SALINAN

BUPATI BOGOR
PROVINSI JAWA BARAT

PERATURAN BUPATI BOGOR
NOMOR 57 TAHUN 2021

TENTANG

PELAKSANAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI
DI PEMERINTAH KABUPATEN BOGOR

DENGAN RAHMAT TUHAN YANG MAHA ESA

BUPATI BOGOR,

Menimbang : a. bahwa berdasarkan ketentuan Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian untuk Pengamanan Informasi di Pemerintah Daerah, pemerintah daerah wajib mengelola informasi yang dimilikinya dan untuk melindungi informasi perlu dilakukan upaya pengamanan informasi melalui penyelenggaraan persandian;

b. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, perlu membentuk Peraturan Bupati tentang Pelaksanaan Persandian untuk Pengamanan Informasi di Pemerintah Kabupaten Bogor;

Mengingat : 1. Undang-Undang Nomor 14 Tahun 1950 tentang Pemerintahan Daerah Kabupaten dalam Lingkungan Provinsi Djawa Barat (Berita Negara Republik Indonesia Tahun 1950 Nomor 8) sebagaimana telah diubah dengan Undang-Undang Nomor 4 Tahun 1968 tentang Pembentukan Kabupaten Purwakarta dan Kabupaten Subang dengan mengubah Undang-Undang Nomor 14 Tahun 1950 tentang Pembentukan Daerah-Daerah Kabupaten dalam Lingkungan Provinsi Djawa Barat (Lembaran Negara Republik Indonesia Tahun 1968 Nomor 31, Tambahan Lembaran Negara Republik Indonesia Nomor 2851);

2. Undang-Undang Nomor 28 Tahun 1999 tentang Penyelenggaraan Negara yang Bersih dan Bebas dari Kolusi, Korupsi dan Nepotisme (Lembaran Negara Republik Indonesia Tahun 1999 Nomor 75, Tambahan Lembaran Negara Republik Indonesia Nomor 3851);

3. Undang-Undang Nomor 39 Tahun 1999 tentang Hak Asasi Manusia (Lembaran Negara Republik Indonesia Tahun 1999 Nomor 165, Tambahan Lembaran Negara Republik Indonesia Nomor 3886);

4. Undang-Undang...

4. Undang-Undang Nomor 40 Tahun 1999 tentang Pers (Lembaran Negara Republik Indonesia Tahun 1999 Nomor 40, Tambahan Lembaran Negara Republik Indonesia Nomor 2815);
5. 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):
6. 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);
7. Undang-Undang Nomor 37 Tahun 2008 tentang Ombudsman Republik Indonesia (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 139, Tambahan Lembaran Negara Republik Indonesia Nomor 4899);
8. Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik (Lembaran Negara Republik Indonesia Tahun 2009 Nomor 112, Tambahan Lembaran Negara Republik Indonesia Nomor 5038);
9. Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 244, Tambahan Lembaran Negara Republik Indonesia Nomor 5587) sebagaimana telah beberapa kali diubah, terakhir dengan Undang-Undang Nomor 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);
10. Peraturan Pemerintah Nomor 61 Tahun 2010 tentang Pelaksanaan Undang-Undang Nomor 41 Tahun 2008 tentang Keterbukaan Informasi Publik (Lembaran Negara Republik Indonesia Tahun 2010 Nomor 99, Tambahan Lembaran Negara Republik Indonesia Nomor 5149);
11. Peraturan Pemerintah Nomor 96 Tahun 2012 tentang Pelaksanaan Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik (Lembaran Negara Republik Indonesia Tahun 2012 Nomor 215, Tambahan Lembaran Negara Republik Indonesia Nomor 5357);
12. 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);

