terkait Keamanan Informasi.
(2) Manajemen pengetahuan dilakukan melalui serangkaian proses pengumpulan, pengolahan, penyimpanan, penggunaan dan alih pengetahuan dan teknologi yang dihasilkan dalam pelaksanaan Keamanan Informasi Pemerintah Daerah.
(3) Manajemen pengetahuan sebagaimana dimaksud pada ayat (2) dilaksanakan berdasarkan pedoman manajemen pengetahuan Keamanan Informasi Pemerintah Daerah.
(4) Manajemen pengetahuan sebagaimana dimaksud pada ayat (1) dilakukan oleh Dinas.
(5) Dalam pelaksanaan manajemen pengetahuan, Dinas berkoordinasi dan berkonsultasi dengan BSSN.

Paragraf 4

Pengamanan Sistem Elektronik dan Pengamanan Informasi Nonelektronik

Pasal 19

Pengamanan Sistem Elektronik dan Pengamanan Informasi nonelektronik sebagaimana dimaksud dalam Pasal 9 huruf c dilaksanakan oleh Dinas.

Pasal 20

Pengamanan Sistem Elektronik sebagaimana dimaksud dalam Pasal 19 terdiri atas:

a. penjaminan kerahasiaan, keutuhan, ketersediaan, keaslian dan nirsangkal terhadap data dan informasi;
b. penjaminan ketersediaan infrastruktur yang terdiri atas pusat data, jaringan intra pemerintah dan sistem penghubung layanan penyelenggaraan pemerintahan berbasis elektronik; dan
c. penjaminan keutuhan, ketersediaan dan keaslian aplikasi.

Pasal 21

(1) Dalam melaksanakan Pengamanan Sistem Elektronik sebagaimana dimaksud dalam Pasal 20, Dinas melakukan:

a. identifikasi;
b. deteksi;
c. proteksi; dan
d. penanggulangan dan pemulihan.

(2) Identifikasi sebagaimana dimaksud pada ayat (1) huruf a dilakukan melalui kegiatan analisis kerawanan dan risiko terhadap Sistem Elektronik.

(3) Deteksi sebagaimana dimaksud pada ayat (1) huruf b dilakukan melalui kegiatan analisis untuk menentukan adanya ancaman atau kejadian insiden pada Sistem Elektronik.

(4) Proteksi sebagaimana dimaksud pada ayat (1) huruf c dilakukan dengan kegiatan mitigasi risiko dan penerapan pelindungan terhadap Sistem Elektronik untuk menjamin keberlangsungan penyelenggaraan pemerintahan berbasis elektronik.

(5) Penanggulangan dan pemulihan sebagaimana dimaksudpada ayat (1) huruf d dilakukan dengan kegiatan penanganan yang tepat dan perbaikan terhadap adanya insiden pada Sistem Elektronik agar penyelenggaraan pemerintahan berbasis elektronik berfungsi kembali dengan baik.

Pasal 22

(1) Dalam mendukung penyelenggaraan Pengamanan Sistem Elektronik sebagaimana dimaksud dalam Pasal 21 ayat (1) Pemerintah Daerah dapat menyelenggarakan pusat operasi Pengamanan Informasi sesuai standar yang ditetapkan oleh BSSN.

(2) Pusat operasi Pengamanan Informasi sebagaimana dimaksud pada ayat (1) bertujuan untuk pengamanan Sistem Elektronik dengan melakukan proses pengawasan, penanggulangan dan pemulihan atas insiden keamanan Sistem Elektronik dengan memperhatikan aspek personel, proses pelaksanaan dan ketersediaan teknologi.

Pasal 23

(1) Pengamanan informasi nonelektronik sebagaimana dimaksud dalam Pasal 19 dilakukan pada tahapan pemrosesan, pengiriman, penyimpanan dan pemusnahan informasi nonelektronik.

(2) Pengamanan Informasi nonelektronik sebagaimana dimaksud pada ayat (1) dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 24

(1) Dinas melaksanakan audit Keamanan Informasi di lingkup Pemerintah Daerah.
(2) Audit Keamanan Informasi meliputi audit keamanan Sistem Elektronik dan audit pelaksanaan sistem manajemen.
(3) Audit Keamanan Informasi sebagaimana dimaksud pada ayat (2) dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

Paragraf 5

Penyediaan Layanan Keamanan Informasi

Pasal 25

(1) Penyediaan Layanan Keamanan Informasi sebagaimana dimaksud dalam Pasal 9 huruf d dilaksanakan oleh Dinas.
(2) Layanan Keamanan Informasi sebagaimana dimaksud pada ayat (1) disediakan untuk Pengguna Layanan yang terdiri atas:
    a. Kepala Daerah dan Wakil Kepala Daerah;
    b. Perangkat Daerah;
    c. pegawai atau Aparatur Sipil Negara pada Pemerintah Daerah; dan
    d. pihak lainnya.

Pasal 26

Jenis Layanan Keamanan Informasi sebagaimana dimaksud dalam Pasal 25 ayat (1) meliputi:

a. identifikasi kerentanan dan penilaian risiko terhadap Sistem Elektronik;
b. asistensi dan fasilitasi penguatan keamanan Sistem Elektronik;
c. penerapan Sertifikat Elektronik untuk melindungi Sistem Elektronik dan dokumen elektronik;
d. pelindungan Informasi melalui penyediaan perangkat teknologi Keamanan Informasi dan JKS;
e. fasilitasi sertifikasi penerapan manajemen pengamanan Sistem Elektronik;
f. audit Keamanan Sistem Elektronik;
g. audit keamanan pelaksanaan sistem manajemen;
h. literasi Keamanan Informasi dalam rangka peningkatan kesadaran Keamanan Informasi dan pengukuran tingkat kesadaran Keamanan Informasi di lingkungan Pemerintah Daerah dan publik;

i. peningkatan kompetensi sumber daya manusia di bidang Keamanan Informasi dan/atau Persandian;
j. pengelolaan pusat operasi Pengamanan Informasi melalui SOC;
k. penanganan Insiden Siber;
l. forensik digital;
m. pelindungan Informasi pada kegiatan penting Pemerintah Daerah melalui teknik pengamanan gelombang frekuensi atau sinyal;
n. pelindungan Informasi pada aset/fasilitas penting milik atau yang akan digunakan Pemerintah Daerah melalui kegiatan kontra penginderaan;
o. konsultasi Keamanan Informasi bagi Pengguna Layanan; dan/atau
p. jenis Layanan Keamanan Informasi lainnya.

Pasal 27

(1) Penanganan Insiden Siber sebagaimana dimaksud dalam Pasal 26 huruf k dan forensik digital sebagaimana dimaksud dalam Pasal 26 huruf I dilakukan oleh Tim Tanggap Insiden Siber.
(2) Tim Tanggap Insiden Siber sebagaimana dimaksud ayat (1) terdiri atas:
    a. Tim Tanggap Insiden Siber nasional;
    b. Tim Tanggap Insiden Siber sektoral;
    c. Tim Tanggap Insiden Siber organisasi; dan
    d. Tim Tanggap Insiden Siber khusus.
(3) Tim Tanggap Insiden Siber sebagaimana dimaksud pada ayat (1) paling sedikit terdiri atas:
    a. ketua;
    b. anggota; dan
    c. narahubung.
(4) Tim Tanggap Insiden Siber sektoral dibentuk oleh:
    a. kementerian atau lembaga yang berwenang melakukan pengawasan pada sektornya; atau
    b. institusi yang ditunjuk oleh kementerian atau lembaga yang berwenang melakukan pengawasan pada sektornya.
(5) Sektor sebagaimana dimaksud pada ayat (2) meliputi:
    a. sektor administrasi pemerintahan;
    b. sektor energi dan sumber daya mineral;
    c. sektor transportasi;
    d. sektor keuangan;
    e. sektor kesehatan;

f. sektor teknologi informasi dan komunikasi;
g. sektor pangan;
h. sektor pertahanan; dan
i. sektor lain yang ditetapkan oleh Presiden.

(6) Tim Tanggap Insiden Siber sektoral sebagaimana dimaksud pada ayat (3) melakukan pengelolaan penanganan Insiden Siber pada sektornya.

