SALINAN

BUPATI HULU SUNGAI SELATAN
PROVINSI KALIMANTAN SELATAN

PERATURAN BUPATI HULU SUNGAI SELATAN

NOMOR 10 TAHUN 2022

TENTANG

PELAKSANAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI

DENGAN RAHMAT TUHAN YANG MAHA ESA

BUPATI HULU SUNGAI SELATAN,

Menimbang:

a. bahwa Pemerintah Daerah wajib mengelola Informasi yang dimilikinya dan untuk melindungi Informasi perlu dilakukan upaya pengamanan Informasi melalui penyelenggaraan persandian;

b. bahwa berdasarkan ketentuan Pasal 12 ayat (2) huruf o Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah 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, penyelenggaraan persandian untuk pengamanan Informasi Pemerintah Daerah Kabupaten merupakan Urusan Pemerintahan Wajib yang tidak berkaitan dengan pelayanan dasar yang menjadi kewenangan Pemerintah Daerah Kabupaten;

c. bahwa berdasarkan ketentuan Pasal 4 ayat (2) Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian untuk Pengamanan Informasi di Pemerintah Daerah, Bupati bertanggung jawab terhadap pelaksanaan persandian untuk pengamanan informasi, untuk itu perlu adanya pedoman pelaksanaan pengamanan informasi;

d. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b, dan huruf c, perlu menetapkan Peraturan Bupati tentang Pelaksanaan Persandian untuk Pengamanan Informasi;

Mengingat:

1. Undang-Undang Nomor 27 Tahun 1959 tentang Penetapan Undang-Undang Darurat Nomor 3 Tahun 1953 tentang Pembentukan Daerah Tingkat II di Kalimantan (Lembaran Negara Republik Indonesia Tahun 1953 Nomor 9) sebagai Undang-Undang (Lembaran Negara Republik Indonesia Tahun 1959 Nomor 72, Tambahan Lembaran Negara Republik Indonesia Nomor 1820);

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

Tahun 2016 Nomor 251, Tambahan Lembaran Negara Republik Indonesia Nomor 5952);

3. Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 61, Tambahan Lembaran Negara Republik Indonesia Nomor 4846);
4. Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik (Lembaran Negara Republik Indonesia Tahun 2009 Nomor 112, Tambahan Lembaran Negara Republik Indonesia Nomor 5038);
5. 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);
6. Peraturan Pemerintah Nomor 12 Tahun 2017 tentang Pembinaan dan Pengawasan Penyelenggaraan Pemerintah Daerah (Lembaran Negara Republik Indonesia Tahun 2017 Nomor 73, Tambahan Lembaran Negara Republik Indonesia Nomor 6041);
7. Undang-Undang Nomor 11 Tahun 2020 tentang Cipta Kerja (Lembaran Negara Republik Indonesia Tahun 2020 Nomor 245, Tambahan Lembaran Negara Republik Indonesia Nomor 6573);
8. Peraturan Pemerintah Nomor 18 Tahun 2016 tentang Perangkat Daerah (Lembaran Negara Republik Indonesia Tahun 2016 Nomor 114, Tambahan Lembaran Negara Republik Indonesia Nomor 5887) sebagaimana telah diubah dengan Peraturan Pemerintah Nomor 72 Tahun 2019 tentang Perubahan Atas Peraturan Pemerintah Nomor 18 Tahun 2016 tentang Perangkat Daerah (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 187, Tambahan Lembaran Negara Republik Indonesia Nomor 6402);
9. Peraturan Menteri Komunikasi dan Informatika Nomor 13 Tahun 2016 tentang Hasil Pemetaan Urusan Pemerintahan Daerah di Bidang Komunikasi dan Informatika (Berita Negara Republik Indonesia Tahun 2016 Nomor 1307);
10. Peraturan Menteri Komunikasi dan Informatika Nomor 14 Tahun 2016 tentang Pedoman Nomenklatur Perangkat Daerah Bidang Komunikasi dan Informatika (Berita Negara Republik Indonesia Tahun 2016 Nomor 1308);
11. Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik (Berita Negara Republik Indonesia Tahun 2016 Nomor 1829);
12. Peraturan Menteri Dalam Negeri Nomor 5 Tahun 2017 tentang Pedoman Nomenklatur Perangkat Daerah Provinsi dan Daerah Kabupaten/Kota yang Melaksanakan Fungsi Penunjang Penyelenggaraan Urusan Pemerintahan (Berita Negara Republik Indonesia Tahun 2017 Nomor 197);
13. Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian untuk Pengamanan Informasi di Pemerintah Daerah (Berita Negara Republik Indonesia Tahun 2019 Nomor 1054);

14. Peraturan Menteri Dalam Negeri Nomor 70 Tahun 2019 tentang Sistem Informasi Pemerintahan Daerah (Berita Negara Republik Indonesia Tahun 2019 Nomor 1114);
15. Peraturan Daerah Kabupaten Hulu Sungai Selatan Nomor 6 Tahun 2020 tentang Pembentukan dan Susunan Perangkat Daerah (Lembaran Daerah Kabupaten Hulu Sungai Selatan Tahun 2020 Nomor 6, Tambahan Lembaran Negara Republik Indonesia Nomor 3);

MEMUTUSKAN:

Menetapkan: PERATURAN BUPATI TENTANG PELAKSANAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI.

BAB I

KETENTUAN UMUM

Pasal 1

Dalam Peraturan Bupati ini yang dimaksud dengan:

1. Daerah adalah Kabupaten Hulu Sungai Selatan.
2. Pemerintah Daerah adalah Kepala Daerah sebagai unsur penyelenggara Pemerintahan Daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan Daerah otonom.
3. Kepala Daerah yang selanjutnya disebut Bupati adalah Bupati Hulu Sungai Selatan.
4. Perangkat Daerah adalah unsur pembantu Kepala Daerah dan Dewan Perwakilan Rakyat Daerah dalam penyelenggaraan Unsur Pemerintahan yang menjadi kewenangan Daerah.
5. Dinas Komunikasi dan Informatika Kabupaten Hulu Sungai Selatan yang selanjutnya disebut Dinas adalah Perangkat Daerah yang menyelenggarakan urusan di bidang komunikasi, informatika, statistik, dan persandian.
6. Badan Siber dan Sandi Negara yang selanjutnya disingkat BSSN adalah lembaga pemerintah yang menyelenggarakan tugas pemerintahan di bidang keamanan siber dan persandian.
7. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi Informasi dan komunikasi untuk memberikan layanan kepada pengguna SPBE.
8. Informasi adalah keterangan, pernyataan, gagasan, dan tanda-tanda yang mengandung nilai, makna, dan pesan baik data, fakta, maupun penjelasannya yang dapat dilihat, didengar, dan dibaca yang disajikan dalam berbagai kemasan dan format sesuai dengan perkembangan teknologi Informasi dan komunikasi secara elektronik ataupun non-elektronik.
9. 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.
10. Keamanan Informasi adalah terjaganya kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan Informasi.
11. Jaring Komunikasi Sandi adalah keterhubungan antar pengguna Persandian melalui jaring telekomunikasi.
12. Pengamanan Informasi adalah segala upaya, kegiatan, dan tindakan untuk mewujudkan Keamanan Informasi.
13. Informasi Berklasifikasi adalah informasi publik yang dikecualikan menurut peraturan perundang-undangan yang berlaku.