13. Peraturan...

13. Peraturan Pemerintah Nomor 12 Tahun 2019 tentang Pengelolaan Keuangan Daerah (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 42, Tambahan Lembaran Negara Republik Indonesia Nomor 6322);
14. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
15. Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik (Berita Negara Republik Indonesia Tahun 2016 Nomor 1829);
16. Peraturan Menteri Dalam Negeri Republik Indonesia Nomor 70 Tahun 2019 tentang Sistem Informasi Pemerintahan Daerah (Berita Negara Republik Indonesia Tahun 2019 Nomor 1114);
17. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 26 Tahun 2020 tentang Pedoman Evaluasi Pelaksanaan Reformasi Birokrasi (Berita Negara Republik Indonesia Tahun 2020 Nomor 442);
18. Peraturan Kepala Lembaga Sandi Negara Nomor 14 Tahun 2010 tentang Pedoman Gelar Jaring Komunikasi Sandi (Berita Negara Republik Indonesia Tahun 2010 Nomor 292);
19. Peraturan Kepala Lembaga Sandi Negara Nomor 10 Tahun 2017 tentang Penyelenggaraan Sertifikat Elektronik (Berita Negara Republik Indonesia Tahun 2017 Nomor 907);
20. 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);
21. Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2020 tentang Sistem Pengamanan Dalam Penyelenggaraan Sistem Elektronik (Berita Negara Republik Indonesia Tahun 2020 Nomor 1375);
22. Peraturan Menteri Dalam Negeri Nomor 77 Tahun 2020 tentang Pedoman Teknis Pengelolaan Keuangan Daerah (Berita Negara Republik Indonesia Tahun 2020 Nomor 1781);
23. Peraturan Daerah Provinsi Jawa Barat Nomor 4 Tahun 2021 tentang Penyelenggaraan Komunikasi dan Informatika, Statistik, dan Persandian (Lembaran Daerah Provinsi Jawa Barat Tahun 2021 Nomor 4, Tambahan Lembaran Daerah Provinsi Jawa Barat Nomor 248);
24. Peraturan Daerah Kabupaten Bogor Nomor 8 Tahun 2009 tentang Pokok-Pokok Pengelolaan Keuangan Daerah (Lembaran Daerah Kabupaten Bogor Tahun 2009 Nomor 8, Tambahan Lembaran Daerah Kabupaten Bogor Nomor 37);

25.Peraturan...

25. Peraturan Daerah Kabupaten Bogor Nomor 12 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah (Lembaran Daerah Kabupaten Bogor Nomor 12, Tambahan Lembaran Daerah Kabupaten Bogor Nomor 96) sebagaimana telah diubah dengan Peraturan Daerah Kabupaten Bogor Nomor 2 Tahun 2020 tentang Perubahan atas Peraturan Daerah Nomor 12 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah (Lembaran Daerah Kabupaten Bogor Nomor 12, Tambahan Lembaran Daerah Kabupaten Bogor Nomor 96);
26. Peraturan Bupati Bogor Nomor 63 tahun 2020 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik (Berita Daerah Kabupaten Bogor Tahun 2020 Nomor 64);
27. Peraturan Bupati Bogor Nomor 93 Tahun 2020 tentang Kedudukan, Susunan Organisasi, Tugas dan Fungsi Serta Tata Kerja Dinas Komunikasi dan Informatika (Berita Daerah Kabupaten Bogor Tahun 2020 Nomor 94);

MEMUTUSKAN:

Menetapkan : PERATURAN BUPATI BOGOR TENTANG PELAKSANAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI DI PEMERINTAH KABUPATEN BOGOR.

BAB I

KETENTUAN UMUM

Pasal 1

Dalam Peraturan Bupati ini yang dimaksud dengan:

1. Daerah adalah Kabupaten Bogor.
2. Pemerintah Daerah adalah pemerintah Kabupaten Bogor.
3. Gubernur adalah Gubernur Jawa Barat.
4. Bupati adalah Bupati Bogor.
5. Perangkat Daerah adalah perangkat daerah di lingkungan Pemerintah Kabupaten Bogor.
6. Dinas Komunikasi dan Informatika, yang selanjutnya disebut Dinas, adalah Dinas Komunikasi dan Informatika Kabupaten Bogor.
7. Kepala Dinas Komunikasi dan Informatika, yang selanjutnya disebut Kepala Dinas, adalah Kepala Dinas Komunikasi dan Informatika Kabupaten Bogor.
8. Badan Siber dan Sandi Negara, yang selanjutnya disingkat BSSN, adalah lembaga pemerintah yang menyelenggarakan tugas pemerintahan di bidang keamanan siber dan persandian.