(7) Pengelolaan penanganan Insiden Siber sebagaimana dimaksud pada ayat (5) dilakukan terhadap Insiden Siber yang mengakibatkan gangguan pada keberlangsungan layanan Sistem Elektronik pada paling sedikit 2 (dua) organisasi dan paling banyak setengah jumlah organisasi di 1 (satu) sektor.

Pasal 28

Tim Tanggap Insiden Siber sektoral sebagaimana dimaksud dalam pasal 27 bertugas:

a. menyelenggarakan layanan Tim Tanggap Insiden Siber sesuai dengan kebutuhan penanganan Insiden Siber di tingkat sektor;
b. mengoordinasikan penanganan Insiden Siber tingkat sektor dan Insiden Siber tingkat organisasi yang terjadi dalam lingkup sektornya;
c. merumuskan panduan teknis penanganan Insiden Siber tingkat sektor;
d. melakukan koordinasi dengan Tim Tanggap Siber Nasional;
e. memberikan bantuan yang diperlukan kepada pihak yang menerima layanan;
f. menyusun dan menyampaikan laporan penanganan Insiden Siber tingkat sektor dan Insiden Siber tingkat organisasi yang terjadi dalam lingkup sektornya setiap tahun dan/atau sewaktu-waktu jika diperlukan kepada Tim Tanggap Insiden Siber nasional;
g. menyediakan fasilitas dan mekanisme kerja untuk menerima laporan penanganan Insiden Siber dari pihak yang menerima layanan; dan
h. melakukan koordinasi dan/atau kerja sama dengan pihak lain dengan memperhatikan kerahasiaan inforamsi, perlindungan data dan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 29

(1) Pelaksanaan tugas Tim Tanggap Insiden Siber dapat dilakukan melalui koordinasi antar Tim Tanggap Insiden Siber.

(2) Pelaksanaan koordinasi sebagaimana dimaksud pada ayat (1) dilakukan oleh narahubung di setiap Tim Tanggap Insiden Siber.

Pasal 30

(1) Tim Tanggap Insiden Siber menyelenggarakan:
   a. layanan utama; dan
   b. layanan tambahan.
(2) Layanan utama sebagaimana dimaksud pada ayat (1) huruf a dan layanan tambahan sebagaimana dimaksud pada ayat (1) huruf b diselenggarakan berdasarkan standar nasional Indonesia ISO/IEC 27035 atau ketentuan lain sesuai dengan peraturan perundang-undangan.
(3) Layanan utama dan layanan tambahan sebagaimana dimaksud pada ayat (2) diberikan oleh Tim Tanggap Insiden Siber sektoral kepada pihak yang menerima layanan, meliputi:
   a. Tim Tanggap Insiden Siber organisasi dalam lingkup sektornya; dan
   b. institusi dalam lingkup sektornya yang menyelenggarakan Sistem Elektronik, namun belum memiliki Tim Tanggap Insiden Siber organisasi.

Pasal 31

(1) Layanan utama sebagaimana dimaksud dalam Pasal 30 ayat (1) huruf a terdiri atas:
   a. pemberian peringatan terkait keamanan siber; dan
   b. pengelolaan Insiden Siber.
(2) Pemberian peringatan terkait keamanan siber sebagaimana dimaksud pada ayat (1) huruf a merupakan penyebarluasan informasi keamanan siber kepada pihak yang menerima layanan.
(3) Pengelolaan Insiden Siber sebagaimana dimaksud pada ayat (1) huruf b merupakan kegiatan menerima, menanggapi dan menganalisis Insiden Siber.

Pasal 32

(1) Layanan Tambahan sebagaimana dimaksud dalam Pasal 30 ayat (2) huruf b terdiri atas:
   a. penanganan kerentanan sistem elektronik;
   b. penanganan artefak digital;
   c. pemberitahuan hasil pengamatan potensi ancaman;
   d. pendeteksian serangan;
   e. analisis risiko keamanan siber;
   f. konsultasi terkait kesiapan penanganan Insiden Siber; dan/atau

g. pembangunan kesadaran dan kepedulian terhadap keamanan siber.

(2) Penanganan kerentanan sistem elektronik sebagaimana dimaksud pada ayat (1) huruf a merupakan kegiatan analisis teknikal yang dilakukan dengan memeriksa kerentanan pada perangkat lunak maupun perangkat keras, serta melakukan proses verifikasi kerentanan yang mungkin dieksploitasi dengan tujuan menyusun rencana untuk memperbaiki kerentanan yang ada.

(3) Penanganan artefak digital sebagaimana dimaksud pada ayat (1) huruf b merupakan kegiatan analisis teknikal yang dilakukan dengan mencari jejak digital yang diduga digunakan untuk melakukan tindakan yang tidak sah terhadap Sistem Elektronik.

(4) Pemberitahuan hasil pengamatan potensi ancaman sebagaimana dimaksud pada ayat (1) huruf c merupakan penyampaian kepada pihak yang menerima layanan terkait ancaman terhadap Sistem Elektronik yang dapat muncul akibat perkembangan teknologi, politik, ekonomi dan perkembangan lainnya.

(5) Pendeteksian serangan sebagaimana dimaksud pada ayat (1) huruf d merupakan kegiatan menganalisis data untuk mendeteksi adanya serangan terhadap Sistem Elektronik.

(6) Analisis risiko keamanan siber sebagaimana dimaksud pada ayat (1) huruf e merupakan teknik untuk mengidentifikasi dan menilai risiko keamanan siber serta merekomendasikan tindak lanjut untuk menghadapi risiko tersebut.

(7) Konsultasi terkait kesiapan penanganan Insiden Siber sebagaimana dimaksud pada ayat (1) huruf f merupakan kegiatan konseling yang dilakukan dengan tujuan memberikan wawasan, pemahaman dan cara yang perlu dilaksanakan dalam rangka membantu penanganan Insiden Siber.

(8) Pembangunan kesadaran dan kepedulian terhadap keamanan siber sebagaimana dimaksud pada ayat (1) huruf g merupakan kegiatan diseminasi di bidang keamanan siber kepada pihak yang menerima layanan.

Pasal 33

(1) Dalam pelaksanaan layanan Tim Tanggap Insiden Siber sebagaimana dimaksud dalam Pasal 30, diperlukan sumber daya.

(2) Sumber daya sebagaimana dimaksud pada ayat (1) terdiri atas:

a. sumber daya manusia;
b. perangkat pendukung; dan
c. pendanaan.

(3) Sumber daya manusia sebagaimana dimaksud pada ayat (2) huruf a merupakan orang yang memiliki kompetensi di bidang keamanan siber.

(4) Sumber daya manusia sebagaimana dimaksud pada ayat (2) huruf b merupakan perangkat untuk mendukung operasional layanan Tim Tanggap Insiden Siber.

(5) Pendanaan sebagaimana dimaksud pada ayat (2) huruf c berasal dari sumber yang sah.

Pasal 34

Tim Tanggap Insiden Siber sektoral sebagaimana dimaksud dalam Pasal 27 ayat (2) huruf b melakukan registrasi kepada Tim Tanggap Insiden Siber nasional sebagaimana dimaksud dalam Pasal 27 ayat (2) huruf a.

Pasal 35

Registrasi sebagaimana dimaksud dalam Pasal 34 memiliki tahapan yang terdiri atas:

a. pengajuan permohonan;
b. validasi berkas permohonan; dan
c. penerbitan surat tanda register.

Pasal 36

(1) Pengajuan permohonan sebagaimana dimaksud dalam Pasal 35 huruf a disampaikan kepada Tim Tanggap Insiden Siber nasional.

(2) Dalam hal Tim Tanggap Insiden Siber nasional sebagaimana dimaksud pada ayat (1) belum terbentuk di BSSN, permohonan ditujukan kepada pejabat pimpinan tinggi madya yang melaksanakan tugas dan fungsi di bidang penanggulangan dan pemulihan insiden.

(3) Pengajuan permohonan sebagaimana dimaksud pada ayat (1) dilakukan dengan menyampaikan surat permohonan dengan melampirkan berkas yang terdiri atas:
a. formulir registrasi;
b. dokumen yang memuat profil Tim Tanggap Insiden Siber sesuai format *request for comment* 2350; dan

c. dokumen legal yang memuat pembentukan atau pelaksanaan tugas Tim Tanggap Insiden Siber.