14. *Database* atau basis data adalah kumpulan data yang terorganisir, yang umumnya disimpan dan diakses secara elektronik dari suatu sistem komputer.
15. *Knowledge Repository* adalah aplikasi untuk menghimpun, menyimpan, dan menyebarkan informasi yang dihasilkan oleh suatu institusi.
16. Arsitektur Keamanan Informasi adalah struktur, aturan, komponen-komponen, hubungan antar komponen dan peta kontrol-kontrol keamanan yang diterapkan pada infrastruktur Teknologi Informasi di organisasi.
17. Pusat Data adalah suatu fasilitas yang digunakan untuk menempatkan sistem komputer dan komponen-komponen terkaitnya, seperti sistem telekomunikasi dan penyimpanan data
18. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi elektronik.
19. 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 Balai Sertifikasi Elektronik pada Badan Siber dan Sandi Negara) dan/atau lembaga penyelenggara Sertifikasi Elektronik dalam negeri yang telah diakui
20. Layanan Keamanan Informasi adalah keluaran dari pelaksanaan 1 (satu) atau beberapa kegiatan penyelenggaraan Urusan Pemerintahan bidang Persandian dan yang memiliki nilai manfaat.
21. Informasi Publik adalah Informasi yang dihasilkan, disimpan, dikelola, dikirim, dan/atau diterima oleh suatu badan publik yang berkaitan dengan penyelenggara dan penyelenggaraan negara dan/atau penyelenggara dan penyelenggaraan badan publik lainnya yang sesuai dengan peraturan perundang-undangan serta Informasi lain yang berkaitan dengan kepentingan publik.
22. Pengguna Layanan Keamanan Informasi yang selanjutnya disebut Pengguna Layanan adalah para pihak yang memanfaatkan Layanan Keamanan Informasi.
23. Dokumen Elektronik adalah setiap Informasi elektronik yang dibuat, diteruskan, dikirimkan, diterima atau disimpan dalam bentuk analog, digital, elektromagnetik, optik atau sejenisnya yang dapat dilihat, ditampilkan dan/atau didengar melalui komputer atau sistem elektronik, tetapi tidak terbatas pada tulisan, suara, gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, kode akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya.
24. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan Informasi seperti kerahasiaan data, keabsahan data, integritas data, serta otentikasi data.
25. Sumber Daya Manusia Teknologi Informasi Komunikasi adalah pegawai Perangkat Daerah yang memiliki tugas dan wewenang terkait dengan teknologi Informasi dan komunikasi.
26. Tanda Tangan Elektronik adalah tanda tangan yang terdiri atas Informasi elektronik yang dilekatkan, terasosiasi atau terkait dengan Informasi elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi.
27. Balai Sertifikasi Elektronik yang selanjutnya disebut BSrE merupakan unit pelaksana teknis penyelenggara Otoritas Sertifikat Digital Badan Siber dan Sandi Negara yang berada di bawah dan bertanggung jawab kepada Kepala Lembaga Sandi Negara.
28. Pola Hubungan Komunikasi Sandi adalah bentuk atau pola hubungan antara dua entitas atau lebih dalam proses pengiriman dan penerimaan Informasi/pesan/berita secara aman menggunakan persandian.

29. Kerahasiaan adalah penjaminan atas aset SPBE yang informasinya tidak tersedia atau diungkapkan kepada individu, entitas, atau proses yang tidak mempunyai hak untuk mengaksesnya.
30. Keutuhan adalah properti bahwa suatu aset SPBE akurat dan lengkap.
31. Ketersediaan adalah properti bahwa aset SPBE dapat diakses dan digunakan atas permintaan oleh entitas yang berwenang.
32. Keaslian adalah properti bahwa aset SPBE terkait merupakan entitas yang diklaimnya.
33. Kenirsangkalan adalah kemampuan untuk membuktikan terjadinya suatu peristiwa yang diklaim atau tindakan dan entitas asalnya.
34. Steganografi adalah seni dan ilmu menulis pesan tersembunyi atau menyembunyikan pesan dengan suatu cara sehingga selain si pengirim dan si penerima, tidak ada seorang pun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia.
35. Ruangan TEMPEST adalah ruang yang menggunakan standar TEMPEST yang mengamanatkan elemen seperti jarak peralatan dari dinding, jumlah pelindung di gedung dan peralatan, kabel pemisah jarak, filter pada kabel, jarak dan pelindung antara kabel atau peralatan, dan pencegahan kebocoran pancaran elektromagnetik yang juga mencakup suara dan getaran mekanis.

Pasal 2

Pelaksanaan Persandian untuk Pengamanan Informasi Pemerintah Daerah bertujuan untuk:

a. menciptakan harmonisasi dalam melaksanakan Persandian untuk Pengamanan Informasi di Pemerintah Daerah;
b. meningkatkan komitmen, efektivitas, dan kinerja Pemerintah Daerah dalam melaksanakan kebijakan, program, dan kegiatan pelaksanaan Persandian untuk Pengamanan Informasi; dan
c. memberikan pedoman bagi Pemerintah Daerah dalam menetapkan Pola Hubungan Komunikasi Sandi antar Perangkat Daerah.

Pasal 3

Pelaksanaan Persandian untuk Pengamanan Informasi Pemerintah Daerah sebagaimana dimaksud dalam Pasal 2 meliputi:

a. penyelenggaraan Persandian untuk Pengamanan Informasi Pemerintahan Daerah; dan
b. penetapan Pola Hubungan Komunikasi sandi antar Perangkat Daerah Kabupaten Hulu Sungai Selatan.

BAB II

PENYELENGGARAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI PEMERINTAH DAERAH

Bagian Kesatu

Umum

Pasal 4

(1) Penyelenggaraan Persandian untuk Pengamanan Informasi Pemerintah Daerah sebagaimana dimaksud dalam Pasal 3 huruf a dilaksanakan melalui:
    a. penyusunan kebijakan Pengamanan Informasi;
    b. pengelolaan sumber daya Keamanan Informasi;

c. pengamanan Sistem Elektronik dan Pengamanan Informasi non-elektronik; dan

d. penyediaan layanan Keamanan Informasi.

(2) Pelaksana penyelenggaraan Persandian untuk Pengamanan Informasi Pemerintah Daerah adalah Bupati dibantu oleh Dinas.

(3) Bupati bertanggung jawab terhadap penyelenggaraan Persandian untuk Pengamanan Informasi sebagaimana dimaksud pada ayat (1).

(4) Dinas bertanggung jawab atas kinerja pelaksanaan urusan pemerintahan bidang Persandian sesuai dengan tugas dan fungsinya.

Bagian Kedua

Penyusunan Kebijakan Pengamanan Informasi

Pasal 5

Penyusunan kebijakan Pengamanan Informasi sebagaimana dimaksud dalam Pasal 4 ayat (1) huruf a dilakukan dengan:

a. menyusun rencana strategis Pengamanan Informasi;

b. menetapkan Arsitektur Keamanan Informasi; dan

c. menetapkan aturan mengenai tata kelola Keamanan Informasi.

