SALINAN

BERITA DAERAH KABUPATEN LABUHANBATU
NOMOR 28 TAHUN 2018

BUPATI LABUHANBATU
PROVINSI SUMATERA UTARA

PERATURAN BUPATI LABUHANBATU
NOMOR 28 TAHUN 2018
TENTANG
SISTEM MANAJEMEN KEAMANAN INFORMASI
PEMERINTAHAN BERBASIS ELEKTRONIK DI LINGKUNGAN
PEMERINTAH KABUPATEN LABUHANBATU

DENGAN RAHMAT TUHAN YANG MAHA ESA

BUPATI LABUHANBATU

Menimbang : a. bahwa globalisasi teknologi informasi dan komunikasi telah melahirkan sistem pemerintahan berbasis elektronik (*electronic government*) yang bertujuan untuk meningkatkan penyelenggaraan pemerintahan yang baik, transparan, efektif, efisien, dan akuntabel;

b. bahwa dengan adanya penggunaan dan pemanfaatan teknologi informasi, dan komunikasi berbasis elektronik di lingkungan Pemerintahan Kabupaten Labuhanbatu perlu ditata sistem manajemen keamanan informasi pemerintahan berbasis elektronik;

c. bahwa berdasarkan pertimbangan sebagaimana dimaksud pada huruf a dan huruf b, perlu menetapkan Peraturan Bupati tentang Sistem Manajemen Keamanan Informasi Pemerintahan Berbasis Elektronik Di Lingkungan Pemerintah Kabupaten Labuhanbatu;

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

2. Undang-Undang Nomor 7 Drt Tahun 1956 tentang Pembentukan Daerah Otonom Kabupaten- Kabupaten Dalam Lingkungan Daerah Propinsi Sumatera Utara (Lembaran Negara Republik Indonesia Tahun 1956 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 1092);

3. Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi (Lembaran Negara Republik Indonesia Tahun 1999 Nomor 154, Tambahan Lembaran Negara Republik Indonesia Nomor 3881);

4. 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);

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. Undang-Undang Nomor 30 Tahun 2014 tentang Administrasi Pemerintahan (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 292, Tambahan Lembaran Negara Republik Indonesia Nomor 5601);

7. Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2012 Nomor 189, Tambahan Lembaran Negara Republik Indonesia Nomor 5348);

8. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik;

9. Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016

tentang Sistem Manajemen Pengamanan Informasi (Berita Negara Republik Indonesia Tahun 2016 Nomor 551);

MEMUTUSKAN:

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

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Bupati ini yang dimaksud dengan:

1. Daerah adalah Kabupaten Labuhanbatu.
2. Pemerintahan Daerah adalah penyelenggaraan urusan pemerintahan oleh pemerintah daerah dan Dewan Perwakilan Rakyat Daerah menurut asas otonomi dan tugas pembantuan dengan prinsip otonomi seluas-luasnya dalam sistem dan prinsip Negara Kesatuan Republik Indonesiase bagaimana dimaksud dalam Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.
3. Perangkat daerah adalah unsur pembantu kepala daerah dan Dewan Perwakilan Rakyat Daerah dalam penyelenggaraan urusan pemerintahan yang menjadi kewenangan daerah.

4. Dinas adalah Dinas Komunikasi dan Informatika Kabupaten Labuhanbatu.

5. Aparatur Sipil Negara yang selanjutnya disingkat ASN adalah profesi bagi pegawai negeri sipil dan pegawai pemerintah dengan perjanjian kerja yang bekerja pada instansi pemerintah.

6. Keamanan informasi adalah terjaganya kerahasiaan (*confidentiality*), keutuhan *(integrity)* dan ketersediaan (*availability)* informasi.

7. Prosedur adalah rangkaian langkah atau kegiatan yang saling berhubungan satu sama lain secara esensial yang diikuti pendekatan fungsional.

8. Sistem Pemerintahan Berbasis Elektronik (*Electronic Government*) yang selanjutnya disebut *e-Government* adalah penggunaan teknologi informasi dan komunikasi untuk meningkatkan efisiensi, efektivitas, transparansi, dan akuntabilitas layanan pemerintahan.

9. Sistem Manajemen Keamanan Informasi Pemerintahan Berbasis Elektronik adalah pengaturan kewajiban bagi penyelenggara sistem elektronik demi terjaganya kerahasiaan, keutuhan dan ketersediaan informasi pada layanan pemerintahan.