9. Sistem…

9. Sistem Pemerintahan Berbasis Elektronik, yang selanjutnya disingkat SPBE, adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada pengguna.
10. 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.
11. Keamanan Informasi adalah terjaganya kerahasiaan (*confidentiality*), keutuhan (*integrity*), ketersediaan (*availability*), keaslian, dan kenirsangkalan (*nonrepudiation*) Informasi.
12. Jaring Komunikasi Sandi adalah keterhubungan antar pengguna persandian melalui jaring telekomunikasi.
13. Pengamanan Informasi adalah segala upaya, kegiatan, dan tindakan untuk mewujudkan keamanan informasi.
14. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi elektronik.
15. 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 BSSN dan/atau lembaga penyelenggara sertifikasi elektronik dalam negeri yang telah diakui.
16. Layanan Keamanan Informasi adalah keluaran dari pelaksanaan 1 (satu) atau beberapa kegiatan penyelenggaraan urusan pemerintahan bidang persandian dan yang memiliki nilai manfaat.
17. 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.
18. 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 Undang-Undang serta informasi lain yang berkaitan dengan kepentingan publik.

19. Pengguna...

19. Pengguna Layanan Keamanan Informasi, yang selanjutnya disebut Pengguna Layanan, adalah para pihak yang memanfaatkan layanan keamanan informasi.
20. Dokumen Elektronik adalah setiap informasi elektronik yang dibuat, diteruskan, dikirimkan, diterima atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal 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.
21. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta otentikasi data
22. Sumber Daya Manusia Teknologi Informasi Komunikasi adalah pegawai perangkat daerah yang memiliki tugas dan wewenang terkait dengan teknologi informasi dan komunikasi.
23. 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.
24. Tim Tanggap Insiden Keamanan Komputer (*Computer Security Incident Response Team),* yang selanjutnya disebut tim BOGORKAB-CSIRT, adalah layanan reaktif, layanan proaktif dan layanan manajemen kualitas keamanan di Kabupaten Bogor.
25. Balai Sertifikasi Elektronik, yang selanjutnya disebut BSrE, adalah unit pelaksana teknis penyelenggara Otoritas Sertifikat Digital (OSD) Badan Siber dan Sandi Negara yang berada di bawah dan bertanggung jawab kepada Kepala Lembaga Sandi Negara.
26. 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.
27. Kerahasiaan adalah penjaminan atas aset SPBE yang informasinya tidak tersedia atau diungkapkan kepada individu, entitas, atau proses yang tidak mempunyai hak untuk mengaksesnya.
28. Keutuhan adalah properti yang menyatakan bahwa suatu aset SPBE akurat dan lengkap.
29. Ketersediaan adalah properti yang menyatakan bahwa aset SPBE dapat diakses dan digunakan atas permintaan oleh entitas yang berwenang.

30. Keaslian…

30. Keaslian adalah properti yang menyatakan bahwa aset SPBE terkait merupakan entitas yang diklaimnya.
31. Kenirsangkalan adalah kemampuan untuk membuktikan terjadinya suatu peristiwa yang diklaim atau tindakan dan entitas asalnya.

BAB II

MAKSUD DAN TUJUAN

Pasal 2

Maksud dibentuknya Peraturan Bupati ini adalah:

a. menjadi acuan penyelenggaraan persandian untuk pengamanan informasi Pemerintah Daerah; dan
b. menjadi pedoman penetapan pola hubungan komunikasi sandi antar perangkat daerah.

Pasal 3

Pelaksanaan persandian untuk pengamanan informasi di Daerah bertujuan untuk:

a. menciptakan harmonisasi dalam melaksanakan persandian untuk pengamanan informasi di Pemerintah Daerah;
b. meningkatkan komitmen, efektifitas, 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.

BAB III

PENYELENGGARAAN PERSANDIAN UNTUK PENGAMANAN INFORMASI PEMERINTAH DAERAH KABUPATEN BOGOR

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...

c. pengamanan sistem elektronik dan pengamanan informasi nonelektronik; dan

d. penyediaan layanan keamanan informasi.

(2) Bupati sesuai dengan kewenangannya bertanggung jawab terhadap penyelenggaraan persandian untuk pengamanan informasi sebagaimana dimaksud pada ayat (1).

(3) 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 sesuai dengan kewenangannya menyusun rencana strategis pengamanan informasi sebagaimana dimaksud dalam Pasal 5 huruf a.