Pasal 6

(1) Bupati menyusun rencana strategis Pengamanan Informasi sebagaimana dimaksud dalam Pasal 5 huruf a.

(2) Penyusunan rencana strategis Pengamanan Informasi sebagaimana dimaksud pada ayat (1) dilakukan oleh Dinas.

(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 yang telah disusun sebagaimana dimaksud pada ayat (1) diintegrasikan ke dalam rencana pembangunan jangka menengah Daerah.

(5) Dalam melakukan penyusunan rencana strategis sebagaimana dimaksud pada ayat (1) Bupati dapat melakukan koordinasi dan konsultasi kepada BSSN.

(6) Dalam melakukan koordinasi dan konsultasi sebagaimana dimaksud pada ayat (5) Bupati dapat menugaskan kepala Dinas.

(7) Penugasan kepala Dinas sebagaimana dimaksud pada ayat (6) dapat dilaksanakan dengan telaahan staf/nota dinas/disposisi/surat perintah tugas.

Pasal 7

(1) Bupati menetapkan Arsitektur Keamanan Informasi sebagaimana dimaksud dalam Pasal 5 huruf b.

(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) Dalam melakukan penyusunan Arsitektur Keamanan Informasi sebagaimana dimaksud pada ayat (1) Bupati dapat melakukan koordinasi dan konsultasi kepada BSSN.

(4) Dalam melakukan koordinasi dan konsultasi sebagaimana dimaksud pada ayat (3) Bupati dapat menugaskan Dinas.

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

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

Pasal 8

(1) Tata kelola Keamanan Informasi 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.

(2) Dalam melakukan penyusunan aturan mengenai tata kelola Keamanan Informasi sebagaimana dimaksud pada ayat (1) Bupati dapat melakukan koordinasi dan konsultasi kepada BSSN.

(3) Dalam melakukan koordinasi dan konsultasi sebagaimana dimaksud pada ayat (3) Bupati dapat menugaskan kepala Dinas.

(4) Penugasan kepala Dinas sebagaimana dimaksud pada ayat (4) dapat dilaksanakan dengan telaahan staf/nota dinas/disposisi/surat perintah tugas.

Pasal 9

(1) Keamanan sumber daya teknologi Informasi sebagaimana dimaksud pada Pasal 8 ayat (2) huruf a meliputi:

a. aspek keamanan dan keberlangsungan sistem; dan

b. mekanisme dasar.

(2) Aspek keamanan dan keberlangsungan sistem sebagaimana dimaksud pada ayat (1) huruf a yang harus terpenuhi meliputi:

a. Kerahasiaan, akses terhadap data/Informasi dibatasi hanya bagi mereka yang punya otoritas;

b. Keutuhan, data tidak boleh diubah tanpa izin dari yang berhak;

c. Ketersediaan, untuk meyakinkan identitas pengguna sistem; dan

d. Keaslian, terkait dengan ketersediaan layanan, termasuk *up-time* dari sistem dan teknologi Informasi; dan

e. Kenirsangkalan, terkait penerapan tanda tangan digital dan jaminan pihak ketiga terpercaya melalui penggunaan sertifikat digital.

(3) Mekanisme dasar sebagaimana dimaksud pada ayat (1) huruf b untuk memastikan tercapainya aspek keamanan dan keberlangsungan sistem yang harus terpenuhi meliputi:

a. pengamanan dari sisi *software* aplikasi; dan

b. pengamanan dari sisi infrastruktur teknologi.

(4) Pengamanan dari sisi *software* aplikasi sebagaimana dimaksud pada ayat (3) huruf a dapat diimplementasikan melalui:

a. metode *scripting software* yang aman;

b. implementasi mekanisme otentikasi dan otorisasi di dalam *software* yang tepat; dan

c. pengaturan keamanan sistem basis data yang tepat.

(5) Pengamanan dari sisi infrastruktur teknologi sebagaimana dimaksud pada ayat (3) huruf b dapat diimplementasikan melalui:

a. *hardening* dari sisi sistem operasi;

b. *firewall*, sebagai pagar untuk menghadang ancaman dari luar sistem;

c. *Intrusion Detection System/ Intrusion-Prevention Systems* (IDS/IPS), sebagai pendeteksi atau pencegah aktivitas ancaman terhadap sistem;

d. *network monitoring tool*, sebagai usaha untuk melakukan monitoring atas aktivitas di dalam jaringan; dan

e. *log processor & analysis*, untuk melakukan pendeteksian dan analisis kegiatan yang terjadi di sistem.

(6) Dalam hal sumber daya teknologi Informasi dan komunikasi yang kritikal, pengamanan dapat ditempuh melalui penyediaan sistem cadangan yang dapat secara cepat mengambil alih sistem utama jika terjadi gangguan Ketersediaan (*availability*) pada sistem utama.

(7) Dalam hal evaluasi keamanan sumber daya teknologi Informasi, penilaian kerentanan keamanan sistem (*security vulnerability system*) dapat dilakukan secara teratur sesuai dengan kebutuhan.

Pasal 10

(1) Keamanan akses kontrol sebagaimana dimaksud pada Pasal 8 ayat (2) huruf b meliputi:

a. persyaratan organisasi untuk kendali akses;

b. manajemen akses pengguna;

c. tanggung jawab pengguna; dan

d. kendali akses sistem dan aplikasi.

(2) Persyaratan organisasi untuk kendali akses sebagaimana dimaksud pada ayat (1) huruf a meliputi:

a. kebijakan kendali akses, bahwa kebijakan kendali akses harus ditetapkan, didokumentasikan, dan ditinjau berdasarkan persyaratan organisasi dan keamanan Informasi; dan

b. akses ke jaringan dan layanan jaringan, bahwa pengguna hanya akan disediakan akses ke jaringan dan layanan jaringan yang telah secara khusus diberi wewenang untuk digunakan.

(3) Manajemen akses pengguna untuk kendali akses sebagaimana dimaksud pada ayat (1) huruf b meliputi:

a. registrasi dan pembatalan registrasi pengguna, bahwa proses registrasi dan pembatalan registrasi pengguna yang resmi harus diimplementasikan untuk mengaktifkan penetapan hak akses;

b. penyediaan akses pengguna, bahwa proses penyediaan akses pengguna yang resmi harus diimplementasikan untuk menetapkan atau mencabut hak akses untuk semua tipe pengguna ke semua sistem dan layanan;

c. penyediaan akses pengguna, bahwa proses penyediaan akses pengguna yang resmi harus diimplementasikan untuk menetapkan atau mencabut hak akses untuk semua tipe pengguna ke semua sistem dan layanan;

d. manajemen Informasi otentikasi rahasia dari pengguna, bahwa alokasi dari Informasi otentikasi rahasia harus dikendalikan melalui proses manajemen resmi;

e. peninjauan hak akses pengguna, bahwa pemilik aset harus meninjau hak akses pengguna secara periodik; dan

f. penghapusan atau penyesuaian hak akses, bahwa hak akses semua pegawai dan pengguna pihak eksternal pada Informasi dan fasilitas pengolahan Informasi harus dihapus sewaktu terjadi penghentian kepegawaian, kontrak, atau perjanjian, atau disesuaikan atas perubahan yang terjadi.