(4) Formulir registrasi sebagaimana dimaksud pada ayat (3) huruf a paling sedikit memuat:

a. jenis Tim Tanggap Insiden Siber;

b. nama Tim Tanggap Insiden Siber; dan

c. pihak yang menerima layanan.

Pasal 37

(1) Validasi berkas permohonan sebagaimana dimaksud dalam Pasal 35 huruf b dilakukan dengan memeriksa kelengkapan dan kesesuaian berkas permohonan.

(2) Validasi sebagaimana dimaksud pada ayat (1) dilaksanakan dalam waktu paling lama 30 (tiga puluh) hari kerja sejak berkas permohonan diterima.

(3) Dalam hal hasil validasi sebagaimana dimaksud pada ayat (2) menyatakan berkas permohonan telah lengkap dan sesuai, Tim Tanggap Insiden Siber sektoral mengajukan permohonan diberikan surat tanda register.

(4) Dalam hal hasil validasi sebagaimana dimaksud pada ayat (2) menyatakan berkas permohonan belum lengkap dan belum sesuai, berkas permohonan dimaksud dikembalikan kepada Tim Tanggap Siber sektoral yang mengajukan permohonan untuk dilengkapi dan disesuaikan.

Pasal 38

(1) Penerbitan surat tanda register sebagaimana dimaksud dalam Pasal 35 huruf c dilakukan oleh ketua Tim Tanggap Insiden Siber nasional.

(2) Dalam hal Tim Tanggap Insiden Siber nasional belum terbentuk, surat tanda register sebagaimana dimaksud pada ayat (1) ditandatangani oleh pejabat pimpinan tinggi madya yang melaksanakan tugas dan fungsi di bidang penanggulangan dan pemulihan insiden.

(3) Surat tanda register sebagaimana dimaksud pada ayat (1) paling sedikit memuat:

a. nomor register;

b. jenis Tim Tanggap Insiden Siber;

c. nama Tim Tanggap Insiden Siber; dan

d. tanggal penerbitan surat tanda register.

Pasal 39

Surat tanda register sebagaimana dimaksud dalam Pasal 38 dinyatakan tidak berlaku apabila terdapat perubahan sektor yang mengakibatkan perubahan Tim Tanggap Insiden Siber sektoral;

Pasal 40

(1) Dalam menyediakan Layanan Keamanan Informasi sebagaimana dimaksud dalam Pasal 26, Dinas melaksanakan manajemen Layanan Keamanan Informasi.
(2) Manajemen Layanan Keamanan Informasi sebagaimana dimaksud pada ayat (1) bertujuan untuk menjamin keberlangsungan dan meningkatkan kualitas Layanan Keamanan Informasi kepada Pengguna Layanan.
(3) Manajemen Layanan Keamanan Informasi sebagaimana dimaksud pada ayat (1) merupakan penanganan terhadap keluhan, gangguan, masalah, permintaan dan/atau perubahan Layanan Keamanan Informasi dari Pengguna Layanan.
(4) Manajemen Layanan Keamanan Informasi sebagaimana dimaksud pada ayat (3) dilaksanakan berdasarkan pedoman Manajemen Layanan Keamanan Informasi.

Bagian Ketiga

Penetapan Pola Hubungan Komunikasi Sandi antar Perangkat Daerah

Pasal 41

(1) Penetapan pola hubungan komunikasi sandi antar perangkat daerah sebagaimana dimaksud dalam Pasal 7 ayat (1) huruf b ditetapkan oleh Bupati.
(2) Penetapan pola hubungan komunikasi sandi antar perangkat daerah dan kabupaten sebagaimana dimaksud pada ayat (1) untuk menentukan JKS internal Pemerintah Daerah.
(3) JKS internal Pemerintah Daerah sebagaimana dimaksud pada ayat (2) terdiri atas:
    a. JKS antar perangkat daerah
    b. JKS internal perangkat daerah; dan
    c. JKS pimpinan daerah.
(4) JKS antar perangkat daerah sebagaimana dimaksud pada ayat (3) huruf a menghubungkan seluruh perangkat daerah.

(5) JKS internal perangkat daerah sebagaimana dimaksud pada ayat (3) huruf b menghubungkan antar pengguna layanan di lingkup internal perangkat daerah.

(6) JKS pimpinan daerah sebagaimana dimaksud pada ayat (3) huruf c menghubungkan Bupati, wakil Bupati dan kepala perangkat daerah.

Pasal 42

(1) Penetapan pola hubungan komunikasi sandi antar perangkat daerah sebagaimana dimaksud dalam Pasal 41 ayat (1) dilaksanakan melalui:
   a. identifikasi pola hubungan komunikasi sandi; dan
   b. analisis pola hubungan komunikasi sandi.

(2) Identifikasi pola hubungan komunikasi sandi sebagaimana dimaksud pada ayat (1) huruf a, dilakukan terhadap:
   a. pola hubungan komunikasi pimpinan dan pejabat struktural internal Pemerintah Daerah;
   b. alur informasi yang dikomunikasikan antar perangkat daerah dan internal perangkat daerah;
   c. teknologi informasi dan komunikasi;
   d. infrastruktur komunikasi; dan
   e. kompetensi personel.

(3) Analisis pola hubungan komunikasi sandi sebagaimana dimaksud pada ayat (1) huruf b dilakukan terhadap hasil identifikasi pola hubungan komunikasi sandi sebagaimana dimaksud pada ayat (2).

(4) Analisis pola hubungan komunikasi sandi sebagaimana dimaksud pada ayat (3) memuat:
   a. pengguna layanan yang akan terhubung dalam JKS;
   b. topologi atau bentuk atau model keterhubungan JKS antar pengguna layanan;
   c. perangkat keamanan teknologi informasi dan komunikasi, infrastruktur komunikasi serta fasilitasi lainnya yang dibutuhkan; dan
   d. tugas dan tanggung jawab pengelola dan pengguna layanan.

(5) Hasil analisis pola hubungan komunikasi sandi sebagaimana dimaksud pada ayat (4) ditetapkan sebagai pola hubungan komunikasi sandi antar perangkat daerah kabupaten oleh Bupati dalam bentuk Keputusan Bupati.

(6) Keputusan sebagaimana dimaksud pada ayat (5) paling sedikit memuat:
   a. entitas pengguna layanan yang terhubung dalam JKS;

b. topologi atau bentuk atau model keterhubungan antar pengguna layanan;
c. sarana dan prasana yang digunakan; dan
d. tugas dan tanggung jawab pengelola dan pengguna layanan.

(7) Salinan keputusan sebagaimana dimaksud pada ayat (6) disampaikan oleh Bupati Kepada Gubernur dan ditembuskan kepada Kepala BSSN.

Bagian Keempat

Penyelenggaraan Sertifikat Elektronik di Lingkungan Pemerintah Daerah guna Mendukung Sistem Pemerintahan Berbasis Elektronik

Pasal 43

(1) Dalam melaksanakan Pengamanan Sistem Elektronik, wajib menggunakan Sertifikat Elektronik pada setiap layanan publik dan layanan pemerintahan berbasis elektronik.

(2) Sertifikat Elektronik sebagaimana dimaksud pada ayat (1) diterbitkan oleh Balai Sertifikasi Elektronik.

(3) Penyelenggaraan Sertifikat Elektronik di lingkungan Pemerintah Daerah bertujuan:
a. meningkatkan kapabilitas dan tata kelola keamanan informasi dalam penyelenggaraan Sistem Elektronik;
b. meningkatkan keamanan informasi dalam sistem elektronik;
c. meningkatkan kepercayaan, kerahasiaan, keaslian, keutuhan, ketersediaan dan kenirsangkalan terhadap implementasi Sistem Elektronik; dan
d. meningkatkan efisiensi dan efektifitas penyelenggaraan pemerintahan dan pelayanan publik.

(4) Dinas berkedudukan sebagai Otoritas Pendaftaran (OP).