10. Perangkat keras (*hardware*) adalah peralatan fisik dan rangkaian sistem dari jaringan komputer.

11. Perangkat lunak (*software*) adalah berbagai program yang memungkinkan beroperasinya dan berfungsinya system dan jaringan komputer.

12. Sistem Informasi adalah sistem yang menyajikan informasi elektronik menggunakan teknologi telematika.

13. Infrastruktur adalah sarana dan prasarana yang tersedia dan memadai dalam pelaksanaan pemerintahan.

14. Komputer adalah sekumpulan alat elektronik yang salling bekerja sama dapat menerima data (*input*) proses mengolah data dan memberi informasi (*output*) serta terkoordinasi di bawah control program yang tersimpan dalam memori.

15. *Data base* adalah kumpulan data yang disimpan secara sistematis di dalam komputer yang dapat diolah atau dimanipulasi menggunakan perangkat lunak (program aplikasi) untuk menghasilkan informasi.

16. *Processor adalah bagian dari perangkat keras komputer* yang melakukan pemrosesan aritmatika dan logika serta pengendalian operasi komputer secara keseluruhan.

17. *Memory* adalah media penyimpanan data dan intruksi dan program yang sedang dijalankan pada komputer yang dibagi menjadi 2 (dua) jenis, yaitu *memory internal* dan *memoryeksternal.*

18. Jaringan adalah hubungan berbagai sistem komputer melalui program dan sarana kabel LAN/WAN, sehingga memungkinkan adanya komunikasi antar komputer.

19. Jaringan Lokal adalah jaringan komputer dalam suatu unit organisasi, yang biasa dikenal dengan *Local Area Network.*

20. *Local Area Network* yang selanjutnya disingkat LAN adalah jaringan komputer yang jaringannya hanya mencakup wilayah kecil.

21. *WideArea Network* yang selanjutnya disingkat WAN adalah jaringan komputer yang jaringannya hanya mencakup area yang besar.

22. *File* adalah kumpulan dari data dan informasi yang saling berhubungan dan juga tersimpan di dalam ruang penyimpanan sekunder

23. *Harddisk* 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.

24. *Flashdisk* adalah sebuah alat penyimpanan data eksternal yang dihubungkan port USB yang mampu menyimpan berbagai format data dan memiliki kapasitas penyimpanan yang cukup besar.

25. Kartu memori adalah sebuat alat penyimpan data digital.

26. Pita magnetis adalah salah satu alat penyimpanan eksternal yang menggunakan pita magnetik yang terbuat dari plastik.

27. *Filling cabinet* adalah sebuah lemari khusus yang terbuat dari bahan logam dan berukuran tegak seperti lemari.

28. *Asset* adalah kekayaan (sumber daya) yang dimiliki oleh entitas bisnis yang bisa diukur secara jelas

menggunakan satuan uang serta sistem pengurutannya berdasar pada seberapa cepat perubahannya dikonversi menjadi satuan uang kas.

29. *Interoperabilitas* adalah dimana suatu aplikasi bisa berinteraksi dengan aplikasi lainnya melalui suatu protokol yang disetujui bersama lewat bermacam-macam jalur komunikasi.

30. *Software* adalah sekumpulan data elektronik yang disimpan dan diatur oleh komputer, data elektronik yang disimpan oleh komputer itu dapat berupa program atau instruksi yang akan menjalankan suatu perintah.

31. *System Development Life Cycle (SDLC)* adalah proses pembuatan dan pengubahan sistem serta model dan metodologi yang digunakan untuk mengembangkan sistem.

32. *Username* adalah nama yang menjadi identitas pengguna komputer atau internet, bagian dari syarat pembuatan sebuah account.

33. *Password* adalah sandi yang harus dimasukan kedalam suatu sistem baik itu sistem komputer yang menggunakan *system* operasi *windows* atau bukan yang berupa karakter tulisan, suara, atau ciri-ciri khusus yang harus diingat.

34. Bisnis proses aplikasi adalah suatu kumpulan aktivitas yang terstruktur yang saling terkait dalam sebuah aplikasi untuk menyelesaikan suatu masalah atau yang menghasilkan suatu layanan.

35. *Sitemap* adalah sebuah peta yang berisi berbagai macam direktori yang terdapat dalam sebuah website/blog.

36. *Source code* adalah kumpulan pernyataan atau deklarasi bahasa pemrograman komputer yang ditulis dan dapat di baca manusia.

