SALINAN

BUPATI PATI

PROVINSI JAWA TENGAH

PERATURAN BUPATI PATI

NOMOR 53 TAHUN 2021

TENTANG

SISTEM MANAJEMEN KEAMANAN INFORMASI PEMERINTAHAN BERBASIS ELEKTRONIK DI LINGKUNGAN PEMERINTAH KABUPATEN PATI

DENGAN RAHMAT TUHAN YANG MAHA ESA

BUPATI PATI,

Menimbang : a. bahwa dalam rangka melindungi kerahasiaan, keutuhan dan ketersediaan asset Informasi di Pemerintah Kabupaten Pati dari berbagai ancaman Keamanan Informasi baik dari dalam maupun luar, perlu melakukan pengelolaan Keamanan Informasi;

b. bahwa berdasarkan pertimbangan sebagaimana dimaksud huruf a, perlu menetapkan Peraturan Bupati tentang Sistem Manajemen Keamanan Informasi Pemerintahan Berbasis Elektronik di Lingkungan Pemerintah Kabupaten Pati;

Mengingat : 1. Undang-Undang Nomor 13 Tahun 1950 tentang Pembentukan Daerah-Daerah Kabupaten dalam Lingkungan Propinsi Jawa Tengah;

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...

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 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);
6. Undang-Undang Nomor 11 Tahun 2020 tentang Cipta Kerja (Lembaran Negara Republik Indonesia Tahun 2020 Nomor 245, Tambahan Lembaran Negara Republik Indonesia Nomor 6573);
7. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 185, Tambahan Lembaran Negara Republik Indonesia Nomor 6400);
8. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
9. Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi (Berita Negara Republik Indonesia Tahun 2016 Nomor 551);
10. Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elektronik;

11. Peraturan...

11. Peraturan Daerah Kabupaten Pati Nomor 12 Tahun 2016 tentang Urusan Pemerintahan Kabupaten Pati (Lembaran Daerah Kabupaten Pati Tahun 2016 Nomor 12, Tambahan Lembaran Daerah Kabupaten Pati Nomor 98);

MEMUTUSKAN :

Menetapkan : PERATURAN BUPATI TENTANG SISTEM MANAJEMEN KEAMANAN INFORMASI PEMERINTAHAN BERBASIS ELEKTRONIK DI LINGKUNGAN PEMERINTAH KABUPATEN PATI.

BAB I

KETENTUAN UMUM

Pasal 1

Dalam Peraturan Bupati ini yang dimaksud dengan :

1. Daerah adalah Kabupaten Pati.
2. Pemerintah Daerah adalah Bupati sebagai unsur penyelenggara Pemerintahan Daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan daerah otonom.
3. Bupati adalah Bupati Pati.
4. Sekretaris Daerah adalah Sekretaris Daerah Kabupaten Pati.
5. Perangkat Daerah adalah unsur pembantu Bupati dan Dewan Perwakilan Rakyat Daerah dalam penyelenggaraan urusan pemerintahan yang menjadi kewenangan daerah.
6. Dinas adalah Dinas Komunikasi dan Informatika Kabupaten Pati.
7. Aparatur Sipil Negara yang selanjutnya disingkat ASN adalah profesi bagi Pegawai Negeri Sipil dan pegawai pemerintah dengan perjanjian kerja yang bekerja pada instansi pemerintah.
8. Data adalah catatan atas kumpulan fakta yang belum diolah dan apa adanya.

9. Admin...

9. Admin Keamanan Informasi adalah pejabat struktural atau staf yang menangani Teknologi Informasi pada Perangkat Daerah.
10. 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.
11. Sistem Informasi adalah sistem yang menyajikan Informasi elektronik menggunakan Teknologi telematika.
12. Teknologi Informasi adalah suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan/atau menyebarkan Informasi.
13. Komputer adalah alat untuk memproses data elektronik, mengetik atau sistem yang melaksanakan fungsi logika, aritmatika dan menyimpan.
14. Aplikasi adalah program Komputer yang dibangun untuk membantu proses pekerjaan.
15. Perangkat Lunak (*Software*) adalah satu atau sekumpulan program Komputer, prosedur dan/atau dokumentasi yang terkait dalam pengoperasian sistem elektronik.
16. Perangkat Keras (*Hardware*) adalah peralatan fisik dan rangkaian sistem dari Jaringan Komputer.
17. File adalah kumpulan dari data dan Informasi yang saling berhubungan dan juga tersimpan di dalam ruang penyimpanan sekunder.

18. *Hard disk*...