Bagian Kelima

Manajemen Keamanan Informasi SPBE

Pasal 44

(1) Penyelenggaraan manajemen keamanan informasi SPBE berpedoman pada serangkaian proses manajemen keamanan informasi yang meliputi:
c. penetapan ruang lingkup;
d. penetapan penanggung jawab;

e. perencanaan;
f. dukungan pengoperasian;
g. evaluasi kinerja; dan
h. perbaikan berkelanjutan.

(2) Pemerintah Daerah mengkomunikasikan dan mendokumentasikan kegiatan manajemen keamanan informasi SPBE.

Pasal 45

(1) Penetapan ruang lingkup sebagaimana dimaksud dalam Pasal 44 ayat (1) huruf a dilakukan oleh Bupati.

(2) Penetapan ruang lingkup sebagaimana dimaksud pada ayat (1) dilakukan dengan mendefinisikan:
a. isu internal keamanan informasi SPBE dalam organisasi; dan
b. isu eksternal keamanan informasi SPBE.

(3) Isu internal keamanan informasi SPBE pada Pemerintah Daerah sebagaimana dimakud pada ayat (2) huruf a didefinisikan berdasarkan area yang menjadi prioritas organisasi terhadap pelaksanaan keamanan informasi SPBE.

(4) Area yang menjadi prioritas organisasi terhadap pelaksanaan keamanan informasi SPBE sebagaimana dimaksud pada ayat (3) paling sedikit meliputi:
a. data dan informasi SPBE;
b. aplikasi SPBE;
c. aset infrastruktur SPBE; dan
d. kebijakan keamanan informasi SPBE yang telah dimiliki.

(5) Isu eksternal keamanan informasi SPBE sebagaimana dimaksud pada ayat (2) huruf b didefinisikan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 46

(1) Penetapan penanggung jawab sebagaimana dimaksud dalam Pasal 44 ayat (1) huruf b dilaksanakan oleh Bupati.

(2) Penanggung jawab sebagaimana dimaksud pada ayat (1) dijabat oleh sekretaris daerah pada Pemerintah Daerah.

(3) Dalam melaksanakan tugas sebagai penanggung jawab keamanan SPBE, sekretaris daerah pada Pemerintah Daerah disebut sebagai koordinator SPBE.

Pasal 47

(1) Dalam melaksanakan tugas sebagai penanggung jawab keamanan SPBE, koordinator SPBE sebagaimana dimaksud dalam Pasal 46 ayat (3) menetapkan pelaksana teknis keamanan SPBE.

(2) Pelaksana teknis keamanan SPBE sebagaimana dimaksud pada ayat (1) terdiri atas:

a. pejabat pimpinan tinggi pratama yang melaksanakan tugas dan fungsi di bidang keamanan teknologi, informasi dan komunikasi pada Pemerintah Daerah, dalam hal ini adalah kepala Dinas.

b. pejabat administrator yang membawahi, membangun, memelihara dan/atau mengembangkan Aplikasi SPBE.

Pasal 48

(1) Kepala Dinas sebagaimana dimaksud dalam Pasal 47 ayat (2) huruf a mempunyai tugas

a. memastikan penerapan standar teknis dan prosedur kemanan SPBE;

b. merumuskan, mengoordinasikan dan melaksanakan program kerja dan anggaran keamanan SPBE; dan

c. melaporkan pelaksanaan manajemen keamanan informasi SPBE dan penerapan standar teknis dan prosedur keamanan SPBE kepada koordinator SPBE Pemerintah Daerah.

(2) Pejabat administrator sebagaimana dimaksud dalam Pasal 47 ayat (2) huruf b mempunyai tugas:

a. menerapkan standar teknis dan prosedur keamanan aplikasi di unit kerja masing-masing;

b. memastikan seluruh pembangunan atau pengembangan aplikasi dan infrastruktur SPBE yang dilakukan oleh pihak ketiga memenuhi standar teknis dan prosedur kemanan SPBE yang telah ditetapkan;

c. memastikan keberlangsungan proses bisnis SPBE; dan

d. berkoordinasi dengan kepala dinas terkait perumusan program kerja dan anggaran keamanan SPBE.

Pasal 49

(1) Perencanaan sebagaimana dimaksud dalam Pasal 44 ayat (1) huruf c dilakukan oleh pelaksana teknis keamanan SPBE.

(2) Perencanaan sebagaimana dimaksud pada ayat (1) dilakukan dengan merumuskan:

a. program kerja keamanan SPBE yang disusun berdasarkan kategori risiko keamanan SPBE; dan
b. target realisasi program kerja keamanan SPBE.

(3) Program kerja keamanan SPBE sebagaimana dimaksud pada ayat (2) huruf a paling sedikit meliputi:
a. edukasi kesadaran keamanan SPBE;
b. penilaian kerentanan keamanan SPBE;
c. peningkatan keamanan SPBE;
d. penanganan insiden keamanan SPBE; dan
e. audit keamanan SPBE.

(4) Kategori risiko keamanan SPBE sebagaimana dimaksud pada ayat (2) huruf a ditentukan sesuai dengan ketentuan peraturan perundang-undangan.

(5) Target realisasi program kerja keamanan SPBE sebagaimana dimaksud pada ayat (2) huruf b ditetapkan berdasarkan kebutuhan Pemerintah Daerah.

Pasal 50

Edukasi kesadaran keamanan SPBE sebagaimana dimaksud dalam Pasal 49 ayat (3) huruf a dilaksanakan paling sedikit melalui kegiatan:
a. sosialisasi; dan
b. pelatihan.

Pasal 51

Penilaian kerentanan keamanan SPBE sebagaimana dimaksud dalam Pasal 49 ayat (3) huruf b dilaksanakan paling sedikit melalui:
a. menginventarisasi seluruh *asset* SPBE meliputi data dan informasi, aplikasi dan infrastruktur;
b. mengidentifikasi kerentanan dan ancaman terhadap *asset* SPBE; dan
c. mengukur tingkat risiko keamanan SPBE.

Pasal 52

(1) Peningkatan keamanan SPBE sebagaimana dimaksud dalam Pasal 49 ayat (3) huruf c dilaksanakan berdasarkan hasil dari penilaian kerentanan keamanan SPBE sebagaimana dimaksud dalam Pasal 49 ayat (3) huruf b.

(2) Peningkatan keamanan SPBE dilaksanakan paling sedikit melalui:
a. menerapkan standar teknis dan prosedur keamanan SPBE; dan

b. menguji fungsi keamanan tehadap aplikasi SPBE dan infrastruktur SPBE.

Pasal 53

Penanganan insiden keamanan SPBE sebagaimana dimaksud dalam Pasal 49 ayat (3) huruf d dilaksanakan paling sedikit melalui:

a. mengidentifikasi sumber serangan;
b. menganalisis informasi yang berkaitan dengan insiden selanjutnya;
c. memprioritaskan penanganan insiden berdasarkan tingkat dampak yang terjadi;
d. mendokumentasi bukti insiden yang terjadi; dan
e. memitigasi atau mengurangi dampak risiko Keamanan SPBE.

Pasal 54

Audit keamanan SPBE sebagaimana dimaksud dalam Pasal 49 ayat (3) huruf e dilakukan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 55

(1) Dukungan pengoperasian sebagaimana dimaksud dalam Pasal 44 ayat (1) huruf d dilakukan oleh koordinator SPBE.
(2) Dukungan pengoperasian sebagaimana dimaksud pada ayat (1) dilakukan dengan meningkatkan kapasitas terhadap:
    a. sumber daya manusia keamanan SPBE; dan
    b. anggaran keamanan SPBE.
(3) Sumber daya manusia keamanan SPBE sebagaimana dimaksud pada ayat (2) huruf a paling sedikit harus memiliki kompetensi:
    a. keamanan infrastruktur teknologi, informasi dan komunikasi; dan
    b. keamanan aplikasi.
(4) Untuk memenuhi kompetensi sebagaimana dimaksud pada ayat (3), Pemerintah Daerah paling sedikit melakukan kegiatan:
    a. pelatihan dan/atau sertifikasi kompetensi keamanan infrastruktur teknologi, informasi dan komunikasi dan keamanan aplikasi; dan
    b. bimbingan teknis mengenai standar keamanan SPBE.
(5) Anggaran keamanan SPBE sebagaimana dimaksud pada ayat (2) huruf b disusun berdasarkan perencanaan yang telah ditetapkan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 56

(1) Evaluasi kinerja sebagaimana dimaksud dalam Pasal 44 ayat (1) huruf e dilakukan oleh koordinator SPBE.
(2) Evaluasi kinerja sebagaimana dimaksud pada ayat (1) dilakukan terhadap pelaksanaan keamanan SPBE;
(3) Evaluasi kinerja sebagaimana dimaksud pada ayat (2) dilaksanakan dengan:
    a. mengidentifikasi area proses yang memiliki risiko tinggi terhadap keberhasilan pelaksanaan keamanan SPBE;
    b. menetapkan indikator kinerja pada setiap area proses;
    c. memformulasi pelaksanaan keamanan SPBE dengan mengukur kuantitatif kinerja yang diharapkan;
    d. menganalisis efektifitas pelaksanaan keamanan SPBE; dan
    e. mendukung dan merealisasikan program audit keamanan SPBE.
(4) Evaluasi kinerja sebagaimana dimaksud pada ayat (1) dilaksanakan paling sedikit 1 (satu) tahun.