37. *Data center* yang selanjutnya disebut dengan Pusat data adalah bangunan untuk menempatkan perangkat keras, perangkat lunak, jaringan, dan manajemen pengelolaan.

38. CCTV adalah singkatan dari Closed Circuit Television adalah alat yang menyiratkan viktimisasi sinyal buatan tertutup atau tersembunyi, berbeda dengan sinyal siaran TV biasa.

39. Redundansi adalah sesuatu yang bisa diramalkan atau diprediksikan.

40. *Backup site backup* 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. *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.

42. Data adalah kelompok teratur simbol-simbol yang mewakili kuantitas, tindakan, benda, dan sebagainya.

43. Basis Data adalah kumpulan dan berbagai jenis data yang disusun secara sistematis dan terstruktur berdasarkan metode tertentu sesuai kaidah teknologi informasi, dan merupakan dasar penyusunan informasi.

44. 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.

45. *Online* adalah suatu keadaan komputer yang dapat saling bertukar informasi karena sudah terhubung.

46. *Website* adalah sebuah halaman yang menyajikan informasi baik dalam bentuk tulisan, gambar, suara, atau video yang diletakkan di dalam sebuah server/hosting dimana untuk mengaksesnya diperlukan jaringan internet.

47. Sumber daya manusia adalah potensi manusia yang dapat dikembangkan untuk proses produksi.

BAB II
MAKSUD, TUJUAN DAN SASARAN

Pasal 2

Maksud ditetapkannya Peraturan Bupati ini adalah untuk terciptanya sistem pengendalian keamanan yang terpadu dan menjamin keberlangsungan Sistem Manajemen Keamanan Informasi Pemerintahan Berbasis Elektronik dengan meminimalkan dampak resiko keamanan informasi.

Pasal 3

Tujuan ditetapkannya Peraturan Bupati ini adalah untuk:

a. memberikan landasan hukum dalam penerapan sistem keamanan informasi di lingkungan pemerintahan daerah;
b. memberikan pedoman dan acuan dalam hal penerapan sistem keamanan baik untuk perangkat keras maupun *lunak bagi setiap perangkat daerah dalam mengelola dan* menggunakan perangkat dan sistem yang terkait dengan teknologi informasi dan komunikasi guna meningkatkan pelayanan publik;
c. menciptakan kesamaan persepsi bagi setiap perangkat daerah dalam sistem manajemen keamanan informasi di lingkungan pemerintahan daerah.

Pasal 4

Sasaran ditetapkannya Peraturan Bupati ini adalah seluruh perangkat daerah.

BAB III
RUANG LINGKUP

Pasal 5

Ruang lingkup yang diatur dalam Peraturan Bupati ini meliputi :

a. pengolahan dan penyimpanan aset informasi;
b. standar sistem manajemen keamanan informasi.

BAB IV
PENGOLAHAN DAN PENYIMPANAN ASET INFORMASI

Pasal 6

(1) Aset informasi sebagaimana dimaksud dalam Pasal 5 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 layar komputer dan dikirimkan melalui jaringan telekomunikasi.

(2) Aset pengolahan informasi sebagaimana dimaksud dalam Pasal 5 huruf a berupa:
   a. peralatan mekanik yang digerakkan dengan tangan secara manual;
   b. peralatan elektronik yang bekerja secara elektronik penuh.

(3) Penyimpanan informasi sebagaimana dimaksud dalam Pasal 5 huruf a menggunakan media:
   a. elektronik, meliputi antara lain *harddisk*, *flashdisk*, kartu memori, pita magnetis dan lain-lain;
   b. non-elektronik, meliputi antara lain lemari, rak, laci, *fillingcabinet*, dan lain-lain.

BAB V
STANDAR SISTEM MANAJEMEN KEAMANAN INFORMASI

Pasal 7

(1) Untuk melakukan pengamanan informasi perlu adanya koordinator keamanan teknologi informasi.

(2) Koordinator keamanan teknologi informasi sebagaimana dimaksud pada ayat (1) bertanggung jawab memastikan teknologi informasi yang digunakan mendukung proses tata kelola pemerintahan dan pencapaian tujuan organisasi.

(3) Koordinator keamanan teknologi informasi sebagaimana dimaksud pada ayat (2) memiliki wewenang sebagai berikut:
   a. menyusun prosedur penyelenggaraan keamanan informasi yang diterapkan secara efektif baik bagi perangkat daerah maupun pengguna;
   b. melakukan evaluasi kinerja penyelenggaraan teknologi informasi.