18. *Hard Disk* adalah salah satu komponen perangkat keras (*hardware*) pendukung Komputer atau laptop yang menyediakan ruang untuk menyimpan data atau output dari proses data yang dilakukan oleh Komputer dan manusia.
19. Kartu Memori adalah sebuah alat penyimpan data digital.
20. *Filling Cabinet* adalah sebuah lemari khusus yang terbuat dari bahan logam dan berukuran tegak seperti lemari.
21. *Database* adalah kumpulan data yang secara logika berkaitan satu sama lain dan disimpan atau diakses berbasiskan Komputer.
22. *Website* adalah kumpulan halaman web yang dapat diakses publik dan saling terkait yang berbagi satu nama domain.
23. Prosedur adalah rangkaian langkah atau kegiatan yang saling berhubungan satu sama lain secara esensial yang diikuti pendekatan fungsional.
24. Keamanan Informasi adalah perlindungan aset Informasi dari berbagai bentuk ancaman untuk memastikan kelangsungan kegiatan, menjamin kerahasiaan, keutuhan dan ketersediaan aset Informasi.
25. Sistem Manajemen Keamanan Informasi Pemerintahan Berbasis Elektronik adalah pengaturan kewajiban bagi penyelenggara sistem elektronik demi terjaganya kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*) Informasi pada layanan pemerintah.
26. Aset Informasi adalah unit Informasi yang dapat dipahami, dibagi, dilindungi dan dimanfaatkan secara efektif.
27. Aset Pengolahan Informasi adalah suatu perangkat baik elektronik maupun non-elektronik yang dapat digunakan untuk membuat dan menyunting Informasi.
28. Penyimpanan Informasi adalah suatu proses menyimpan Informasi dengan menggunakan media baik elektronik maupun non-elektronik.

29. Telekomunikasi...

29. Telekomunikasi adalah setiap pemancaran, pengiriman dan/atau penerimaan dari setiap Informasi dalam bentuk tanda-tanda, isyarat, tulisan, gambar, suara bunyi melalui kawat, optik, radio atau sistem elektromagnetik lainnya.
30. Pusat Data adalah suatu fasilitas yang digunakan untuk menempatkan sistem elektronik dan komponen terkaitnya untuk keperluan penempatan, penyimpanan, dan pengolahan data.
31. Tim Respon Insiden Keamanan Informasi (*Computer Security Incident Response Team*) adalah tim yang bertanggung jawab untuk menerima, meninjau dan menanggapi laporan dan aktifitas insiden Keamanan Teknologi Informasi.
32. Risiko adalah peluang terjadinya suatu peristiwa yang akan mempengaruhi keberhasilan terhadap pencapaian tujuan.
33. Manajemen Risiko adalah pendekatan sistematis yang meliputi proses, pengukuran, struktur, dan budaya untuk menentukan tindakan terbaik terkait risiko.
34. *Sistem Development Life Cycle* (SDLC) adalah proses pembuatan dan pengubahan sistem serta model dan metodologi yang digunakan untuk mengembangkan sistem.
35. *Username* adalah nama yang menjadi indentitas pengguna Komputer atau internet, bagian dari syarat pembuatan sebuah *account*.
36. *Password* adalah sandi yang harus dimasukan kedalam suatu sistem baik itu sistem Komputer yang menggunakan sistem operasi *windows* atau bukan yang berupa karakter tulisan, suara, atau ciri-ciri khusus yang harus diingat.
37. *Interoperabilitas* adalah dimensi suatu *Aplikasi* bisa berintaraksi dengan *Aplikasi* lainnya melalui protokol yang disetujui bersama lewat bermacam-macam jalur komunikasi.
38. *Sitemap* adalah sebuah peta yang berisi berbagai macam direktori yang terdapat dalam sebuah *Website/blog*.

39. *Closed...*

39. *Closed Circuit Television* yang selanjutnya disingkat CCTV adalah seperangkat kamera video digital yang berfungsi untuk memantau kondisi di suatu tempat tertentu.
40. *Backup Site* adalah proses membuat data cadangan dengan cara menyalin atau membuat arsip data Komputer sehingga data tersebut dapat digunakan kembali apabila terjadi kerusakan atau kehilangan.
41. Pusat Pemulihan Bencana *(Disaster recovery center)* adalah sebuah tempat yang ditujukan untuk menempatkan perangkat IT, sistem, *Aplikasi* dan data cadangan untuk persiapan menghadapi bencana yang diperlukan oleh perusahaan besar dan organisasi pemerintahan.