(2) Penyusunan rencana strategis pengamanan informasi sebagaimana dimaksud pada ayat (1), dilaksanakan oleh Dinas.

(3) Dalam penyusunan rencana strategis sebagaimana dimaksud pada ayat (1), Bupati baik secara langsung maupun melalui Dinas dapat melakukan koordinasi dan konsultasi kepada BSSN.

(4) 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.

(5) Rencana…

(5) Rencana strategis pengamanan informasi yang telah disusun sebagaimana dimaksud pada ayat (1) diintegrasikan ke dalam Rencana Pembangunan Jangka Menengah Daerah.

Pasal 7

(1) Bupati sesuai dengan kewenangannya 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 menunjuk Dinas.

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

(6) Bupati melakukan evaluasi arsitektur keamanan informasi pada paruh waktu dan tahun terakhir pelaksanaan atau sewaktu-waktu sesuai dengan kebutuhan.

Pasal 8

(1) Bupati sesuai dengan kewenangannya menetapkan aturan mengenai tata kelola keamanan informasi sebagaimana dimaksud dalam Pasal 5 huruf c.

(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...

g. keamanan pusat data; dan/atau

h. keamanan komunikasi.

(3) Dalam melakukan penyusunan aturan mengenai tata kelola 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 menunjuk Dinas.

Pasal 9

(1) Keamanan sumber daya teknologi informasi sebagaimana dimaksud dalam 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, meliputi:

a. *confidentiality*, yaitu akses terhadap data/informasi dibatasi hanya bagi mereka yang punya otoritas;

b. *integrity*, yaitu data tidak boleh diubah tanpa ijin dari yang berhak;

c. *authentication*, yaitu untuk meyakinkan identitas pengguna sistem;

d. *availability*, yaitu terkait dengan ketersediaan layanan, termasuk *up-time* dari sistem dan teknologi informasi; dan

e. *non-repudiation*, yaitu 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-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. metoda *scripting software* aplikasi yang aman;

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

c. pengaturan keamanan sistem basis data yang tepat.

(5) Pengamanan…

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

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

(6) Untuk mencapai 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) Guna melaksanakan evaluasi keamanan sumber daya teknologi informasi, *assessment* kerentanan keamanan sistem (*security vulnerability system*) dapat dilakukan secara teratur sesuai dengan kebutuhan.

Pasal 10

(1) Keamanan akses kontrol sebagaimana dimaksud dalam 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 harus ditetapkan, didokumentasikan, dan direviu berdasarkan persyaratan organisasi dan kemanan informasi; dan

b. akses ke jaringan dan layanan jaringan yang telah secara khusus diberi wewenang untuk digunakan.

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

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

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

c. manajemen...

c. manajemen hak akses istimewa dilakukan dengan cara pengalokasian dan penggunaan hak akses istimewa harus dibatasi dan dikendalikan;

d. manajemen informasi otentikasi rahasia dari pengguna, dilakukan dengan cara alokasi dari informasi otentikasi rahasia harus dikendalikan melalui proses manajemen resmi;

e. reviu hak akses pengguna, dilakukan dengan cara pemilik aset harus mereviu hak akses pengguna secara periodik; dan

f. penghapusan atau penyesuaian hak akses, dilakukan dengan cara harus dilakukan penghapusan hak akses semua pegawai dan pengguna pihak eksternal pada informasi dan fasilitas pengolahan informasi 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, yakni 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, yaitu akses ke informasi dan fungsi sistem aplikasi harus dibatasi sesuai dengan kebijakan kendali akses;

b. prosedur *log-on* yang aman, yaitu ketika disyaratkan oleh kebijakan pengendalian akses, akses ke sistem dan aplikasi harus dikendalikan oleh prosedur *log-on* yang aman;

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

d. penggunaan program utilitas istimewa, yaitu 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, yaitu akses ke kode sumber program harus dibatasi.

Pasal 11

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

a. perlindungan...

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 logik.