(4) Koordinator keamanan teknologi informasi sebagaimana dimaksud pada ayat (1) adalah Dinas.

Pasal 8

(1) Untuk mendukung pengamanan informasi perlu adanya operator teknologi informasi.

(2) Operator sebagaimana dimaksud pada ayat (1) terdiri dari:
   a. ASN di daerah;
   b. tenaga ahli di bidang teknologi informasi.

(3) *Rekrutman* operator sebagaimana dimaksud pada ayat (2) dilakukan sesuai ketentuan peraturan perundang-undangan.

Pasal 9

(1) Operator sebagaimana dimaksud dalam Pasal 8 memiliki tugas mengoperasikan, mengelola, mengendalikan dan menyimpan seluruh aset teknologi informasi.

(2) Operator sebelum melakukan tugasnya harus menandatangani perjanjian kerahasiaan (*non-disclosure agreement*) dengan memperhatikan tingkat sensitivitas dari aset yang diakses.

Pasal 10

(1) Operator harus mematuhi seluruh kebijakan dan prosedur perangkat daerah terkait keamanan informasi.

(2) Operator harus diberikan informasi yang memadai terkait tugas dan tanggung jawab keamanan informasi.

Pasal 11

Setiap pelanggaran terhadap kebijakan dan prosedur sebagaimana dimaksud dalam Pasal 10 ayat (1) harus ditindaklanjuti sesuai peraturan perundang-undangan.

Pasal 12

Apabila terjadi pemberhentian dan/atau pergantian operator maka operator tersebut harus terlebih dahulu:

a. mengembalikan seluruh aset organisasi;

b. menonaktifkan atau menghapus seluruh hak akses organisasi; dan
c. menyesuaikan seluruh hak akses organisasi.

Pasal 13

(1) Penyelenggara sistem teknologi informasi wajib melakukan proses manajemen resiko dalam menerapkan sistem manajemen keamanan informasi.

(2) Proses manajemen resiko sebagaimana dimaksud pada ayat (1) meliputi:
a. identifikasi;
b. pengukuran;
c. pemantauan; dan
d. pengendalian atas resiko terkait penggunaan teknologi informasi.

(3) Manajemen resiko 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 resiko harus dilakukan secara terintegrasi pada setiap penggunaan operasional teknologi informasi terkait sistem yang digunakan.

Pasal 14

Setiap perangkat daerah berkordinasi dengan koordinator keamanan teknologi informasi dalam menyediakan sumber daya yang dibutuhkan untuk membentuk, mengimplementasikan, memelihara dan meningkatkan penerapan sistem manajemen keamanan informasi secara *berkesinambungan*.

Pasal 15

Setiap pengguna sistem wajib membangun kesadaran keamanan informasi dan keberlangsungan sistem serta kenyamanan dalam menggunakan teknologi informasi dan komunikasi pada lingkungan pemerintahan daerah.

Pasal 16

(1) Setiap operasi sistem teknologi infomasi dan komunikasi harus memperhatikan persyaratan minimal aspek keamanan sistem, keberlangsungan sistem, terutama sistem teknologi informasi dan komunikasi yang memfasilitasi layanan kritikal.

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

(3) Aspek keamanan sebagaimana dimaksud pada ayat (1) 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 dari 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 informasi secara logika sebagaimana dimaksud pada ayat (3) huruf b dimulai dari mendesain aplikasi, membuat alur proses hingga sistem penyimpanan yang dibuat sedemikian rupa.

Pasal 17

(1) Demi terjaminnya sistem keamanan informasi, maka program aplikasi yang dibangun oleh perangkat daerah atau bekerja sama dengan pihak ketiga wajib memenuhi persyaratan antara lain:

a. aplikasi dan website harus dibuat oleh orang atau badan yang memiliki kompetensi dan dapat dibuktikan dengan sertifikat pembuatan aplikasi dan website baik nasional ataupun internasional;
b. memiliki pengalaman yang berhubungan dengan pembuatan aplikasi dan website yang dibuktikan *dengan portofolio (hasil kerja yang pernah dibuat)*;
c. pembuat aplikasi dan website bisa dilakukan oleh ASN atau non ASN sepanjang memenuhi kriteria yang telah ditetapkan;
d. hasil rekomendasi kelayakan yang dikeluarkan oleh dinas.