BAB II

MAKSUD DAN TUJUAN

Pasal 2

(1) Maksud ditetapkannya Peraturan Bupati ini adalah untuk terciptanya sistem pengendalian keamaman yang terpadu dan menjamin keberlangsungan Sistem Manajemen Keamanan Informasi Pemerintahan Berbasis Elektronik dengan meminimalkan dampak risiko Keamanan Informasi.

(2) Tujuan ditetapkannya Peraturan Bupati ini adalah untuk :

a. memberikan landasan hukum dalam penerapan Sistem Manajemen Keamanan Informasi Pemerintahan Berbasis Elektronik di lingkungan Pemerintah Daerah.

b. memberikan pedoman dalam hal pengelolaan Sistem Manajemen Keamanan Informasi secara terpadu untuk memastikan terjaganya kerahasiaan *(confidentiality*), keutuhan *(integrity*) dan ketersediaan *(availability*).

BAB III

RUANG LINGKUP

Pasal 3

Ruang Lingkup Peraturan Bupati ini meliputi :

a. pengamanan Informasi;
b. standar sistem manajemen.

BAB IV

PENGAMANAN INFORMASI

Pasal 4

Pengamanan Informasi meliputi :

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

Pasal 5

(1) Aset Informasi sebagaimana dimaksud dalam Pasal 4 huruf a merupakan aset dalam bentuk :
    a. fisik, meliputi Informasi yang tercetak, tertulis dan tersimpan dalam bentuk fisik seperti di atas kertas, papan tulis, spanduk, atau di dalam buku dan dokumen.
    b. elektronik, meliputi Informasi tercetak, tertulis dan tersimpan dalam bentuk elektronik seperti Database, pada file di dalam Komputer, ditampilkan pada *Website*, layar Komputer dan dikirimkan melalui Jaringan Telekomunikasi.
(2) Aset Pengolahan Informasi sebagaimana dimaksud dalam Pasal 4 huruf b berupa :
    a. pengolahan peralatan mekanik yang digerakkan dengan tangan secara manual;
    b. pengolahan peralatan elektronik yang bekerja secara elektronik penuh.
(3) Penyimpanan Informasi sebagaimana dimaksud dalam Pasal 4 huruf c menggunakan media :
    a. elektronik, meliputi antara lain *server*, *Hard Disk*, *flash disk*, Kartu Memori dan lain-lain.

b. non-elektronik...

b. non-elektronik, meliputi antara lain lemari, rak, laci, *filling cabinet* dan lain-lain.

BAB V

STANDAR SISTEM MANAJEMEN

Bagian Kesatu

Koordinator Keamanan Informasi

Pasal 6

(1) Koordinator Keamanan Informasi bertanggung jawab memastikan Teknologi Informasi yang digunakan untuk mendukung proses tata kelola pemerintahan dan pencapaian tujuan organisasi.

(2) Koordinator Keamanan Informasi sebagaimana dimaksud pada ayat (1) memiliki wewenang :
   a. menyusun prosedur penyelenggaraan Keamanan Informasi yang diterapkan secara efektif baik bagi Perangkat Daerah maupun pengguna;
   b. melakukan evaluasi kinerja penyelenggaraan Keamanan Informasi.

(3) Koordinator Keamanan Informasi wajib mengidentifikasi dan memantau aktivitas operasional Teknologi Informasi untuk memastikan efektifitas, efisiensi, dan Keamanan dari aktivitas tersebut antara lain dengan :
   a. menerapkan parameter fisik dan lingkungan di area kerja dan pusat data;
   b. mengendalikan hak akses secara memadai sesuai kewenangan yang ditetapkan;
   c. menerapkan pengendalian terhadap Informasi yang diproses;
   d. memastikan ketersediaan dan kecukupan kapasitas layanan Jaringan komunikasi baik yang dikeloa secara internal maupun oleh pihak lain penyedia jasa;
   e. melakukan pemantauan kegiatan operasional;
   f. melakukan pemantauan terhadap Aplikasi yang digunakan oleh Perangkat Daerah maupun pengguna.

(4) Koordinator…

(4) Koordinator Keamanan Informasi sebagaimana dimaksud pada ayat (1) adalah Kepala Dinas.

Bagian Kedua

Admin Keamanan Informasi

Pasal 7

(1) Untuk mendukung tugas Keamanan Informasi koordinator membentuk Tim Respon Insiden Keamanan Informasi (*Computer Security Incident Response Team*).

(2) Tim Respon Insiden Keamanan Informasi (*Computer Security Incident Response Team*) sebagaimana dimaksud pada ayat (1) diketuai oleh Kepala Dinas.