(4) Tanggung jawab pengguna sebagaimana dimaksud pada ayat (1) huruf c berkenaan dengan penggunaan Informasi otentikasi rahasia, bahwa pengguna harus mengikuti praktik organisasi dalam penggunaan Informasi otentikasi rahasia.

(5) Kendali akses sistem dan aplikasi sebagaimana dimaksud pada ayat (1) huruf d meliputi:

a. pembatasan akses Informasi, bahwa akses ke Informasi dan fungsi sistem aplikasi harus dibatasi sesuai dengan kebijakan kendali akses;

b. prosedur *login* yang aman, bahwa ketika disyaratkan oleh kebijakan pengendalian akses, akses ke sistem dan aplikasi harus dikendalikan oleh prosedur *login* yang aman;

c. sistem manajemen kata kunci, bahwa sistem manajemen kata kunci harus interaktif dan manajemen kualitas kata kunci;

d. penggunaan program utilitas istimewa, bahwa penggunaan program utilitas yang mungkin mampu membatalkan kendali sistem dan aplikasi harus dibatasi dan dikendalikan secara ketat; dan

e. kendali akses ke kode sumber program, bahwa akses ke kode sumber program harus dibatasi.

Pasal 11

(1) Keamanan data dan Informasi sebagaimana dimaksud pada Pasal 8 ayat (2) huruf c dilaksanakan melalui perlindungan Informasi berklasifikasi, mencakup:

a. perlindungan fisik, dilakukan untuk melindungi keberadaan dan fungsi sarana fisik komunikasi serta segala kegiatan yang berlangsung di dalamnya dari ancaman dan gangguan seperti pencurian, perusakan, dan radiasi gelombang elektromagnetik;

b. perlindungan administrasi, dilakukan untuk mencegah kelalaian dan tindakan indisipliner; dan

c. perlindungan logis, dilakukan dengan menggunakan teknik Kriptografi dan Steganografi untuk memenuhi aspek Kerahasiaan, Keutuhan, Keaslian, dan Kenirsangkalan.

(2) Perlindungan fisik sebagaimana dimaksud pada ayat (2) huruf a dilakukan melalui:

a. kendali akses ruang;

b. pemasangan teralis;

c. penggunaan kunci ganda;

d. pemasangan *closed-circuit television* (CCTV); dan/atau

e. penggunaan Ruangan *TEMPEST*.

(3) Perlindungan administrasi sebagaimana dimaksud pada ayat (1) huruf b dituangkan dalam bentuk peraturan tertulis yang menerangkan kebijakan, standar, dan prosedur operasional dalam Pengamanan Informasi Berklasifikasi.

(4) Perlindungan logis, sebagaimana dimaksud pada ayat (2) huruf c harus memenuhi standar dan direkomendasikan oleh BSSN.

Pasal 12

(1) Keamanan sumber daya manusia sebagaimana dimaksud pada Pasal 8 ayat (2) huruf d mencakup:

a. sumber daya manusia sebelum dipekerjakan;

b. sumber daya manusia selama bekerja; dan

c. sumber daya manusia saat penghentian dan perubahan kepegawaian.

(2) Keamanan sumber daya manusia sebelum dipekerjakan sebagaimana dimaksud pada ayat (1) huruf a dilaksanakan untuk memastikan bahwa Perangkat Daerah menyadari dan memenuhi tanggung jawab keamanan Informasi mereka, meliputi:

a. penyaringan, bahwa verifikasi latar belakang dari semua calon pegawai harus dilaksanakan berdasarkan peraturan perundang-undangan dan harus proporsional terhadap persyaratan Pemerintah Daerah, klasifikasi Informasi yang akan diakses dan risiko yang dipersepsikan; dan

b. syarat dan ketentuan kepegawaian, bahwa perjanjian tertulis dengan dan Pemerintah Daerah harus menyatakan tanggung jawab Keamanan Informasi.

(3) Keamanan sumber daya manusia selama bekerja sebagaimana dimaksud pada ayat (1) huruf b dilaksanakan untuk memastikan bahwa Perangkat Daerah menyadari dan memenuhi tanggung jawab Keamanan Informasi mereka, meliputi:

a. tanggung jawab manajemen;

b. kepedulian, pendidikan, dan pelatihan Keamanan Informasi; dan

c. proses pendisiplinan.

(4) Keamanan sumber daya manusia saat penghentian dan perubahan kepegawaian sebagaimana dimaksud pada ayat (1) huruf c dilaksanakan untuk melindungi kepentingan organisasi sebagai bagian dari proses pengubahan atau penghentian kepegawaian, dengan cara penghentian atau perubahan tanggung jawab kepegawaian.

Pasal 13

(1) Keamanan jaringan sebagaimana dimaksud pada Pasal 8 ayat (2) huruf e dilaksanakan untuk menjamin perlindungan Informasi dalam jaringan dan fasilitas pendukung pengolahan Informasi.

(2) Keamanan jaringan sebagaimana dimaksud pada Pasal 8 ayat (2) huruf e dilaksanakan melalui:

a. kendali jaringan, bahwa jaringan harus dikelola dan dikendalikan untuk melindungi Informasi dalam sistem dan aplikasi;

b. keamanan layanan jaringan, bahwa mekanisme jaringan, tingkat layanan dan persyaratan manajemen dari semua layanan jaringan harus diidentifikasi dan dimasukkan dalam perjanjian layanan jaringan; dan

c. pemisahan dalam jaringan, bahwa kelompok layanan Informasi, pengguna dan sistem Informasi harus dipisahkan pada jaringan.

Pasal 14

(1) Keamanan surat elektronik sebagaimana dimaksud pada Pasal 8 ayat (2) huruf f dilaksanakan melalui pemanfaatan layanan Sertifikat Elektronik.

(2) Proses pemanfaatan layanan Sertifikat Elektronik sebagaimana dimaksud pada ayat (1) dilakukan melalui:

a. pelaksanaan verifikasi identitas dan berkas untuk pendaftaran, pembaruan dan pencabutan Sertifikat Elektronik;

b. pengembangan aplikasi pendukung penggunaan Sertifikat Elektronik;

c. fasilitasi kegiatan sosialisasi dan bimbingan teknis terkait Sertifikat Elektronik; dan

d. pengawasan dan evaluasi penggunaan Sertifikat Elektronik.

(3) Pelaksanaan verifikasi identitas dan berkas untuk pendaftaran, pembaruan dan pencabutan Sertifikat Elektronik sebagaimana dimaksud pada ayat (2) huruf a, meliputi:

a. menangani verifikasi identitas berdasarkan identitas resmi, keanggotaan pada instansi, dan rekomendasi dari instansi;

b. menyetujui/menolak permintaan pendaftaran Sertifikat Elektronik;

c. menindaklanjuti permintaan Sertifikat Elektronik kepada BSrE;

d. menyampaikan Sertifikat Elektronik kepada pemohon; dan

e. melakukan pengarsipan berkas pendaftaran Sertifikat Elektronik berupa *hardcopy* dan *softcopy*.

Pasal 15

(1) Keamanan Pusat Data sebagaimana dimaksud pada Pasal 8 ayat (2) huruf g meliputi kontrol akses dan keamanan fisik dan logis.