(2) Demi keberlangsungan aplikasi dan website maka perlu adanya perjanjian yang mengikat antara perangkat daerah dengan pihak ketiga antara lain:
a. dokumen perjanjian masa pemeliharaan aplikasi atau website dari pihak ketiga minimal 1 (satu) tahun;
b. *untuk pemeliharaan tahun berikutnya* dapat diterbitkan perjanjian baru jika dipandang perlu;
c. pihak ketiga wajib berkoordinasi dengan ASN yang dihunjuk sebagai penanggung jawab keberlangsungan aplikasi dan website demi terjaganya keamanan dan keberlangsungan sistem;
d. selama masa pemeliharaan semua resiko dan tanggung jawab atas keberlangsungan aplikasi dan website *menjadi tanggung jawab pihak ketiga*;
e. berita acara serah terima aplikasi atau website yang memuat data diri orang atau badan pembuat aplikasi *atau website dengan melampirkan:*
    1. tanda bukti kompetensi orang atau badan pembuat aplikasi atau website;
    2. perjanjian masa pemeliharaan;
    3. perjanjian resiko hukum jika terjadi pengingkaran perjanjian;

4. kwitansi pembayaran pembuatan aplikasi atau website;
5. hasil rekomendasi kelayakan yang dikeluarkan oleh dinas;
6. peryataan bersedia melakukan penyeragaman tampilan *(layout) website.*

Pasal 18

Program aplikasi dibangun dan dikembangkan untuk dapat dioperasionalkan dalam jaringan pemerintah daerah dengan mempertimbangkan prinsip *interoperabilitas.*

Pasal 19

(1) Setiap *software* aplikasi harus selalu menyertakan prosedur *recovery* serta mengimplementasikan fungsinya di dalam software aplikasi;

(2) Setiap pembuatan dan pengembangan aplikasi harus dilengkapi dengan:
   a. dokumentasi hasil aktivitas tahapan-tahapan dalam *System Development 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 dibuktikan dengan berfungsinya aplikasi;
   f. manual pengguna, operasi, dukungan teknis dan administrasi materi transfer pengetahuan dan materi training;
   g. lama dan jumlah penggunaan aplikasi tidak terbatas;
   h. laporan hasil asesmen resiko dari Dinas, Badan Siber dan Sandi Negara.

Pasal 20

Kontrol manajemen sistem keamanan informasi berdasarkan ketentuan peraturan perundang-undangan.

Pasal 21

(1) Otentifikasi dalam teknologi dan informasi merupakan proses konfirmasi keabsahan pengguna (*user*) sesuai dengan yang terdapat dalam *database*.

(2) Dalam otentifikasi sebagaimana dimaksud pada ayat (1) terdapat 3 (tiga) jenis, yaitu:
   a. *user name* dan *password;*
   b. kunci *algoritma*, sandi, dan *smartcard*; dan
   c. *biometric*, seperti sidik jari, pola suara, dan *deoxyribonucleic acid* (DNA).

Pasal 22

(1) Otorisasi merupakan pengecekan kewenangan *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 *user* dengan masing-masing tugas/kewenangan terhadap sumber daya sistem.

(4) Daftar kemampuan (*capability list*) sebagaimana dimaksud pada ayat (2) huruf b ditekankan pada masing-masing tugas/kewenangan terhadap sumber daya sistem.

Pasal 23

(1) Keamanan komunikasi di lakukan untuk melindungi data dan/atau informasi ketika sedang ditransmisikan dari upaya penyadapan, manipulasi, atau perusakan.

(2) Keamanan komunikasi sebagaimana dimaksud pada ayat (1) meliputi:
   a. otentifikasi, yaitu proses konfirmasi keabsahan seseorang sebelum diizinkan mengakses informasi dalam sistem;
   b. pembatasan akses, yaitu pembatasan jumlah dan jenis informasi yang boleh diperoleh oleh seseorang dari sistem;
   c. kerahasiaan, yaitu melindungi informasi dalam sistem agar hanya dapat diakses oleh pihak-pihak yang berhak saja;
   d. integritas data, yaitu melindungi data dari perubahan-perubahan yang tidak dikehendaki baik secara sengaja ataupun tidak sengaja;
   e. tidak dapat disangkal (*non repudiation*), yaitu seseorang yang telah mengakses tidak dapat menyangkal aktifitas tersebut;
   f. kebijakan, yaitu keputusan-keputusan yang mengikat bagi pengguna sistem;
   g. ketersediaan, yaitu jaminan bahwa sistem dapat selalu diakses oleh pengguna; dan
   h. *kriptografi*, yaitu teknik untuk melacak informasi dengan tata cara dan kunci tertentu agar tidak terbaca oleh pihak yang tidak berhak.