(3) Keanggotaan Tim Respon Insiden Keamanan Informasi (*Computer Security Incident Response Team*) sebagaimana dimaksud pada ayat (1) meliputi :
   a. ASN yang membidangi Teknologi Informasi pada Dinas; dan
   b. Admin Keamanan Informasi.

(4) Admin Keamanan Informasi sebagaimana dimaksud pada ayat (3) terdiri dari :
   a. ASN Daerah; dan/atau
   b. Tenaga ahli di bidang Teknologi Informasi;

(5) Admin Keamanan Informasi memiliki tugas mengoperasikan, mengelola, mengendalikan dan menyimpan seluruh Aset Teknologi Informasi.

(6) Admin Keamanan Informasi wajib :
   a. mematuhi seluruh kebijakan dan prosedur Perangkat Daerah terkait Keamanan Informasi;
   b. membangun kesadaran Keamanan Informasi dan keberlangsungan sistem serta kenyamanan dalam menggunakan Teknologi Informasi dan komunikasi pada lingkungan Pemerintah Daerah.

(7) Apabila terjadi pemberhentian dan/atau pergantian Admin Keamanan Informasi maka admin Keamanan Informasi wajib :
   a. mengembalikan seluruh aset organisasi;
   b. menonaktifkan atau menghapus seluruh hak akses organisasi; dan
   c. menyesuaikan seluruh hak akses organisasi.

Bagian…

Bagian Ketiga

Manajemen Risiko

Pasal 8

(1) Setiap Perangkat Daerah penyelenggara Teknologi Informasi wajib melakukan proses Manajemen Risiko dalam menerapkan Sistem Manajemen Keamanan Informasi.

(2) Proses Manajemen Risiko sebagaimana dimaksud pada ayat (1) meliputi :
   a. identifikasi;
   b. pengukuran;
   c. pemantauan; dan
   d. pengendalian atas Risiko terkait penggunaan Teknologi Informasi.

(3) Manajemen Risiko sebagaimana dimaksud pada ayat (2) mencakup :
   a. pengembangan sistem;
   b. operasional Teknologi Informasi;
   c. Jaringan komunikasi;
   d. penggunaan perangkat Komputer;
   e. pengendalian terhadap Informasi; dan
   f. penggunaan pihak ketiga sebagai penyedia jasa Teknologi Informasi.

(4) Penerapan Manajemen Risiko harus dilakukan secara terintegrasi pada setiap penggunaan operasional Teknologi Informasi terkait sistem yang digunakan.

Bagian Keempat

Sumber Daya Manusia

Pasal 9

Setiap Perangkat Daerah menyediakan sumber daya manusia yang dibutuhkan untuk membentuk, mengimplementasikan, memelihara dan meningkatkan penerapan Sistem Manajemen Keamanan Informasi secara berkesinambungan.

Bagian…

Bagian Kelima

Aspek Keamanan Sistem

Pasal 10

(1) Setiap operasi sistem Teknologi Informasi harus memperhatikan persyaratan minimal aspek Keamanan sistem, keberlangsungan sistem, terutama sistem Teknologi Informasi dan komunikasi yang memfasilitasi layanan kritikal.

(2) Aspek Keamanan sebagaimana dimaksud pada ayat (1) menerapkan prinsip sebagai berikut :
   a. *confidentiality*, yaitu akses terhadap data/Informasi dibatasi hanya bagi mereka yang punya otoritas.
   b. *integrity,* data tidak boleh berubah tanpa izin dari yang berhak.
   c. *authentication,* identitas pengguna sistem harus diketahui; dan
   d. *availability,* yaitu ketersediaan layanan.

(3) Aspek Keamanan sebagaimana dimaksud pada ayat (2) mencakup 2 (dua) area, yaitu :
   a. Keamanan Informasi secara fisik; dan
   b. Keamanan Informasi secara logika.

(4) Keamanan Informasi secara fisik sebagaimana dimaksud pada ayat (3) huruf a merupakan upaya perlindungan terhadap sistem organisasi/instansi dalam serangan secara fisik meliputi :
   a. mesin Aplikasi;
   b. ruangan mesin; dan
   c. gedung/tempat mesin.

(5) Keamanan Informasi secara fisik sebagaimana dimaksud pada ayat (3) huruf a juga termasuk mengamankan saluran komunikasi melalui kabel ataupun melalui gelombang (*wireless*) dari usaha penyadapan dan kerusakan.

(6) Keamanan Informasi secara logika sebagaimana dimaksud pada ayat (3) huruf b merupakan perlindungan terhadap data/Informasi yang penting dan sensitif agar tidak dapat diakses oleh pihak-pihak yang tidak berhak.