(2) Kontrol akses dan keamanan fisik dan logis Pusat Data sebagaimana dimaksud pada ayat (1) wajib memenuhi persyaratan sebagai berikut:

a. memiliki pengaman fisik di setiap jendela yang memungkinkan akses langsung ke Pusat Data;

b. memastikan setiap sumber daya manusia di Pusat Data memiliki pengetahuan dan kesadaran yang cukup terhadap keamanan fisik Pusat Data;

c. melakukan pengamanan Pusat Data selama 24 (dua puluh empat) jam dengan jumlah petugas paling sedikit 2 (dua) orang per-*shift*;

d. memasang perangkat sistem pemantau visual yang berfungsi untuk memantau dan merekam setiap aktivitas pada ruang komputer, ruang mekanik dan kelistrikan, ruang telekomunikasi dan kawasan kantor;

e. menggunakan sistem akses elektronik dan sistem pengawasan (*surveillance*) yang dikendalikan dengan mekanisme otentikasi yang berfungsi untuk mencegah dan menanggulangi akses fisik tanpa izin terhadap fasilitas, peralatan dan sumber daya dalam ruang komputer;

f. memastikan setiap tamu/pengunjung memiliki izin dan dilengkapi dengan tanda masuk serta tanda pengenal untuk dapat masuk ke ruang komputer, ruang mekanikal dan kelistrikan, ruang telekomunikasi dan kawasan kantor;

g. melengkapi Pusat Data dengan sistem audit trail untuk pencatatan akses fisik dan akses logis yang terjadi;

h. memasang perangkat *smoke detector* (pendeteksi asap) untuk memantau kondisi ruangan Pusat Data; dan

i. memiliki alat pemadam api ringan (APAR) khusus yang dapat digunakan untuk peralatan elektronik.

Pasal 16

(1) Keamanan komunikasi sebagaimana dimaksud pada Pasal 8 ayat (2) huruf h mencakup keamanan perpindahan Informasi.

(2) Perpindahan Informasi sebagaimana dimaksud pada ayat (1) dilaksanakan untuk memelihara keamanan Informasi yang dipindahkan antar Perangkat Daerah ataupun pihak luar.

(3) Perpindahan Informasi sebagaimana dimaksud pada ayat (1) dilaksanakan melalui:

a. prosedur dan kebijakan perpindahan Informasi, bahwa kebijakan, prosedur dan kendali perpindahan yang resmi harus ada untuk melindungi perpindahan Informasi melalui penggunaan semua jenis fasilitas komunikasi;

b. perjanjian perpindahan Informasi, bahwa perjanjian harus mengatur perpindahan Informasi yang aman antara Perangkat Daerah dan pihak luar;

c. pesan elektronik, bahwa Informasi yang terdapat dalam pesan elektronik harus dilindungi dengan tepat; dan

d. perjanjian kerahasiaan atau menjaga rahasia (*nondisclosure agreement*), bahwa persyaratan untuk perjanjian kerahasiaan atau menjaga rahasia mencerminkan kebutuhan Pemerintah Daerah untuk perlindungan Informasi harus diidentifikasi, ditinjau secara teratur dan didokumentasikan.

Bagian Ketiga

Pengelolaan Sumber Daya Keamanan Informasi

Pasal 17

(1) Dinas melaksanakan pengelolaan sumber daya keamanan informasi sebagaimana dimaksud dalam Pasal 4 ayat (1) huruf b.

(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.

Paragraf 1

Pengelolaan Aset Keamanan Teknologi Informasi dan Komunikasi

Pasal 18

(1) Pengelolaan aset keamanan teknologi Informasi dan komunikasi sebagaimana dimaksud dalam Pasal 17 ayat (2) huruf a dilakukan melalui perencanaan, pengadaan, pemanfaatan, dan penghapusan terhadap aset keamanan teknologi Informasi dan komunikasi sesuai dengan ketentuan peraturan perundang-undangan.

(2) 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 19

(1) Pemerintah Daerah merumuskan rencana kebutuhan aset keamanan teknologi Informasi dan komunikasi dan menetapkannya sebagai aset keamanan teknologi Informasi dan komunikasi Pemerintah Daerah.

(2) Perumusan rencana aset keamanan teknologi Informasi dan komunikasi harus berdasarkan pada aset keamanan teknologi Informasi dan komunikasi yang telah direkomendasikan oleh BSSN.

(3) Hasil penetapan aset keamanan teknologi Informasi dan komunikasi diajukan Pemerintah Daerah kepada BSSN untuk permohonan pemenuhan peralatan sandi kebutuhan Pemerintah Daerah.

Pasal 20

(1) Bupati melalui Dinas bertanggung jawab dalam pengadaan aset keamanan teknologi Informasi dan komunikasi.

(2) Perangkat Daerah berwenang untuk melakukan pengajuan terkait pengadaan aset keamanan teknologi Informasi dan komunikasi.

(3) Pengadaan aset keamanan teknologi Informasi dan komunikasi dilaksanakan berdasarkan prinsip efisien, efektif, transparan & terbuka, bersaing, adil, dan akuntabel.

Pasal 21

(1) Dinas sesuai dengan kewenangannya melakukan pengelolaan dan pemanfaatan aset keamanan teknologi Informasi dan komunikasi.

(2) Aset keamanan teknologi Informasi dan komunikasi dimanfaatkan untuk kepentingan Pengamanan Informasi.

(3) Pemanfaatan aset keamanan teknologi Informasi dan komunikasi dilaksanakan melalui:

a. penggunaan aset keamanan teknologi Informasi dan komunikasi;

b. pemeliharaan aset keamanan teknologi Informasi dan komunikasi;

c. perbaikan aset keamanan teknologi Informasi dan komunikasi;

d. pendistribusian aset keamanan teknologi Informasi dan komunikasi; dan

e. pengawasan dan pengendalian aset keamanan teknologi Informasi dan komunikasi.

(4) Penggunaan aset keamanan teknologi Informasi dan komunikasi sebagaimana dimaksudkan pada ayat (3) huruf a meliputi:

a. materiil sandi;

b. tempat kegiatan sandi; dan

c. alat pendukung utama (APU) Persandian.

(5) Pemeliharaan aset keamanan teknologi Informasi dan komunikasi sebagaimana dimaksudkan pada ayat (3) huruf b mencakup:

a. memastikan peralatan sandi bebas dari debu/kotoran atau benda lain yang memicu gangguan operasional peralatan sandi;

b. menjaga Ketersediaan dan kestabilan arus listrik sesuai persyaratan pada peralatan sandi;

c. menjaga dan memonitor Ketersediaan koneksi saluran telekomunikasi pada peralatan sandi;

d. memastikan peralatan sandi dapat berfungsi sebagaimana mestinya;

e. menjaga kestabilan suhu ruangan tempat peletakan peralatan sandi;

f. meletakkan peralatan sandi pada tempat yang aman dari kemungkinan bencana, pencurian, dan kehilangan.

g. memastikan kelengkapan perangkat; dan

h. memastikan kelengkapan dokumen serah terima barang, berita acara serah terima dan/atau penarikan.