Pasal 57

(1) Perbaikan berkelanjutan sebagaimana dimaksud dalam Pasal 44 ayat (1) huruf f dilakukan oleh pelaksana teknis keamanan SPBE.
(2) Perbaikan berkelanjutan sebagaimana dimaksud pada ayat (1) merupakan tindak lanjut dari hasil evaluasi kinerja.
(3) Perbaikan berkelanjutan sebagaimana dimaksud pada ayat (1) dilakukan dengan:
    a. Mengatasi permasalahan dalam pelaksanaan keamanan SPBE; dan
    b. Memperbaiki pelaksanaan keamanan SPBE secara periodik.

Bagian Keenam

Standar Teknis dan Prosedur Keamanan SPBE

Pasal 58

(1) Setiap Pemerintah Daerah harus menerapkan Keamanan SPBE
(2) Penerapan Keamanan SPBE sebagaimana dimaksud pada ayat (1) harus memenuhi standar teknis dan prosedur keamanan SPBE.

Pasal 59

Standar teknis dan prosedur Keamanan SPBE sebagaimana dimaksud dalam Pasal 58 ayat (2) diterapkan untuk:

a. keamanan data dan informasi;
b. keamanan Aplikasi SPBE;
c. keamanan Sistem Penghubung Layanan;
d. keamanan Jaringan Intra; dan
e. keamanan Pusat Data Nasional;

Pasal 60

Standar teknis keamanan data dan informasi sebagaimana dimaksud dalam Pasal 59 huruf a terdiri atas terpenuhinya aspek:

a. kerahasiaan;
b. keaslian;
c. keutuhan;
d. kenirsangkalan; dan
e. ketersediaan;

Pasal 61

(1) Terpenuhinya aspek kerahasiaan sebagaimana dimaksud dalam Pasal 60 huruf a dilakukan dengan prosedur:
    a. menetapkan klasifikasi informasi;
    b. menerapkan enkripsi dengan sistem kriptografi; dan menerapkan pembatasan akses terhadap data dan informasi sesuai dengan kewenangan dan kebijakan yang telah ditetapkan.
(2) Terpenuhinya aspek keaslian sebagaimana dimaksud dalam Pasal 60 huruf b dilakukan dengan prosedur:
    a. menyediakan mekanisme verifikasi;
    b. menyedianakan mekanisme validasi; dan
    c. menerapkan sistem *hash function*;
(3) Terpenuhinya aspek keutuhan sebagaimana dimaksud dalam Pasal 60 huruf c dilakukan dengan prosedur:
    a. menerapkan pendeteksian modifikasi; dan
    b. menerapkan tanda tangan elektronik tersertifikasi.
(4) Terpenuhinya aspek kenirsangkalan sebagaimana dimaksud dalam Pasal 60 huruf d dilakukan dengan prosedur:
    a. menerapkan tanda tangan elektronik tersertifikasi;

b. penjaminan oleh penyelenggara sertifikasi elektronik melalui sertifikat elektronik.

(5) Terpenuhinya aspek ketersediaan sebagaimana dimaksud dalam Pasal 60 huruf e dilakukan dengan prosedur:

a. menerapkan sistem pencadangan secara berkala;
b. membuat perencanaan untuk menjamin data dan informasi dapat selalu diakses; dan
c. menerapkan sistem pemulihan.

Pasal 62

(1) Standar teknis dan prosedur keamanan Aplikasi SPBE sebagaimana dimaksud dalam Pasal 59 huruf b diterapkan pada:

a. aplikasi berbasis web; dan
b. aplikasi berbasis *mobile.*

(2) Aplikasi berbasis web sebagaimana dimaksud pada ayat (1) huruf a merupakan aplikasi yang diakses melalui peramban saat terhubung dengan koneksi internet atau intranet.

(3) Aplikasi berbasis *mobile* sebagaimana dimaksud pada ayat (1) huruf b merupakan aplikasi yang dalam pengoperasiannya dapat berjalan di perangkat bergerak dan memiliki sistem operasi yang mendukung perangkat lunak secara *standalone.*

(4) Aplikasi SPBE sebagaimana dimaksud pada ayat (1) harus dilakukan pengujian keamanan setiap periode tertentu yang dilakukan dengan:

a. mengidentifikasi persyaratan minimum keamanan yang belum diterapkan;
b. memastikan pengkodean pemrograman aplikasi yang dibuat tidak memiliki kerawanan;
c. melakukan pemindaian otomatis dan/atau pengujian penetrasi sistem;
d. mengidentifikasi kerentanan dan mengelola ancaman sejak awal siklus pengembangan Aplikasi SPBE; dan
e. menganalisis kerentanan.

Pasal 63

Standar teknis keamanan aplikasi berbasis web sebagaimana dimaksud dalam Pasal 62 ayat (1) huruf a terdiri atas terpenuhi fungsi:

a. autentikasi;
b. manajemen sesi;

c. persyaratan kontrol akses;
d. validasi input;
e. kriptografi dan verifikasi statis;
f. penanganan *error* dan pencatatan *log*;
g. proteksi data;
h. keamanan komunkasi
i. pengendalian kode berbahaya;
j. logika bisnis;
k. *file*;
l. keamanan API dan *web service*; dan
m. keamanan konfigurasi.

Pasal 64

(1) Terpenuhinya fungsi autentikasi sebagaimana dimaksud dalam Pasal 63 huruf a dilakukan dengan prosedur:
   a. menggunakan manajemen kata sandi untuk proses autentikasi;
   b. menerapkan verifikasi kata sandi pada sisi *server*;
   c. mengatur jumlah karakter, kombinasi jenis karakter dan masa berlaku dari kata sandi;
   d. mengatur jumlah maksimum kesalahan dalam pemasukan kata sandi;
   e. mengatur mekanisme pemulihan kata sandi;
   f. menjaga kerahasiaan kata sandi yang disimpan melalui mekanisme kriptografi; dan
   g. menggunakan jalur komunikasi yang diamankan untuk proses autentikasi.

(2) Terpenuhinya fungsi manajemen sesi sebagaimana dimaksud dalam Pasal 63 huruf b dilakukan dengan prosedur:
   a. menggunakan pengendali sesi untuk proses manajemen sesi;
   b. menggunakan pengendali sesi yang disediakan oleh kerangka kerja aplikasi;
   c. mengatur pembuatan dan keacakan token sesi yang dihasilkan oleh pengendali sesi;
   d. mengatur kondisi dan jangka waktu habis sesi;
   e. validasi dan pencantuman *session id*;
   f. pelindungan terhadap lokasi dan pengiriman token untuk sesi terautentikasi ; dan
   g. pelindungan terhadap duplikasi dan mekanisme persetujuan pengguna;

(3) Terpenuhinya fungsi persyaratan kontrol akses sebagaimana dimaksud dalam Pasal 63 huruf c dilakukan dengan prosedur:
   a. menetapkan otorisasi pengguna untuk membatasi kontrol akses;
   b. mengatur peringatan terhadap bahaya serangan otomatis apabila terjadi akses yang bersamaan atau akses yang terus menerus pada fungsi;
   c. mengatur antarmuka pada sisi administrator; dan
   d. mengatur verifikasi kebenaran token ketika mengakses data dan informasi yang dikecualikan.