Pasal 24

(1) Perangkat daerah wajib melakukan pemeliharaan terhadap sistem informasi.

(2) Pemeliharaan sebagaimana dimaksud pada ayat (1) mencakup:
a. pemeliharaan perangkat keras (*hardware*);
b. pemeliharaan perangkat lunak (*software*); dan/atau
c. pemeliharaan lain untuk menghilangkan gangguan kinerja jaringan komputer.

Pasal 25

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.

Pasal 26

Setiap perangkat dareah berkewajiban mengadakan pemeliharaan dan pengamanan terhadap keberadaan perangkat keras dan perangkat lunak yang ada di masing-masing perangkat daerah.

Pasal 27

(1) Setiap perangkat daerah bertanggung jawab dalam memastikan kegiatan operasional teknologi informasi yang stabil dan aman.

(2) Penyelenggaraan pemrosesan transaksi pada operasional teknologi informasi harus memenuhi prinsip kehati-hatian.

(3) Koordinator keamanan teknologi informasi wajib mengidentifikasi dan memantau aktivitas operasional teknologi informasi untuk memastikan efektifitas, efesiensi, dan keamanan dari aktivitas tersebut antara lain dengan :

a. menerapkan parameter fisik dan lingkungan di area kerja dan *data center*;
b. mengendalikan hak akses secara memadai sesuai kewenangan yang ditetapkan;
c. menerapkan pengendalian terhadap informasi yang diproses;
d. memastikan ketersediaan dan kecukupan kapasitas layanan jaringan komunikasi baik yang dikelola secara internal maupun oleh pihak lain penyedia jasa;
e. melakukan pemantauan kegiatan operasional teknologi informasi;
f. melakukan pemantauan terhadap aplikasi yang *digunakan oleh perangkat daerah maupun pengguna.*

Pasal 28

(1) Koordinator keamanan teknologi informasi harus memastikan ketersediaan data dan sistem dalam rangka menjaga kelangsungan teknologi informasi melalui penyelenggaraan fasilitas *data center* baik dikelola oleh internal maupun oleh pihak penyedia jasa.

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

Pasal 31

(1) Pemerintah daerah wajib memiliki *data center* yang terintegrasi dan pusat pemulihan bencana (*disaster recovery center*).

(2) *Data center* dan pusat pemulihan bencana (*disaster recovery center*) sebagaimana dimaksud pada ayat (1) wajib ditempatkan di wilayah pemerintah daerah.

(3) *Data center* dan pusat pemulihan bencana (*disaster recovery center*) sebagaimana dimaksud pada ayat (2) dikelola oleh dinas sebagai koordinator keamanan teknologi informasi di pemerintahan daerah Kabupaten Labuhanbatu.

(4) Setiap perangkat daerah wajib memiliki *back up data/mirroring/redundant* untuk mengembalikan data yang ada apabila terjadi gangguan.

Pasal 32

Pengamanan fisik dan lingkungan bagi area kerja, penyimpanan perangkat pengolahan serta penyimpanan informasi, seperti *data center, disaster recovery center* atau ruang arsip harus dilakukan oleh perangkat daerah.

Pasal 33

Setiap area yang di dalamnya terdapat informasi dan fasilitas pengolahan informasi perangkat daerah, harus dilindungi dengan menerapkan pengamanan fisik pada parameter area tersebut.

Pasal 34

(1) Setiap area sebagaimana dimaksud dalam Pasal 33 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) ditetapkan oleh dinas.

Pasal 35

Untuk area *data center, 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 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 *data center, disaster recovery center* dan ruang arsip pemerintah daerah Kabupaten Labuhanbatu; dan
g. keadaan barang harus dilaporkan dan diperiksa sebelum barang tersebut dapat dipindahkan dari area bongkar muat atau penerimaan barang ke *data center, disaster*

recovery center dan ruang arsip pemerintah daerah Kabupaten Labuhanbatu.