(6) Perbaikan aset keamanan teknologi Informasi dan komunikasi sebagaimana dimaksudkan pada ayat (3) huruf c dilakukan melalui perbaikan umum, yang merupakan perbaikan yang tidak berkaitan dengan aspek Kriptografi, dilakukan oleh Dinas dengan berkoordinasi dengan BSSN.

(7) Pendistribusian aset keamanan teknologi Informasi dan komunikasi sebagaimana dimaksudkan pada ayat (3) huruf d wajib memperhatikan ketentuan:

a. dilengkapi dengan berita acara penyerahan;

b. terjamin keamanan dan keutuhannya sehingga terhindar dari kehilangan dan kerusakan; dan

c. dalam keadaan netral atau non aktif (tidak terisi kunci sistem sandi).

(8) Pengawasan dan pengendalian aset keamanan teknologi Informasi dan komunikasi sebagaimana dimaksudkan pada ayat (3) huruf e harus dilakukan secara menyeluruh, terus menerus, dan berkesinambungan.

Pasal 22

(1) Dinas bertanggung jawab dalam penghapusan aset keamanan teknologi Informasi dan komunikasi.

(2) Perangkat Daerah berwenang untuk melakukan pengajuan terkait penghapusan aset keamanan teknologi Informasi dan komunikasi.

(3) Penghapusan aset keamanan teknologi Informasi dan komunikasi dilakukan berdasarkan prinsip kehati-hatian dan ketepatan.

(4) Penghapusan aset keamanan teknologi Informasi dan komunikasi meliputi:

a. penghapusan dari daftar barang pengguna dan/atau daftar barang kuasa pengguna terkait aset keamanan teknologi Informasi dan komunikasi Pemerintah Daerah; dan

b. penghapusan dari daftar barang milik Pemerintah Daerah terkait aset keamanan teknologi Informasi dan komunikasi Pemerintah Daerah.

Pasal 23

(1) Penghapusan dari daftar barang pengguna dan/atau daftar barang kuasa pengguna terkait aset keamanan teknologi Informasi dan komunikasi Pemerintah Daerah sebagaimana dimaksud dalam Pasal 22 ayat (4) huruf a dilakukan dalam hal barang milik Daerah sudah tidak berada dalam penguasaan Pemerintah Daerah.

(2) Penghapusan sebagaimana dimaksud pada ayat (1) dilakukan dengan menerbitkan keputusan penghapusan dari Dinas setelah mendapatkan persetujuan dari Bupati untuk barang milik Daerah dan BSSN untuk barang milik negara.

(3) Penghapusan aset keamanan teknologi Informasi dan komunikasi dilakukan karena:

a. pengalihan status penggunaan;

b. pemindahantangan; atau

c. pemusnahan.

(4) Bupati melalui Dinas dapat mendelegasikan persetujuan Penghapusan aset keamanan teknologi Informasi dan komunikasi kepada BSSN.

(5) Pelaksanaan penghapusan aset keamanan teknologi Informasi dan komunikasi dilaporkan kepada BSSN.

Pasal 24

(1) Penghapusan dari daftar barang milik Daerah terkait aset keamanan teknologi Informasi dan komunikasi Pemerintah Daerah sebagaimana dimaksud dalam Pasal 22 ayat (4) huruf b dilakukan dalam hal barang milik Daerah sudah beralih kepemilikannya, terjadi pemusnahan, atau karena sebab lain.

(2) Penghapusan sebagaimana pada ayat (1) dilakukan berdasarkan keputusan dan/atau laporan penghapusan dari Pemerintah Daerah melalui Dinas.

Paragraf 2

Pengelolaan Sumber Daya Manusia

Pasal 25

(1) Dinas melakukan pengelolaan sumber daya manusia sebagaimana dimaksud dalam Pasal 17 ayat (2) huruf b.

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

a. pengembangan kompetensi;

b. pembinaan karier;

c. pendayagunaan; dan

d. pemberian tunjangan pengamanan Persandian.

Pasal 26

(1) Pengembangan kompetensi sebagaimana dimaksud dalam Pasal 25 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 berkaitan dengan pengembangan kompetensi sumber daya manusia di bidang Keamanan Informasi;

b. mengikuti berbagai kegiatan pengembangan kompetensi yang dilaksanakan oleh BSSN, pihak lain, atau Pemerintah Daerah; dan

c. memenuhi jumlah waktu minimal seorang pegawai untuk meningkatkan kompetensi bidangnya.

(2) Pembinaan karir sebagaimana dimaksud dalam Pasal 25 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 25 ayat (2) huruf c dilaksanakan agar seluruh sumber daya manusia yang bertugas di Dinas melaksanakan tugasnya sesuai dengan sasaran kinerja pegawai dan standar kompetensi kerja pegawai yang ditetapkan.

(4) Pemberian tunjangan pengamanan Persandian sebagaimana dimaksudkan dalam Pasal 25 ayat (2) huruf d meliputi tunjangan pengamanan Persandian dan tunjangan jabatan fungsional sandiman.

Paragraf 3

Manajemen Pengetahuan

Pasal 27

(1) Dinas melakukan manajemen pengetahuan sebagaimana dimaksud dalam Pasal 17 ayat (2) huruf c.

(2) Manajemen pengetahuan sebagaimana dimaksud pada ayat (1) dilakukan untuk meningkatkan kualitas Layanan Keamanan Informasi dan mendukung proses pengambilan keputusan terkait Keamanan Informasi.

(3) Manajemen pengetahuan dilakukan melalui serangkaian proses pengumpulan, pengolahan, penyimpanan, penggunaan, dan alih pengetahuan dan teknologi yang dihasilkan dalam pelaksanaan Keamanan Informasi Pemerintah Daerah.

(4) Manajemen pengetahuan sebagaimana dimaksud pada ayat (3) dilaksanakan berdasarkan pedoman manajemen pengetahuan Keamanan Informasi Pemerintah Daerah.

(5) Dalam pelaksanaan manajemen pengetahuan, Dinas berkoordinasi dan dapat melakukan konsultasi dengan BSSN.

Pasal 28

(1) Pengumpulan pengetahuan dilakukan untuk kategori pengetahuan, meliputi:

a. pengetahuan implisit; dan

b. pengetahuan eksplisit.

(2) Pengetahuan implisit sebagaimana dimaksud pada ayat (1) huruf a merupakan pengetahuan yang masih berada dalam pikiran individu yang memiliki pengetahuan tersebut.

(3) Pengetahuan eksplisit sebagaimana dimaksud pada ayat (1) huruf b merupakan pengetahuan yang sudah secara eksplisit diutarakan dan tersedia dalam organisasi.

(4) Pengumpulan pengetahuan dan teknologi yang dihasilkan dalam pelaksanaan Keamanan Informasi dilakukan melalui serangkaian proses untuk mengetahui aset pengetahuan yang dimiliki Pemerintah Daerah, aset ini dapat berupa produk/layanan, portofolio proyek, data, basis data kompetensi organisasi, literatur (buku, majalah, laporan), dan sebagainya.

(5) Pengetahuan yang telah teridentifikasi kemudian diprioritaskan implementasinya, sehingga menjadi ruang lingkup.

Pasal 29

(1) Pengolahan pengetahuan dan teknologi yang dihasilkan dalam pelaksanaan Keamanan Informasi dilakukan dengan mengintegrasikan dengan pengetahuan lainnya.