(4) Terpenuhinya fungsi validasi input sebagaimana dimaksud dalam Pasal 63 huruf d dilakukan dengan prosedur:
   a. menerapkan fungsi validasi input pada sisi *server*;
   b. menerapkan mekanisme penolakan input jika terjadi kesalahan validasi;
   c. memastikan *runtime environment* aplikasi tidak rentan terhadap serangan validasi input;
   d. melakukan validasi positif pada seluruh input;
   e. melakukan filter terhadap data yang tidak dipercaya;
   f. menggunakan fitur kode dinamis;
   g. melakukan pelindungan terhadap akses yang mengandung konten skrip; dan
   h. melakukan pelindungan dari serangan injeksi basis data.

(5) Terpenuhinya fungsi kriptografi pada verifikasi statis sebagaimana dimaksud dalam Pasal 63 huruf e dilakukan dengan prosedur:
   a. menggunakan algoritma kriptografi, modul kriptografi, protokol kriptografi dan kunci kriptografi sesuai dengan ketentuan peraturan perundang-undangan;
   b. melakukan autentikasi data yang dienkripsi;
   c. menerapkan manajemen kunci kriptografi; dan
   d. membuat angka acak yang menggunakan generator angka acak kriptografi.

(6) Terpenuhinya fungsi penanganan *error* dan pencatatan *log* sebagaimana dimaksud dalam Pasal 63 huruf f dilakukan dengan prosedur:
   a. mengatur konten pesan yang ditampilkan ketika terjadi kesalahan;
   b. menggunakan metode penanganan *error* untuk mencegah kesalahan terprediksi dan tidak terduga serta menangani seluruh pengecualian yang tidak ditangani;
   c. tidak mencantumkan informasi yang dikecualikan dalam pencatatan *log*;

d. mengatur cakupan *log* yang dicatat untuk mendukung upaya penyelidikan ketika terjadi insiden;
e. mengatur pelindungan *log* aplikasi dari akses dan modifikasi yang tidak sah;
f. melakukan enkripsi pada data yang disimpan untuk mencegah injeksi *log*; dan
g. melakukan singkronisasi sumber waktu sumber waktu sesuai dengan zona waktu dan waktu yang benar.

(7) Terpenuhinya fungsi proteksi data sebagaimana dimaksud dalam Pasal 63 huruf g dilakukan dengan prosedur:
a. melakukan identifikasi dan penyimpanan salinan informasi yang dikecualikan;
b. melakukan pelindungan dari akses yang tidak sah terhadap informasi yang dikecualikan yang disimpan sementara dalam aplikasi;
c. melakukan pertukaran, penghapusan dan audit informasi dalam aplikasi;
d. melakukan penentuan jumlah parameter;
e. memastikan data disimpan dengan aman;
f. menentukan metode untuk menghapus dan mengekspor data sesuai permintaan pengguna; dan
g. membersihkan memori setelah tidak diperlukan.

(8) Terpenuhinya fungsi keamanan komunikasi sebagaimana dimaksud dalam Pasal 63 huruf h dilakukan dengan prosedur:
a. menggunakan komunikasi terenkripsi;
b. mengatur koneksi masuk dan keluar yang aman dan terenkripsi dari sisi pengguna;
c. mengatur jenis algoritma yang digunakan dan alat pengujiannya; dan
d. mengatur aktivasi dan konfigurasi sertifikat elektronik yang diterbitkan oleh penyelenggara sertifikasi elektronik.

(9) Terpenuhinya fungsi pengendalian kode berbahaya sebagaimana dimaksud dalam Pasal 63 huruf i dilakukan dengan prosedur:
a. menggunakan analisis kode dalam kontrol kode berbahaya;
b. memastikan kode sumber apliaksi dan pustaka tidak mengandung kode berbahaya dan fungsionalitas lain yang tidak diizinkan;
c. mengatur izin terkait fitur atau sensor terkait privasi;
d. mengatur pelindungan integritas; dan
e. mengatur mekanisme fitur pembaruan.

(10) Terpenuhinya fungsi logika bisnis sebagaimana dimaksud dalam Pasal 63 huruf j dilakukan dengan prosedur:

a. memproses alur logika bisnis dalam urutan langkah dan waktu yang realistis;
b. memastikan logika bisnis memiliki batasan dan validasi;
c. memonitor aktivitas yang tidak biasa;
d. membantu dalam kontrol antiotomatisasi; dan
e. memberikan peringatan ketika terjadi serangan otomatis atau aktivitas yang tidak biasa.

(11) Terpenuhinya fungsi *file* sebagaimana dimaksud dalam Pasal 63 huruf k dilakukan dengan prosedur:

a. mengatur jumlah *file* untuk setiap pengguna dan kuota ukuran *file* yang diunggah;
b. melakukan validasi *file* sesuai dengan tipe konten yang diharapkan;
c. melakukan pelindungan terhadap metadata input dan metadata *file*;
d. melakukan pemindaian *file* yang diperoleh dari sumber yang tidak dipercaya; dan
e. melakukan konfigurasi *server* untuk mengunduh *file* sesuai ekstensi yang ditentukan.

(12) Terpenuhinya fungsi keamana API dan web service sebagaimana dimaksud dalam Pasal 63 huruf l dilakukan dengan prosedur:

a. melakukan konfigurasi layanan web;
b. memverifikasi *uniform resource identifier* API yang tidak menampilkan informasi yang berpotensi sebagai celah keamanan;
c. membuat keputusan otorisasi;
d. menampilkan metode RESTful *hypertext transfer protocol* apabila input pengguna dinyatakan valid;
e. menggunakan validasi skema dan verifikasi sebelum menerima input;
f. menggunakan metode pelindungan layanan berbasis web; dan
g. menerapkan kontrol antiotomatisasi.

(13) Terpenuhinya fungsi keamanan konfigurasi sebagaimana dimaksud dalam Pasal 63 huruf m dilakukan dengan prosedur:

a. mengkonfigurasi *server* sesuai rekomendasi *server* aplikasi dan kerangka kerja aplikasi yang digunakan;
b. mendokumentasi, menyalin konfigurasi dan semua dependensi;
c. menghapus fitur, dokumentasi, sampel dan konfigurasi yang tidak diperlukan;

d. memvalidasi integritas *asset* jika *asset* aplikasi diakses secara eksternal;
e. menggunakan respons aplikasi dan konten yang aman.

Pasal 65

Standar teknis keamanan aplikasi berbasis *mobile* sebagaimana dimaksud dalam Pasal 62 ayat (1) huruf b terdiri atas terpenuhinya fungsi:

a. penyimpanan data dan persyaratan privasi;
b. kriptografi;
c. autentikasi dan manajemen sesi;
d. komunikasi jaringan;
e. interaksi platform;
f. kualitas kode dan pengaturan *build*; dan
g. ketahanan.