(2) Perlindungan fisik sebagaimana dimaksud pada ayat (1) huruf a dilakukan melalui:

a. kendali akses ruang;

b. pemasangan teralis;

c. penggunaan kunci ganda;

d. pemasangan CCTV; dan/atau

e. penggunaan ruang *Telecommunications Electronics Materials Protected from Emanating Spurious Transmission* (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 logik sebagaimana dimaksud pada ayat (1) huruf c dilakukan dengan menggunakan teknik kriptografi dan steganografi untuk memenuhi aspek kerahasiaan, keutuhan, otentikasi, dan kenirsangkalan.

Pasal 12

(1) Keamanan sumber daya manusia sebagaimana dimaksud dalam 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 undang-undang terkait dan harus proporsional terhadap persyaratan Pemerintah Daerah, klasifikasi informasi yang akan diakses dan risiko yang dipersepsikan; dan

b. syarat...

b. syarat dan ketentuan kepegawaian, dikuatkan dengan adanya perjanjian tertulis dengan 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

Keamanan jaringan sebagaimana dimaksud dalam Pasal 8 ayat (2) huruf e dilaksanakan untuk menjamin perlindungan informasi dalam jaringan dan fasilitas pendukung pengolahan informasi, yang meliputi:

a. kendali jaringan, yaitu jaringan harus dikelola dan dikendalikan untuk melindungi informasi dalam sistem dan aplikasi;

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

c. pemisahan dalam jaringan, yaitu kelompok layanan informasi, pengguna dan sistem informasi harus dipisahkan pada jaringan.

Pasal 14

(1) Keamanan surat elektronik sebagaimana dimaksud dalam 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...

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 (*hardcopy* & *softcopy*).

Pasal 15

Penggunaan sertifikat elektronik di lingkungan Pemerintah Daerah diatur lebih lanjut dengan Peraturan Bupati tersendiri.

Pasal 16

(1) Keamanan pusat data sebagaimana dimaksud dalam Pasal 8 ayat (2) huruf g meliputi kontrol akses, keamanan fisik dan *logical*.

(2) Kontrol akses, keamanan fisik dan *logical* 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...

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; dan

g. melengkapi pusat data dengan sistem *audit trail* untuk pencatatan akses fisik dan akses *logical* yang terjadi.

Pasal 17

(1) Keamanan komunikasi sebagaimana dimaksud dalam Pasal 8 ayat (2) huruf g 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, yaitu kebijakan, prosedur dan kendali perpindahan yang resmi harus ada untuk melindungi perpindahan informasi melalui penggunaan semua jenis fasilitas komunikasi;

b. perjanjian perpindahan informasi, yaitu perjanjian harus mengatur perpindahan informasi yang aman antara perangkat daerah dan pihak luar;

c. pesan elektronik, yaitu informasi yang terdapat dalam pesan elektronik harus dilindungi dengan tepat; dan

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

Bagian Ketiga...

Bagian Ketiga

Pengelolaan Sumber Daya Keamanan Informasi

Paragraf 1

Umum

Pasal 18

(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 2

Pengelolaan Aset Keamanan Teknologi Informasi dan Komunikasi

Pasal 19

(1) Pengelolaan aset keamanan teknologi informasi dan komunikasi sebagaimana dimaksud dalam Pasal 18 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 20

(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 bersadarkan 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 21...

Pasal 21

(1) Bupati dibantu oleh 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 22

(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 dimaksud pada ayat (3) huruf a meliputi:

a. materil sandi;

b. tempat kegiatan sandi; dan

c. Alat Pendukung Utama (APU) persandian.

(5) Pemeliharaan aset keamanan teknologi informasi dan komunikasi sebagaimana dimaksud 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…

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 dimaksud pada ayat (3) huruf c dilakukan melalui perbaikan umum, yang merupakan perbaikan yang tidak berkaitan dengan aspek kriptografis, dilakukan oleh Dinas dengan berkoordinasi dengan BSSN.

(7) Pendistribusian aset keamanan teknologi informasi dan komunikasi sebagaimana dimaksud pada ayat (3) huruf d wajib memperhatikan ketentuan sebagai berikut:

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 dimaksud pada ayat (3) huruf e harus dilakukan secara menyeluruh, terus menerus, dan berkesinambungan.

Pasal 23

(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...