(7) Keamanan…

(7) Keamanan Informasi secara logika sebagaimana dimaksud pada ayat (3) huruf b dimulai dari mendesain Aplikasi, membuat alur proses hingga sistem penyimpanan yang dibuat sedemikian rupa.

(8) Program Aplikasi *dan Website* yang dibangun oleh Perangkat Daerah atau bekerjasama dengan pihak ketiga wajib memenuhi persyaratan antara lain :

a. program Aplikasi *dan Website* harus dibuat oleh orang atau badan yang memiliki pengalaman yang berhubungan dengan pembuatan Aplikasi *dan Website* yang dibuktikan dengan portofolio (hasil kerja yang pernah dibuat);
b. pembuat program Aplikasi *dan Website* bisa dilakukan oleh ASN atau non ASN sepanjang memenuhi kriteria yang telah ditetapkan.
c. hasil rekomendasi kelayakan yang dikeluarkan oleh Dinas.

(9) Program Aplikasi *dan Website* wajib memenuhi perjanjian yang mengikat antara Perangkat Daerah dengan pihak ketiga dengan ketentuan sebagai berikut :

a. dokumen perjanjian masa pemeliharaan program Aplikasi atau Website dari pihak ketiga minimal 1 (satu) tahun;
b. untuk pemeliharaan tahun berikutnya dapat diterbitkan perjanjian baru sesuai kebutuhan;
c. pihak ketiga wajib berkoordinasi dengan ASN yang ditunjuk sebagai penanggung jawab keberlangsungan program Aplikasi *dan Website* demi terjaganya Keamanan dan keberlangsungan program Aplikasi *dan Website* demi terjaganya Keamanan dan keberlangsungan sistem;
d. selama masa pemeliharaan semua Risiko dan tanggung jawab atas keberlangsungan program Aplikasi *dan Website* menjadi tanggung jawab pihak ketiga;

e. berita…

e. berita acara serah terima program Aplikasi *dan Website* yang memuat data diri orang dan badan pembuat program Aplikasi *dan Website* dengan melampirkan :
   1) tanda bukti kompetensi orang atau badan pembuat aplikasi atau *Website*;
   2) perjanjian masa pemeliharaan;
   3) perjanjian Risiko hukum jika terjadi pengingkaran perjanjian;
   4) kwitansi pembayaran pembuatan Aplikasi *atau Website*;
   5) hasil rekomendasi kelayakan yang dikeluarkan oleh Dinas;
   6) pernyataan bersedia melakukan penyeragaman tampilan (*layout*) *Website*.

(10) Program Aplikasi *dan Website* yang dibangun dan dikembangkan oleh Perangkat Daerah wajib dapat dioperasionalkan dalam JaringanPemerintah Daerah dengan mempertimbangkan prinsip *interoperabilita*s.

(11) Setiap perangkat lunak (software)/program *Aplikasi* harus selalu menyertakan prosedur *recovery* serta mengimplementasikan fungsinya di dalam Perangkat Lunak (*software)*/program Aplikasi.

(12) Setiap pembuatan dan pengembangan program Aplikasi harus dilengkapi dengan :
   a. dokumen hasil aktivitas tahapan-tahapan dalam *System Dovelopment Life Cycle* (SDLC);
   b. admin *credential* (username dan password);
   c. bisnis proses Aplikasi;
   d. *sitemap* (struktur desain) Aplikasi ataupun *Website*;
   e. *source code* (kode sumber) Aplikasi yang telah final dan dapat di buktikan dengan berfungsinya *Aplikasi*;
   f. manual pengguna, operasi, dukungan teknis dan administrasi materi transfer pengetahuan dan materi training;
   g. laporan hasil *assesment* Risiko dari Dinas, Badan Siber dan Sandi Negara.

Bagian...

Bagian Keenam

Kontrol Manajemen Sistem Keamanan Informasi

Pasal 11

Kontrol manajemen sistem Keamanan Informasi dilaksanakan sesuai ketentuan peraturan perundang-undangan.

Pasal 12

(1) *Autentikasi* dalam Teknologi dan Informasi merupakan proses konfirmasi keabsahan penggguna (*user*) sesuai dengan yang terdapat dalam Database.
(2) Dalam *otentifikasi* sebagaimana dimaksud pada ayat (1) terdapat 3 (tiga) jenis yaitu :
    a. *Username* dan *password*;
    b. kunci algoritma, sandi, dan *smart card*; dan
    c. *biometric*, seperti sidik jari, pola suara dan *deoxyribonucleic acid* (DNA).