Pasal 66

(1) Terpenuhinya fungsi penyimpanan data dan persyaratan privasi sebagaimana dimaksud dalam Pasal 65 huruf a dilakukan dengan prosedur:
   a. menyimpan seluruh data dan informasi yang dikecualikan hanya dalam fasilitas penyimpanan kredensial sistem;
   b. membatasi pertukaran data dan informasi yang dikecualikan dengan *third party*;
   c. menonaktifkan *cache keyboard* pada saat memasukkan data dan informasi yang dikecualikan saat terjadi *inter process communication*; dan
   d. melindungi data dan informasi yang dikecualikan yang dimasukkan melalui antarmuka pengguna.
(2) Terpenuhinya fungsi kriptografi sebagaimana dimaksud dalam Pasal 65 huruf b dilakukan dengan prosedur:
   a. menghindari penggunaan kriptografi simetrik dengan *hardcoded key*;
   b. mengimplementasikan metode kriptografi yang sudah teruji sesuai kebutuhan;
   c. menghindari penggunaan protokol kriptografi atau algoritma kriptografi yang obsolet;
   d. menghindari penggunaan kunci kriptografi yang sama; dan
   e. menggunakan pembangkit kunci acak yang memenuhi kriteria keacakan kunci;

(3) Terpenuhinya fungsi autentikasi dan manajemen sesi sebagaimana dimaksud dalam Pasal 65 huruf c dilakukan dengan prosedur:
   a. menerapkan autentikasi pada *remote endpoint* terhadap aplikasi yang menyediakan akses pengguna untuk layanan jarak jauh;
   b. menggunakan *session identifier* yang acak tanpa perlu mengirimkan kredensial pengguna apabila menggunakan *stateful* manajemen sesi;
   c. memastikan *server* menyediakan token yang telah ditandatangani menggunakan algoritma yang aman apabila menggunakan autentikasi berbasis token;
   d. memastikan *remote endpoint* memutus sesi yang ada saat pengguna *log out*;
   e. menerapkan pengaturan sandi pada *remote endpoint*;
   f. membatasi jumlah percobaan *log in* pada *remote endpoint*;
   g. menentukan masa berlaku sesi dan masa kadaluwarsa token pada *remote endpoint*; dan
   h. melakukan otorisasi pada *remote endpoint*.

(4) Terpenuhinya fungsi komunikasi jaringan sebagaimana dimaksud dalam Pasal 65 huruf d dilakukan dengan prosedur:
   a. Menerapkan *secure socket layer* atau *transport layer security* yang tidak obsolet secara konsisten; dan
   b. Memverifikasi sertifikat *remote endpoint*.

(5) Terpenuhinya fungsi interaksi platform sebagaimana dimaksud dalam Pasal 65 huruf e dilakukan dengan prosedur:
   a. memastikan aplikasi hanya meminta akses terhadap sumber daya yang diperlukan;
   b. melakukan validasi terhadap seluruh input dari sumber eksternal dan pengguna;
   c. menghindari pengiriman fungsionalitas sensitif melalui skema *custom uniform resource locator* dan fasilitas *inter process communication*;
   d. menghindari penggunaan *Javascript* dalam *WebView*;
   e. menggunakan protokol *hypertext transfer protocol secure* pada *WebView*; dan
   f. mengimplementasikan penggunaan serialisasi API yang aman.

(6) Terpenuhinya fungsi kualitas kode dan pengaturan *build* sebagaimana dimaksud dalam Pasal 65 huruf f dilakukan dengan prosedur:
   a. menandatangani aplikasi dengan sertifikat yang valid;
   b. memastikan aplikasi dalam mode rilis;

c. menghapus simbol *debugging* dari *native binary*;
d. menghapus kode *debugging* dan kode bantuan pengembang;
e. mengidentifikasi kelemahan seluruh komponen *third party*;
f. menentukan mekanisme penanganan *error*;
g. mengelola memori secara aman;
h. mengaktifkan fitur keamanan yang tersedia.

(7) Terpenuhinya fungsi ketahanan sebagaimana dimaksud dalam pasal 65 huruf g dilakukan dengan prosedur:
a. mencegah aplikasi berjalan pada perangkat yang telah dilakukan modifikasi yang tidak sah;
b. mendeteksi dan merespons *debugger*;
c. mencegah *executable file* melakukan perubahan pada sumber daya perangkat;
d. mendeteksi dan merespons keberadaan perangkat *reverse engineering*;
e. mencegah aplikasi berjalan dalam emulator;
f. mendeteksi perubahan kode dan data di ruang memori;
g. menerapkan fungsi *device binding* dengan menggunakan *property* unik pada perangkat;
h. melindungi seluruh *file* dan *library* pada aplikasi; dan
i. menerapkan metode *obfuscation*;

BAB IV
OPERASIONAL DUKUNGAN PERSANDIAN

Pasal 67

(1) Kegiatan operasional dukungan persandian merupakan kegiatan operasional yang tidak terkait dengan kriptografi namun mendukung terciptanya keamanan informasi, meliputi hal-hal sebagai berikut:
a. PENTEST;
b. Kontra Penginderaan;
c. *Assessment* keamanan sistem informasi;
d. SOC; dan
e. kegiatan Pengamanan Informasi lainnya.

(2) Penyelenggara persandian daerah bertindak sebagai koordinator dalam pelaksanaan kegiatan operasional dukungan persandian sesuai dengan kewenangannya.

Pasal 68

(1) PENTEST sebagaimana dimaksud dalam Pasal 67 pada ayat (1) huruf a merupakan kegiatan yang dilakukan untuk mencegah serangan pada aplikasi/sistem informasi milik instansi di lingkungan Pemerintah Kabupaten Landak.

(2) PENTEST sebagaimana dimaksud pada ayat (1) dilaksanakan sebelum aplikasi/sistem informasi diterapkan.

(3) Aplikasi/Sistem Informasi milik instansi di lingkungan Pemerintah Kabupaten Landak dilakukan tinjauan sekurang-kurangnya pada paruh waktu dan akhir tahun penerapan atau sewaktu-waktu sesuai kebutuhan.

(4) Laporan hasil PENTEST digunakan sebagai dasar bagi pengelola aplikasi/sistem informasi untuk memperbaiki tingkat keamanan aplikasi/sistem informasi.

Pasal 69

(1) Kontra Penginderaan sebagaimana dimaksud dalam Pasal 67 pada ayat (1) huruf b merupakan kegiatan bersifat terbatas yang dilakukan untuk mencegah adanya pengawasan dari pihak yang tidak berhak terhadap informasi berklasifikasi.

(2) Kontra Penginderaan sebagaimana dimaksud pada ayat (1) dilakukan melalui:
   a. pemeriksaan fisik ruangan dengan memperhatikan barang di dalam ruangan yang berpotensi menjadi peralatan *surveillance*; dan
   b. dilaksanakan di tempat pengolahan informasi berklasifikasi serta ruang yang sering digunakan pimpinan.

(3) Kontra Penginderaan sebagaimana dimaksud pada ayat (1) dilaksanakan secara berkala sekurang-kurangnya 1 (satu) kali dalam 1 (satu) tahun.

(4) Laporan hasil Kontra Penginderaan merupakan informasi berklasifikasi.

Pasal 70

(1) Kegiatan *assessment* keamanan sistem informasi sebagaimana dimaksud dalam Pasal 67 ayat (1) huruf c, untuk mengukur tingkat kerawanan dan keamanan sistem informasi.

(2) Kegiatan *assessment* sebagaimana dimaksud pada ayat (1) dilaksanakan secara berkala sekurang-kurangnya satu kali dalam 1 (satu) tahun, atau jika terjadi pembaharuan/perubahan/peningkatan/perbaikan pada sistem informasi di lingkungan Pemerintah Daerah.

(3) Laporan hasil kegiatan *assessment* merupakan informasi berklasifikasi dan dapat digunakan sebagai dasar untuk melakukan pengembangan sistem informasi.

Pasal 71

(1) SOC sebagaimana dimaksud dalam Pasal 67 ayat (1) huruf d merupakan suatu infrastruktur terpusat untuk melaksanakan kegiatan Pengamanan Informasi dengan melakukan proses pengawasan, pelindungan dan penanggulangan insiden keamanan informasi dengan memperhatikan aspek personil proses pelaksanaan dan ketersediaan teknologi.
(2) Penyelenggara SOC sebagaimana dimaksud pada ayat (1) kabupaten harus berkolaborasi dengan *Network Operation Center* (NOC) setempat.
(3) SOC yang diselenggarakan Pemerintah Daerah kabupaten dibangun secara terpusat dan terhubung dengan BSSN agar kegiatan berlangsung secara *responsive*.

Pasal 72

(1) Kegiatan Pengamanan Informasi lainnya sebagaimana dimaksud dalam Pasal 67 ayat (1) huruf e merupakan kegiatan yang dilaksanakan untuk mendukung pengamanan informasi.
(2) Untuk menyelenggarakan kegiatan Pengamanan Informasi lainnya, sebagaimana dimaksud pada ayat (1) wajib melalui persetujuan serendah-rendahnya Eselon 2 (dua) pada penyelenggara persandian.