(2) Pengolahan pengetahuan dan teknologi yang dihasilkan dalam pelaksanaan Keamanan Informasi juga dapat dilakukan dengan membagi pengetahuan berdasarkan kompetensi atau kategori tertentu sesuai dengan yang telah ditentukan oleh Pemerintah Daerah.

Pasal 30

(1) Pengetahuan yang telah teridentifikasi direkam dan disimpan ke dalam *Database* pengetahuan organisasi atau *Knowledge Repository*.

(2) Setiap Perangkat Daerah wajib mendokumentasikan pengetahuan dan teknologi yang dihasilkan dalam pelaksanaan Keamanan Informasi yang kemudian akan dilakukan penyimpanan oleh Dinas.

Pasal 31

(1) Penggunaan pengetahuan dan teknologi yang dihasilkan dalam pelaksanaan Keamanan Informasi diwujudkan dalam prosedur atau peraturan untuk mengarahkan ke perilaku pada masa yang akan datang.

(2) Pada saat penggunaan pengetahuan dan teknologi yang dihasilkan dalam pelaksanaan Keamanan Informasi dapat melakukan aktivitas pengembangan dan penyempurnaan lebih lanjut dari pengetahuan yang telah didapatkan.

Pasal 32

(1) Kegiatan alih pengetahuan dan teknologi yang dihasilkan dalam pelaksanaan Keamanan Informasi dapat berlangsung secara tradisional maupun dengan menggunakan teknologi pendukung.

(2) Pemerintah Daerah wajib menjamin terjadinya alih pengetahuan dan teknologi yang dihasilkan dalam pelaksanaan Keamanan Informasi antar Perangkat Daerah yang membutuhkan.

(3) Kegiatan alih pengetahuan dan teknologi yang dihasilkan dalam pelaksanaan Keamanan Informasi dilakukan melalui:

a. pendidikan dan pelatihan kerja sesuai dengan kualifikasi jabatan yang diduduki; dan

b. pelaksanaan pelatihan atau pengajaran dalam jangka waktu tertentu.

Pasal 33

Ketentuan lebih lanjut terkait teknis pelaksanaan manajemen pengetahuan yang meliputi proses pengumpulan, pengolahan, penyimpanan, penggunaan, dan alih pengetahuan dan teknologi yang dihasilkan dalam pelaksanaan Keamanan Informasi Pemerintah Daerah ditetapkan oleh kepala Dinas dengan berpedoman pada ketentuan peraturan perundang-undangan.

Bagian Keempat

Pengamanan Sistem Elektronik dan Pengamanan Informasi Non-elektronik

Pasal 34

Dinas melaksanakan pengamanan Sistem Elektronik dan Pengamanan Informasi non-elektronik sebagaimana dimaksud dalam Pasal 4 ayat (1) huruf c sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 35

Pengamanan Sistem Elektronik sebagaimana dimaksud dalam Pasal 34 terdiri atas:

a. penjaminan Kerahasiaan, Keutuhan, Ketersediaan, Keaslian, dan Kenirsangkalan 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 36

(1) Dalam melaksanakan pengelolaan aset dalam melaksanakan pengamanan Sistem Elektronik sebagaimana dimaksud dalam Pasal 35, 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 perlindungan terhadap Sistem Elektronik untuk menjamin keberlangsungan penyelenggaraan pemerintahan berbasis elektronik.

(5) Penanggulangan dan pemulihan sebagaimana dimaksud pada 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 37

(1) Dalam melaksanakan pengamanan Sistem Elektronik sebagaimana dimaksud dalam Pasal 36, Dinas wajib menggunakan Sertifikat Elektronik pada setiap layanan publik dan layanan pemerintahan berbasis elektronik.

(2) Sertifikat Elektronik sebagaimana dimaksud pada ayat (1) diterbitkan oleh BSSN dan/atau lembaga penyelenggara Sertifikasi Elektronik dalam negeri yang telah diakui.

(3) Untuk mendapatkan Sertifikat Elektronik sebagaimana dimaksud pada ayat (2) dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 38

(1) Dalam mendukung penyelenggaraan layanan pemerintahan berbasis elektronik Dinas 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.

(3) Ketentuan lebih lanjut terkait teknis penyelenggaraan pusat operasi Pengamanan Informasi sebagaimana dimaksud pada ayat (1) di lingkungan Pemerintah Daerah ditetapkan oleh kepala Dinas dengan berpedoman pada ketentuan peraturan perundang-undangan.

Pasal 39

(1) Dalam mendukung Pengamanan Informasi non-elektronik sebagaimana dimaksud dalam Pasal 35 dilakukan pada tahapan pemrosesan, pengiriman, penyimpanan, dan pemusnahan Informasi non-elektronik.

(2) Ketentuan lebih lanjut terkait teknis Pengamanan Informasi non-elektronik sebagaimana dimaksud pada ayat (1) di lingkungan Pemerintah Daerah ditetapkan oleh kepala Dinas dengan berpedoman pada ketentuan peraturan perundang-undangan.

Pasal 40

(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) Ketentuan lebih lanjut terkait teknis pelaksanaan audit Keamanan Informasi sebagaimana dimaksud pada ayat (1) di lingkungan Pemerintah Daerah ditetapkan oleh kepala Dinas dengan berpedoman pada ketentuan peraturan perundang-undangan.

Bagian Kelima

Penyediaan Layanan Keamanan Informasi

Pasal 41

(1) Dinas melaksanakan penyediaan Layanan Keamanan Informasi sebagaimana dimaksud dalam Pasal 4 ayat (1) huruf d.

(2) Layanan Keamanan Informasi sebagaimana dimaksud pada ayat (1) disediakan untuk Pengguna Layanan yang terdiri atas:

a. Bupati dan wakil Bupati;

b. Perangkat Daerah;

c. pegawai atau aparatur sipil negara pada Pemerintah Daerah; dan

d. pihak lainnya.

Pasal 42

Jenis Layanan Keamanan Informasi sebagaimana dimaksud dalam Pasal 41 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. perlindungan Informasi melalui penyediaan perangkat teknologi Keamanan Informasi dan jaring komunikasi sandi;

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 Persandian dan Keamanan Informasi;

j. pengelolaan pusat operasi Pengamanan Informasi;

k. penanganan insiden keamanan Sistem Elektronik;

l. forensik digital;

m. perlindungan Informasi pada kegiatan penting Pemerintah Daerah melalui teknik pengamanan gelombang frekuensi atau sinyal;

n. perlindungan Informasi pada aset/fasilitas penting milik atau yang akan digunakan Pemerintah Daerah melalui kegiatan kontra pengindraan;

o. konsultasi Keamanan Informasi bagi Pengguna Layanan; dan/atau

p. jenis Layanan Keamanan Informasi lainnya.

Pasal 43

(1) Dalam menyediakan Layanan Keamanan Informasi sebagaimana dimaksud dalam Pasal 42 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) Ketentuan lebih lanjut terkait teknis pelaksanaan manajemen Layanan Keamanan Informasi sebagaimana dimaksud pada ayat (3) di lingkungan Pemerintah Daerah ditetapkan oleh kepala Dinas dengan berpedoman pada ketentuan peraturan perundang-undangan.