Pasal 36

Setiap perangkat daerah harus memperhatikan aspek pengamanan terhadap perangkat yang digunakan melalui:

a. seluruh perangkat harus ditempatkan di lokasi yang aman, sedemikian rupa sehingga terlindungi dari terjadinya pencurian, akses oleh pihak yang tidak berwenang, kebakaran, 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 penyimpan informasi yang sudah tidak digunakan lagi harus dihancurkan, atau dihapus isinya agar tidak

bisa dibaca dan digunakan lagi oleh pihak yang tidak berwenang.

Pasal 37

Khusus pengamanan area fisik di *data center* 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 *data center* harus dipelihara, diinspeksi sesuai spesifikasi perawatan berkala oleh pihak yang kompeten dan berwenang sesuai dengan rekomendasi dari pembuat perangkat tersebut;
c. *data center* harus dilengkapi dengan ups, generator listrik cadangan, perangkat pemadam kebakaran, dan diusahakan terdapat perlindungan kejut listrik (petir, tegangan tidak stabil);
d. *data center* dan *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 *data center* meliputi:
   1) temperatur antara 18° - 26° celcius;
   2) kelembaban (rh) antara 40% - 60%;
f. kabel listrik dan jaringan telekomunikasi yang membawa data atau mendukung layanan sistem informasi harus dilindungi dari penyambungan yang tidak sah (penyadapan) atau kerusakan.

Pasal 38

Penanganan ensiden dalam sistem keamanan informasi harus dilakukan untuk memastikan adanya pendekatan yang konsisten dan efektif sehingga dapat teridentifikasi

kelemahan yang ada pada sistem, layanan dan jaringan yang dapat menimbulkan gangguan terhadap operasional bisnis dan mengancam sistem keamanan informasi.

Pasal 39

Guna memastikan proses penanganan insiden yang responsif dan efektif, perlu dikembangkan berbagai prosedur yang mencakup:

a. perencanaan dan persiapan penanganan 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 40

(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.

Pasal 41

Setiap insiden keamanan informasi harus ditangani dengan baik untuk mencegah meluasnya insiden, memulihkan layanan atau informasi yang mungkin hilang dan meminimalisasi dampak dari insiden.

Pasal 42

Setiap tindakan yang diidentifikasi untuk menangani kejadian, kelemahan dan insiden keamanan informasi harus dikonsultasikan kepada koordinator keamanan sistem informasi.

Pasal 43

Setiap tindakan penanganan kejadian, kelemahan dan insiden keamanan informasi harus didokumentasikan dengan baik.

Pasal 44

Guna menjamin ketersediaan layanan serta keamanan informasi dalam kondisi darurat/bencana alam pada lokasi utama, perlu adanya redundansi terhadap fasilitas *pengolahan informasi yang disebut sebagai fasilitas backup site.*

Pasal 45

Backup site sebagaimana dimaksud dalam Pasal 44 dapat berupa lokasi kerja pengganti atau *disaster recovery center* (DRC) bagi alternatif area *data center.*

Pasal 46

Ketentuan dalam pengelolaan terkait *backup site* meliputi:

a. lokasi *backup site* secara geografis memiliki probabilitas kejadian bencana alam yang minimal;
b. *backup site* ditujukan sebagai media penyimpanan backup alternatif, serta sebagai fasilitas pengolahan informasi alternatif;

c. pengelola *backup site* beserta 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.

Pasal 47

(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 (1), dinas berkordinasi dengan menteri yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika.

BAB VI
KETENTUAN PERALIHAN

Pasal 48

Seluruh aplikasi dan website yang dibuat sebelum diundangkannya peraturan ini maka harus menyesuaikan dengan ketentuan peraturan ini.

BAB VII
KETENTUAN PENUTUP
Pasal 49

Peraturan Bupati ini mulai berlaku pada tanggal diundangkan.

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

Ditetapkan di Rantauprapat
pada tanggal 20 Desember 2018

Plt. BUPATI LABUHANBATU,

ttd

ANDI SUHAIMI DALIMUNTHE

Diundangkan Dalam Berita Daerah
Kabupaten Labuhanbatu

Nomor 28 Tahun 2018
Tanggal 21 Desember 2018

SEKRETARIS DAERAH
KABUPATEN LABUHANBATU,

ttd

AHMAD MUFLIH

Salinan sesuai dengan aslinya
KEPALA BAGIAN HUKUM SETDAKAB,

SITI HAFSAH SILALAHI, SH
PEMBINA TINGKAT I
NIP. 19741119 200502 2 001