BAB V
PEMANTAUAN, EVALUASI DAN PELAPORAN

Pasal 73

(1) Pemantauan dan evaluasi dimaksudkan untuk memantau, mengidentifikasi hambatan dan upaya perbaikan dalam penyelenggaraan persandian untuk Pengamanan Informasi.
(2) Pemantauan dan evaluasi sebagaimana dimaksud pada ayat (1) terhadap penyelenggaraan persandian dilaksanakan oleh Pemerintah Daerah meliputi:
    a. pemantauan dan evaluasi yang bersifat rutin dan insidentil; dan
    b. pemantauan dan evaluasi yang bersifat tahunan.
(3) Pengawasan dan evaluasi yang bersifat rutin dan insidentil sebagaimana dimaksud pada ayat (2) huruf a berupa:

a. pemantauan penggunaan matsan, aplikasi sandi dan/atau fasilitas layanan Persandian lainnya di lingkungan Pemerintah Daerah; dan
b. melaksanakan kebijakan manajemen risiko penyelenggaraan persandian di lingkungan Pemerintah Daerah.

(4) Pemantauan dan evaluasi yang bersifat tahunan sebagaimana dimaksud pada ayat (2) huruf b berupa:
a. pengukuran tingkat pemanfaatan layanan persandian oleh perangkat daerah;
b. penilaian mandiri (*self assessment*) terhadap penyelenggaraan persandian pada Pemerintah Daerah;
c. pengukuran tingkat kepuasan perangkat daerah terhadap layanan persandian yang dikelola oleh Dinas; dan
d. penyusunan Laporan Penyelenggaraan Persandian Tahunan (LP2T) Pemerintah Daerah.

Pasal 74

Pemantauan penggunaan matsan, aplikasi sandi dan/atau fasilitas layanan persandian lainnya sebagaimana dimaksud dalam Pasal 73 ayat (3) huruf a dilaksanakan dengan memperhatikan ketentuan sebagai berikut:
a. dilakukan terhadap seluruh matsan, aplikasi sandi dan/atau fasilitas layanan persandian lainnya yang dimanfaatkan oleh pengelola persandian;
b. kewenangan pelaksanaan kegiatan ada pada perangkat persandian daerah;
c. dilakukan paling sedikit satu (1) kali selama 3 (tiga) bulan dengan memperhatikan tingkat risiko pemanfaatan matsan, aplikasi sandi dan/atau fasilitas layanan persandian lainnya; dan
d. hasil kegiatan dapat digunakan sebagai data dukung dalam melakukan evaluasi pemanfaatan layanan persandian oleh Pemerintah Daerah.

Pasal 75

Pelaksanaan kebijakan manajemen risiko sebagaimana dimaksud dalam Pasal 73 ayat (3) huruf b dilaksanakan dengan memperhatikan ketentuan sebagai berikut:
a. dilaksanakan sesuai kebijakan manajemen risiko yang ditetapkan oleh BSSN; dan
b. penyelenggara persandian memiliki peran mengoordinasikan pelaksanaan kebijakan manajemen risiko penyelenggaraan persandian oleh penyelenggara persandian kabupaten.

Pasal 76

Pengukuran tingkat pemanfaatan layanan persandian sebagaimana dimaksud dalam Pasal 73 ayat (4) huruf a dilaksanakan dengan memperhatikan ketentuan sebagai berikut:

a. objek yang diukur adalah jumlah Pemerintah Daerah yang memanfaatkan analisis kebutuhan, jumlah Pemerintah Daerah yang melaksanakan pengelolaan dan pelindungan informasi dan jumlah Pemerintah Daerah yang memanfaatkan layanan penyelenggaraan operasional dukungan persandian untuk Pengamanan Informasi;
b. pengukuran dilakukan dengan menghitung persentase objek sesuai dengan huruf a dengan jumlah seluruh Pemerintah Daerah yang ada;
c. kewenangan pelaksanaan ada pada penyelenggara persandian kabupaten; dan
d. laporan hasil pengukuran digunakan untuk evaluasi internal dan dapat dijadikan bahan untuk laporan ke BSSN.

Pasal 77

Penilaian mandiri sebagaimana dimaksud dalam Pasal 73 pada ayat (4) huruf b dilaksanakan dengan memperhatikan ketentuan sebagai berikut:

a. objek yang diukur adalah aspek penyelenggaraan persandian dan dilaksanakan menggunakan instrumen pengukuran penyelenggaraan persandian yang telah ditetapkan oleh BSSN;
b. dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan;
c. kewenangan pelaksanaan ada pada penyelenggara persandian kabupaten; dan
d. laporan hasil penilaian digunakan untuk peningkatan penyelenggaraan persandian di lingkungan Pemerintah Daerah.

Pasal 78

Pengukuran tingkat kepuasan Perangkat Daerah sebagaimana dimaksud dalam Pasal 73 ayat (4) huruf c dilaksanakan dengan memperhatikan ketentuan sebagai berikut:

a. objek yang diukur adalah tingkat kepuasan pengguna persandian terhadap layanan persandian yang dikelola oleh penyelenggara persandian;
b. kewenangan pelaksanaan ada pada penyelenggara persandian;
c. dilakukan dengan metode pengisian kuesioner dan/atau wawancara langsung terhadap pengguna persandian daerah menggunakan instrumen

pengukuran tingkat kepuasan yang ditetapkan oleh penyelenggara persandian setelah berkonsultasi dengan BSSN; dan

d. laporan hasil pengukuran digunakan untuk peningkatan penyelenggaraan persandian.

Pasal 79

Penyusunan Laporan Penyelenggaraan Persandian Tahunan (LP2T) sebagaimana dimaksud dalam Pasal 73 pada ayat (4) huruf d dilaksanakan dengan memperhatikan ketentuan sebagai berikut:

a. objek yang dilaporkan adalah hasil pelaksanaan kebijakan, program dan kegiatan teknis Pemerintah Daerah termasuk hasil kegiatan pengawasan dan evaluasi yang menggambarkan hasil penyelenggaraan urusan pemerintahan di bidang Persandian selama satu tahun;
b. kewenangan pelaksanaan ada pada penyelenggara persandian; dan
c. penyelenggara persandian menyampaikan LP2T kepada BSSN melalui Bupati.

Pasal 80

Pemantauan, evaluasi dan pelaporan terhadap penyelenggaraan persandian untuk Pengamanan Informasi Pemerintah Daerah kabupaten dan penetapan pola hubungan komunikasi sandi antar daerah kabupaten dilakukan sesuai dengan ketentuan peraturan perundang-undangan.

BAB VI

KOORDINASI DAN KONSULTASI

Pasal 81

(1) Dalam rangka pelaksanaan urusan pemerintahan bidang persandian, penyelenggara persandian dapat melaksanakan koordinasi dan/atau konsultasi ke BSSN, Pemerintah Daerah terkait maupun antar pemerintah provinsi dan kabupaten/kota lainnya.
(2) Koordinasi dan konsultasi sebagaimana dimaksud pada ayat (1) dapat dilaksanakan dengan cara melakukan kunjungan langsung di lapangan (*on site*) dan/atau menggunakan media komunikasi lainnya.

BAB VII

PEMBIAYAAN

Pasal 82

Pendanaan pelaksanaan penyelenggaraan persandian untuk pengamanan informasi Pemerintah Daerah dan penetapan pola hubungan komunikasi sandi antar perangkat daerah bersumber dari:

a. Anggaran Pendapatan dan Belanja Daerah Kabupaten; dan/atau
b. sumber lain yang sah dan tidak mengikat sesuai dengan ketentuan peraturan perundang-undangan.

BAB VIII

PENUTUP

Pasal 83

Peraturan Bupati ini mulai berlaku pada tanggal diundangkan.

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

Ditetapkan di Ngabang
pada tanggal 22 juni 2023

Pj. BUPATI LANDAK,

TTD

SAMUEL

Diundangkan di Ngabang
pada tanggal 22 juni 2023
SEKRETARIS DAERAH KABUPATEN LANDAK,

TTD

VINSENSIUS

Salinan sesuai dengan aslinya
KEPALA BAGIAN HUKUM,

DARIANUARTI, SH
NIP. 19661128 199402 2 001

BERITA DAERAH KABUPATEN LANDAK TAHUN 2023 NOMOR 24