Pasal 13

(1) Otorisasi merupakan pengecekan kewenangan pengguna (user) dalam mengakses sumber daya yang diminta.
(2) Dalam otorisasi sebagaimana dimaksud pada ayat (1) terdapat 2 (dua) metode dasar yaitu :
    a. daftar pembatasan akses *(access control list); dan*
    b. daftar kemampuan *(capability list)*.
(3) Daftar pembatasan akses (*access control list*) sebagaimana dimaksud pada ayat (2) huruf a berisi daftar pengguna (*user*) dengan masing-masing tugas/kewenangan terhadap sumber daya sistem.
(4) Daftar kemampuan (*capability list*) sebagaimana dimaksud pada ayat 2 (dua) huruf b ditekankan pada masing-masing tugas/kewenangan terhadap sumber daya sistem.

Bagian Ketujuh

Pemeliharaan

Pasal 14

(1) Perangkat Daerah wajib melakukan pemeliharaan terhadap Sistem Informasi.
(2) Pemeliharaan sebagaimana dimaksud pada ayat (1) mencakup :
    a. pemeliharaan Perangkat Keras (*Hardware*);

b. pemeliharaan...

b. pemeliharaan Perangkat Lunak (*software*);
c. pemeliharaan lain untuk menghilangkan gangguan kinerja Jaringan Komputer.

(3) Untuk kelancaran dan kesinambungan Sistem Informasi, setiap Perangkat Daerah wajib memutakhirkan Perangkat Keras (*Hardware*) dan pemeliharaan Perangkat Lunak (*Software*) sesuai dengan kebutuhan dan kemajuan Teknologi.

(4) Setiap Perangkat Daerah berkewajiban mengadakan pemeliharaan dan pengamanan terhadap keberadaan Perangkat Keras (*Hardware*) dan Perangkat Lunak (*Software*) yang ada di masing-masing Perangkat Daerah.

(5) Setiap Perangkat Daerah bertanggung jawab dalam memastikan kegiatan operasional Teknologi Informasi yang stabil dan aman.

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

Bagian Kedelapan

Pusat Data

Pasal 15

(1) Ketersediaan data dan sistem dalam rangka menjaga kelangsungan Teknologi Informasi melalui penyelenggaraan fasilitas Pusat Data baik yang dikelola oleh internal maupun oleh pihak penyedia jasa harus dipastikan oleh Dinas sebagai koordinator Keamanan Informasi di Pemerintah Daerah.

(2) Setiap aktivitas pada fasilitas di Pusat Data harus terpantau guna menghindari kesalahan proses pada sistem dan memperhatikan aspek perlindungan terhadap data yang diproses dan lingkungan fisik.

Pasal 16

(1) Pemerintah Daerah wajib memiliki Pusat Data yang terintegrasi dan Pusat Pemulihan Bencana (*disaster recovery center*).

(2) Pusat data dan Pusat Pemulihan Bencana (*disaster recovery center*) sebagaimana dimaksud pada ayat 1 (satu) wajib ditempatkan di wilayah Pemerintah Daerah.

(3) Pusat…

(3) Pusat data dan Pusat Pemulihan Bencana (*disaster recovery center*) sebagaimana dimaksud pada ayat (2) dikelola oleh Dinas sebagai koordinator Keamanan Informasi di Pemerintah Daerah.

(4) Setiap Perangkat Daerah wajib memiliki backup data untuk megembalikan data yang ada apabila terjadi gangguan.

Bagian Kesembilan

Aspek Pengamanan Fisik

Pasal 17

Pengamanan fisik dan lingkungan bagi area kerja, penyimpanan perangkat pengolahan serta Informasi, seperti Pusat Data, Pusat Pemulihan Bencana (*disaster recovery center*), atau ruang arsip harus dilakukan oleh Perangkat Daerah.

Pasal 18

Setiap area yang didalamnya terdapat Informasi dan fasilitas pengolahan Informasi Perangkat Daerah, harus dilindungi dengan menerapkan pengamanan fisik pada parameter area tersebut.

Pasal 19

(1) Setiap area sebagaimana dimaksud dalam Pasal 18 harus merupakan akses terbatas.

(2) Akses terbatas sebagaimana dimaksud pada ayat (1) hanya diberikan bagi orang yang telah mendapatkan otorisasi.

(3) Otorisasi sebagaimana dimaksud pada ayat (2) diterapkan oleh Dinas.