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 24

(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 23 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. pemindahtanganan; 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 25

(1) Penghapusan dari daftar barang milik Pemerintah Daerah terkait aset keamanan teknologi informasi dan komunikasi Pemerintah Daerah sebagaimana dimaksud dalam Pasal 23 ayat (4) huruf b dilakukan dalam hal barang milik daerah sudah beralih kepemilikannya, terjadi pemusnahan, atau karena sebab lain sesuai ketentuan peraturan perundang-undangan.

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

Pasal 26…

Pasal 26

Ketentuan lebih lanjut mengenai teknis pengelolaan aset keamanan teknologi informasi dan komunikasi yang meliputi perencanaan, pengadaan, pemanfaatan, dan penghapusan di lingkungan Pemerintah Daerah diatur oleh Kepala Dinas dengan berpedoman pada ketentuan peraturan perundang-undangan.

Paragraf 3

Pengelolaan Sumber Daya manusia

Pasal 27

(1) Dinas melakukan pengelolaan sumber daya manusia sebagaimana dimaksud dalam Pasal 18 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 karir;

c. pendayagunaan; dan

d. pemberian tunjangan pengamanan persandian.

Pasal 28

(1) Pengembangan kompetensi sebagaimana dimaksud dalam Pasal 27 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; dan

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

(2) Pembinaan karir sebagaimana dimaksud dalam Pasal 27 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...

(3) Pendayagunaan sebagaimana dimaksud dalam Pasal 27 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 27 ayat (2) huruf d diberikan sesuai ketentuan peraturan perundang-undangan.

Paragraf 4

Manajemen Pengetahuan

Pasal 29

(1) Dinas melakukan manajemen pengetahuan sebagaimana dimaksud dalam Pasal 18 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 sebagaimana dimaksud pada ayat (1), Dinas berkoordinasi dan dapat melakukan konsultasi dengan BSSN.

Pasal 30

(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…

(4) Pengumpulan pengetahuan dan teknologi yang dihasilkan dalam pelaksanaan keamanan informasi dilakukan melalui serangkaian proses untuk mengetahui aset pengetahuan yang dimiliki Pemerintah Daerah.

(5) Aset pengetahuan sebagaimana dimaksud pada ayat (4) dapat berupa produk/layanan, portofolio proyek, data, *database* kompentensi organisasi, literature (buku, majalah, laporan), dan sebagainya.

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

Pasal 31

(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 32

(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 33

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

(2) Terhadap hasil pengetahuan dan teknologi sebagaimana dimaksud pada ayat (1) dapat dilakukan aktivitas pengembangan dan penyempurnaan.

Pasal 34…

Pasal 34

(1) Kegiatan alih pengetahuan dan teknologi yang dihasilkan dalam pelaksanaan keamanan informasi dapat berlangsung secara manual 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 35

Ketentuan lebih lanjut mengenai teknis pelaksanaan manajemen pengetahuan yang meliputi proses pengumpulan, pengolahan, penyimpanan, penggunaan, dan alih pengetahuan dan teknologi yang dihasilkan dalam pelaksanaan keamanan informasi Pemerintah Daerah diatur oleh Kepala Dinas dengan berpedoman pada ketentuan peraturan perundang-undangan.

Bagian Keempat

Pengamanan Sistem Elektronik dan Pengamanan Informasi Nonelektronik

Pasal 36

Dinas melaksanakan pengamanan sistem elektronik dan pengamanan informasi nonelektronik sebagaimana dimaksud dalam Pasal 4 ayat (1) huruf c sesuai dengan ketentuan peraturan perundang-undangan.

Pasal 37

Pengamanan sistem elektronik sebagaimana dimaksud dalam Pasal 36 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 38

(1) Dalam melaksanakan pengamanan sistem elektronik sebagaimana dimaksud dalam Pasal 36, 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 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 39

(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 40...

Pasal 40

(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 mengenai teknis penyelenggaraan pusat operasi pengamanan informasi sebagaimana dimaksud pada ayat (1) di lingkungan Pemerintah Daerah diatur oleh Kepala Dinas dengan berpedoman pada ketentuan peraturan perundang-undangan.

Pasal 41

(1) Dalam mendukung pengamanan informasi nonelektronik sebagaimana dimaksud dalam Pasal 36 dilakukan pada tahapan pemrosesan, pengiriman, penyimpanan, dan pemusnahan informasi nonelektronik.