BAB III

PENETAPAN POLA HUBUNGAN KOMUNIKASI SANDI

ANTAR PERANGKAT DAERAH

Pasal 44

(1) Bupati melakukan penetapan Pola Hubungan Komunikasi Sandi antar Perangkat Daerah sebagaimana dimaksud dalam Pasal 3 huruf b.

(2) Penetapan Pola Hubungan Komunikasi Sandi antar Perangkat Daerah sebagaimana dimaksud pada ayat (1) untuk menentukan Jaring Komunikasi Sandi internal Pemerintah Daerah.

(3) Jaring Komunikasi Sandi internal Pemerintah Daerah sebagaimana dimaksud pada ayat (2) terdiri atas:

a. Jaring Komunikasi Sandi antar Perangkat Daerah;

b. Jaring Komunikasi Sandi internal Perangkat Daerah; dan

c. Jaring Komunikasi Sandi pimpinan Daerah.

(4) Jaring Komunikasi Sandi antar Perangkat Daerah sebagaimana dimaksud pada ayat (3) huruf a menghubungkan seluruh Perangkat Daerah.

(5) Jaring Komunikasi Sandi internal Perangkat Daerah sebagaimana dimaksud pada ayat (3) huruf b menghubungkan antar Pengguna Layanan di lingkup internal Perangkat Daerah.

(6) Jaring Komunikasi Sandi pimpinan Daerah sebagaimana dimaksud pada ayat (3) huruf c menghubungkan antara Bupati, wakil Bupati, dan kepala Perangkat Daerah.

Pasal 45

(1) Penetapan Pola Hubungan Komunikasi Sandi antar Perangkat Daerah sebagaimana dimaksud dalam Pasal 44 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 pegawai.

(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 Jaring Komunikasi Sandi;

b. topologi atau model keterhubungan Jaring Komunikasi Sandi antar Pengguna Layanan;

c. perangkat keamanan teknologi Informasi dan komunikasi, dan infrastruktur komunikasi, serta fasilitas lainnya yang dibutuhkan; dan

d. tugas dan tanggung jawab pengelola dan Pengguna Layanan.

(5) Bupati menetapkan hasil analisis Pola Hubungan Komunikasi Sandi sebagaimana dimaksud pada ayat (4) sebagai Pola Hubungan Komunikasi Sandi antar Perangkat Daerah dengan Keputusan Bupati.

(6) Keputusan sebagaimana dimaksud pada ayat (5) paling sedikit memuat:

a. entitas Pengguna Layanan yang terhubung dalam jaring komunikasi sandi;

b. topologi atau bentuk keterhubungan antar Pengguna Layanan;

c. sarana dan prasarana 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 Kalimantan Selatan sebagai wakil pemerintah pusat dan ditembuskan kepada kepala BSSN.

(8) Ketentuan lebih lanjut mengenai teknis penetapan Pola Hubungan Komunikasi Sandi antar Perangkat Daerah sebagaimana dimaksud dalam Pasal 44 ayat (1) di lingkungan Pemerintah Daerah ditetapkan oleh kepala Dinas dengan berpedoman pada ketentuan peraturan perundang-undangan.

BAB IV

PEMANTAUAN, EVALUASI, DAN PELAPORAN

Pasal 46

(1) Pemantauan dan evaluasi dilaksanakan terhadap penyelenggaraan Persandian untuk Pengamanan Informasi dan penetapan Pola Hubungan Komunikasi Sandi antar Perangkat Daerah.

(2) Dinas melakukan pemantauan dan evaluasi sebagaimana dimaksud pada ayat (1) setiap 1 (satu) tahun sekali.

(3) Dinas menyampaikan laporan hasil pemantauan dan evaluasi sebagaimana dimaksud pada ayat (1) kepada Bupati dan Gubernur Kalimantan Selatan sebagai wakil pemerintah pusat.

Pasal 47

Ketentuan lebih lanjut mengenai teknis pemantauan, evaluasi, dan pelaporan terhadap penyelenggaraan Persandian untuk Pengamanan Informasi dan penetapan Pola Hubungan Komunikasi Sandi antar Perangkat Daerah sebagaimana dimaksud dalam pasal 45 ditetapkan oleh kepala Dinas dengan berpedoman pada ketentuan peraturan perundang-undangan.

BAB V

PEMBINAAN DAN PENGAWASAN TEKNIS

Pasal 48

(1) Pemerintah Daerah mendapatkan pembinaan dan pengawasan teknis terhadap penyelenggaraan Persandian untuk Pengamanan Informasi Pemerintah Daerah dan penetapan Pola Hubungan Komunikasi Sandi antar Perangkat Daerah dari BSSN dan Gubernur Kalimantan Selatan sebagai wakil pemerintah pusat sesuai dengan kewenangannya.

(2) Dinas sesuai dengan kewenangannya melakukan pembinaan dan pengawasan teknis terhadap Perangkat Daerah terhadap penyelenggaraan Persandian untuk Pengamanan Informasi Pemerintah Daerah dan penetapan Pola Hubungan Komunikasi Sandi antar Perangkat Daerah.

(3) Ketentuan lebih lanjut terkait teknis pelaksanaan pembinaan dan pengawasan teknis terhadap Perangkat Daerah sebagaimana dimaksud dalam ayat (2) ditetapkan oleh kepala Dinas dengan berpedoman pada ketentuan peraturan perundang-undangan.

BAB VI

PEMBIAYAAN

Pasal 49

Pembiayaan 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; dan/atau

b. sumber lain yang sah dan tidak mengikat sesuai dengan ketentuan peraturan perundang-undangan.

BAB VII

KETENTUAN PENUTUP

Pasal 50

Pada saat Peraturan Bupati ini mulai berlaku:

a. kebijakan Pemerintah Daerah dan semua produk hukum Daerah yang mengatur mengenai pelaksanaan Persandian untuk Pengamanan Informasi Pemerintah Daerah yang telah ditetapkan dinyatakan masih tetap berlaku sepanjang tidak bertentangan dengan Peraturan Bupati ini; dan

b. kebijakan Pemerintah Daerah dan semua produk hukum Daerah yang mengatur mengenai Pelaksanaan Persandian untuk Pengamanan Informasi Pemerintah Daerah yang telah ditetapkan wajib menyesuaikan dengan ketentuan dalam Peraturan Bupati ini paling lama 1 (satu) tahun terhitung sejak Peraturan Bupati ini diundangkan.

Pasal 51

Peraturan Bupati ini mulai berlaku pada tanggal diundangkan.

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

Ditetapkan di Kandangan
pada tanggal 14 Februari 2022

BUPATI HULU SUNGAI SELATAN

ttd

ACHMAD FIKRY

Diundangkan di Kandangan
pada tanggal 14 Februari 2022

SEKRETARIS DAERAH
KABUPATEN HULU SUNGAI SELATAN,

ttd

MUHAMMAD NOOR

Salinan sesuai dengan aslinya
SEKRETARIAT DAERAH
KABUPATEN HULU SUNGAI SELATAN
Kepala Bagian Hukum,

FITRI

BERITA DAERAH KABUPATEN HULU SUNGAI SELATAN
TAHUN 2022 NOMOR 10