Pasal 20

Area Pusat Data, Pusat Pemulihan Bencana (*disaster recovery center*)dan ruang arsip Perangkat Daerah harus dilindungi dengan menerapkan pengamanan fisik pada parameter area tersebut dengan kriteria :

a. konstruksi dinding, atap dan lantai yang kuat;
b. pintu akses menuju area harus dilengkapi dengan mekanisme kontrol akses seperti *access door lock*;
c. pintu dan jendela harus senantiasa dalam kondisi terkunci, khususnya pada saat tanpa penjagaan;
d. perangkat CCTV perlu terpasang pada sisi eksterior dan interior area;

e. tidak...

e. tidak diperbolehkan menyimpan bahan-bahan berbahaya yang mudah terbakar;
f. area bongkar muat atau penerimaan barang harus diamankan dan dipantau untuk mencegah akses tanpa izin ke Pusat Data, Pusat Pemulihan Bencana (*disaster recovery center*) dan ruang arsip Pemerintah Daerah; dan
g. keadaan barang harus dilaporkan dan diperiksa sebelum barang tersebut dapat dipindahkan dari area bongkar muat atau penerimaan barang ke Pusat Data, Pusat Pemulihan Bencana (*disaster recovery center*), dan ruang arsip Pemerintah Daerah.

Pasal 21

Setiap Perangkat Daerah harus memperhatikan aspek pengamanan fisik terhadap Perangkat yang digunakan melalui :

a. seluruh perangkat harus ditempatkan di lokasi yang aman, sedemikian rupa sehingga terlindungi dari terjadinya pencurian, akses oleh pihak tidak berwenang, air, debu dan sebagainya;
b. seluruh perangkat di dalam area harus dipelihara, diinspeksi sesuai spesifikasi perawatan berkala oleh pihak yang berwenang untuk menjamin keberlangsungan efektivitas fungsionalnya;
c. pemeliharaan yang dilakukan oleh pihak ketiga harus dilaksanakan sesuai dengan kesepakatan tingkat layanan (*service level agreement*/SLA) yang menjabarkan tingkat pemeliharaan dan kinerja yang harus dipenuhi pihak ketiga;
d. bagi pemeliharaan yang tidak dapat dilakukan di lokasi kantor Perangkat Daerah, maka Informasi rahasia dan kritikal yang tersimpan dalam peralatan tersebut harus dipindahkan terlebih dahulu;
e. pemeliharaan perangkat yang mengharuskan dibawa keluar area harus mendapat persetujuan dari Kepala Perangkat Daerah;
f. peralatan pengolahan dan Penyimpanan Informasi yang tidak digunakan lagi oleh Pemerintah Daerah, baik karena rusak, diganti, atau karena sebab lainnya harus dipastikan tidak lagi menyimpan Informasi sensitif dan kritikal; dan

g. media...

g. media Penyimpanan Informasi yang sudah tidak digunakan lagi harus dihancurkan atau dihapus isinya agar tidak digunakan oleh pihak lain yang tidak berwenang.

Pasal 22

Khusus pengamanan area fisik di Pusat Data harus mempertimbangkan hal-hal sebagai berikut :

a. seluruh perangkat harus ditempatkan di lokasi yang aman sedemikian rupa sehingga terlindungi dari terjadinya kebakaran, kebocoran, debu dan sebagainya;
b. seluruh perangkat di dalam Pusat Data harus dipelihara, diinspeksi sesuai spesifikasi perawatan berkala oleh pihak yang kompeten dan berwenang sesuai dengan rekomendasi dari pembuat perangkat tersebut;
c. Pusat Data harus dilengkapi dengan *Uninterruptible Power Supply*, genarator listrik cadangan, perangkat pemadam kebakaran dan diusahakan terdapat perlindungan listrik;
d. Pusat Data, Pusat Pemulihan Bencana (*disaster recovery center*) dilengkapi dengan sistem sensor deteksi asap, air, suhu dan kelembaban, yang dapat terpantau;
e. parameter temperatur dan kelembaban berikut perlu dijaga untuk Pusat Data meliputi :
   1. temperatur antara 18˚-26˚ celcius;
   2. kelembaban antara 40%-60%;
f. kabel listrik dan Jaringan telekomunikasi yang membawa data atau mendukung layanan Sistem Informasi harus dilindungi dari penyambungan yang yang tidak sah (penyadap) atau kerusakan.

Bagian Kesepuluh

Penanganan Insiden

Pasal 23

Penanganan insiden dalam sistem Keamanan Informasi harus dilakukan untuk memastikan adanya pendekatan yang konsisten dan efektif sehingga dapat terindentifikasi kelemahan yang ada pada sistem, layanan dan Jaringanyang dapat menimbulkan gangguan terhadap operasional bisnis dan mengancam sistem Keamanan Informasi.