(2) Ketentuan lebih lanjut mengenai teknis pengamanan informasi nonelektronik sebagaimana dimaksud pada ayat (1) di lingkungan Pemerintah Daerah diatur oleh Kepala Dinas dengan berpedoman pada ketentuan peraturan perundang-undangan.

Pasal 42

(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 mengenai teknis pelaksanaan audit keamanan informasi sebagaimana dimaksud pada ayat (1) di lingkungan Pemerintah Daerah diatur oleh Kepala Dinas dengan berpedoman pada ketentuan peraturan perundang-undangan.

Bagian Kelima...

Bagian Kelima

Penyedia Layanan Keamanan Informasi

Pasal 43

(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 44

Jenis layanan keamanan informasi sebagaimana dimaksud dalam Pasal 43 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...

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 penginderaan;

o. konsultasi keamanan informasi bagi pengguna layanan; dan/atau

p. jenis layanan keamanan informasi lainnya.

Pasal 45

(1) Dalam menyediakan layanan keamanan informasi sebagaimana dimaksud dalam Pasal 44 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 mengenai teknis pelaksanaan manajemen layanan keamanan informasi sebagaimana dimaksud pada ayat (3) di lingkungan Pemerintah Daerah diatur oleh Kepala Dinas dengan berpedoman pada ketentuan peraturan perundang-undangan.

Pasal 46

Untuk mendukung penyediaan layanan keamanan informasi Pemerintah Daerah dibentuk Tim Tanggap Insiden Keamanan Komputer (*Computer Security Incident Response Team* Kabupaten Bogor) yang ditetapkan dengan Keputusan Bupati.

BAB IV

PENETAPAN POLA HUBUNGAN KOMUNIKASI SANDI ANTAR PERANGKAT DAERAH

Pasal 47

(1) Bupati melakukan penetapan pola hubungan komunikasi sandi antar perangkat daerah sebagaimana dimaksud dalam Pasal 3 huruf b.

(2) Penetapan..

(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 48

(1) Penetapan pola hubungan komunikasi sandi antar perangkat daerah sebagaimana dimaksud dalam Pasal 47 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...

a. pengguna layanan yang akan terhubung dalam jaring komunikasi sandi;

b. topologi atau bentuk 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 atau model 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 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 pada ayat (1) di lingkungan Pemerintah Daerah diatur oleh Kepala Dinas dengan berpedoman pada ketentuan peraturan perundang-undangan.

BAB V

PEMANTAUAN, EVALUASI, DAN PELAPORAN

Pasal 49

(1) Pemantauan dan evaluasi dilaksanakan terhadap penyelenggaraan persandian untuk pengamanan informasi dan penetepan 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 sebagai wakil Pemerintah Pusat.

Pasal 50...

Pasal 50

Ketentuan lebih lanjut mengenai teknis pemantauan, evaluasi, dan pelaporan terhadap penyelenggaraan persandian untuk pengamanan informasi dan penetapan pola hubungan komunikasi sandi antar perangkat daerah di lingkungan Pemerintah Daerah diatur oleh Kepala Dinas dengan berpedoman pada ketentuan peraturan perundang-undangan.

BAB VI

PEMBINAAN DAN PENGAWASAN TEKNIS

Pasal 51

(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 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 mengenai teknis pelaksanaan pembinaan dan pengawasan teknis terhadap perangkat daerah sebagaimana dimaksud pada ayat (2) ditetapkan oleh Kepala Dinas dengan berpedoman pada ketentuan peraturan perundang-undangan.

BAB VII

PENDANAAN

Pasal 52

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; dan/atau

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

BAB VIII...

BAB VIII

KETENTUAN PENUTUP

Pasal 53

Peraturan Bupati ini mulai berlaku pada tanggal diundangkan.

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

Ditetapkan di Cibinong
pada tanggal 6 Juli 2021
BUPATI BOGOR,

ttd

ADE YASIN

Diundangkan di Cibinong
pada tanggal 6 Juli 2021
SEKRETARIS DAERAH KABUPATEN BOGOR,

ttd

BURHANUDIN

BERITA DAERAH KABUPATEN BOGOR
TAHUN 2021 NOMOR 57

Salinan sesuai dengan aslinya
KEPALA BAGIAN
PERUNDANG-UNDANGAN,

HERISON