Pasal...

Pasal 24

Proses penanganan insiden meliputi tahapan :

a. perencanaan dan persiapan penangan insiden;
b. pemantauan analisis dan pelaporan atas insiden;
c. pencatatan atas aktivitas penanganan insiden;
d. penanganan bukti forensik;
e. penilaian dan pengambilan keputusan atas insiden dan kelemahan Keamanan Informasi; dan
f. pemulihan insiden.

Pasal 25

(1) Setiap kejadian insiden Keamanan Informasi harus dianalisis dan diklasifikasikan.
(2) Penanganan insiden sebagaimana dimaksud pada ayat (1) dilakukan berdasarkan klasifikasi dan prioritas yang telah ditetapkan.
(3) Setiap insiden Keamanan Informasi harus ditangani dengan baik untuk mencegah meluasnya insiden, memulihkan layanan atau Informasi yang mungkin hilang dan meminimalisasi dampak dari insiden.
(4) Setiap tindakan yang diidentifikasi untuk menangani kejadian untuk menangani kelemahan dan insiden Keamanan Informasi harus dikonsultasikan kepada koordinator Keamanan sistem Informasi.
(5) Setiap tindakan penangan kejadian, kelemahan dan insiden Keamanan Informasi harus didokumentasikan dengan baik.

Bagian Kesebelas

Backup Site

Pasal 26

(1) Guna menjamin ketersediaan layanan serta Keamanan Informasi dalam kondisi darurat/bencana alam pada lokasi utama, perlu adanya redudansi terhadap fasilitas pengolahan Informasi yang disebut sebagai fasilitas *Backup Site*.
(2) *Backup Site* sebagaimana dimaksud dalam ayat (1) dapat berupa lokasi kerja pengganti atau Pusat Pemulihan Bencana (*disaster recovery center*) bagi alternatif area Pusat Data.

Pasal 27

Ketentuan dalam pengelolaan terkait *Backup Site* meliputi :

a. *Backup Site* secara geografis memiliki probabilitas kejadian bencana alam yang minimal;

b. *Backup*...

b. *Backup Site* ditunjukkan sebagai media penyimpanan backup alternatif, serta sebagai fasilitas pengolahan Informasi alternatif;
c. Pengelolaan *Backup Site* serta pemilik aset Informasi melakukan uji keberlangsungan secara berkala di bawah koordinasi penanggung jawab kelangsungan bisnis, minimal 1 (satu) kali dalam setahun, untuk menguji kesiapan seluruh pihak dalam hal :
   1. memindahkan operasional ke fasilitas *Backup Site;*
   2. memulihkan operasional Aplikasi beserta data sistem Keamanan Informasi.

Bagian Kedua Belas

Audit Keamanan Informasi

Pasal 28

(1) Pelaksanaan audit dan pemeliharaan pada sistem Keamanan Informasi pemerintahan berbasis elektronik di Daerah dilakukan minimal 1 (satu) kali dalam 1 (satu) tahun.
(2) Audit sebagaimana dimaksud pada ayat (1) dilakukan oleh Dinas.
(3) Dalam melaksanakan audit sebagaimana dimaksud pada ayat (2) Dinas berkoordinasi dengan Badan Siber dan Sandi Negara (BSSN).

BAB VI

KETENTUAN PERALIHAN

Pasal 29

Seluruh *Aplikasi dan Website* yang dibuat sebelum diundangkannya Peraturan Bupati ini harus disesuaikan dalam jangka waktu 1 (satu) tahun setelah Peraturan Bupati ini diundangkan.

Pasal 30

Tim Respon Insiden Keamanan Informasi (*Computer Security Incident Response Team*) yang telah terbentuk dinyatakan tetap berlaku.

BAB VII

KETENTUAN PENUTUP

Pasal 31

Peraturan Bupati ini mulai berlaku pada tanggal diundangkan.

Agar...

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

Ditetapkan di Pati
pada tanggal 29 September 2021

BUPATI PATI,

Ttd.

HARYANTO

Diundangkan di Pati
pada tanggal 29 September 2021

SEKRETARIS DAERAH KABUPATEN PATI,

Ttd.

SUHARYONO

BERITA DAERAH KABUPATEN PATI TAHUN 2021 NOMOR 53

Salinan sesuai dengan aslinya
KEPALA BAGIAN HUKUM

PEMERINTAH KABUPATEN PATI
SETDA

IRWANTO, SH., MH.
Pembina
NIP. 19670911 198607 1 001