GUBERNUR NUSA TENGGARA TIMUR

PERATURAN GUBERNUR NUSA TENGGARA TIMUR
NOMOR 19 TAHUN 2021

TENTANG

SISTEM MANAJEMEN KEAMANAN INFORMASI
DI LINGKUNGAN PEMERINTAH PROVINSI NUSA TENGGARA TIMUR

DENGAN RAHMAT TUHAN YANG MAHA ESA
GUBERNUR NUSA TENGGARA TIMUR,

Menimbang : a. bahwa Pemerintah Daerah bertanggung jawab terhadap penyelenggaraan persandian untuk pengamanan informasi Pemerintah Daerah Provinsi, salah satunya dilaksanakan melalui penyusunan kebijakan pengamanan informasi;

b. bahwa berdasarkan Pasal 5 Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian Untuk Pengamanan Informasi Di Pemerintah Daerah, penyusunan kebijakan pengamanan informasi sebagaimana dimaksud pada huruf a, dilakukan dengan menyusun rencana strategis pengamanan informasi, menetapkan arsitektur Keamanan Informasi dan menetapkan aturan mengenai tata kelola Keamanan Informasi;

c. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b, perlu menetapkan Peraturan Gubernur tentang Sistem Manajemen Keamanan Informasi Di Lingkungan Pemerintah Provinsi Nusa Tenggara Timur;

Mengingat : 1. Undang-Undang Nomor 64 Tahun 1958 tentang Pembentukan Daerah-daerah Tingkat I Bali, Nusa Tenggara Barat dan Nusa Tenggara Timur (Lembaran Negara Republik Indonesia Tahun 1958 Nomor 115, Tambahan Lembaran Negara Republik Indonesia Nomor 1649);

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);

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 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 11 Tahun 2020 tentang Cipta Kerja (Lembaran Negara Republik Indonesia Tahun 2020 Nomor 245, Tambahan Lembaran Negara Republik Indonesia Nomor 6573);
5. Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2019 tentang Pelaksanaan Persandian Untuk Pengamanan Informasi Di Pemerintah Daerah;

MEMUTUSKAN:

Menetapkan : **PERATURAN GUBERNUR TENTANG SISTEM MANAJEMEN KEAMANAN INFORMASI DI LINGKUNGAN PEMERINTAH PROVINSI NUSA TENGGARA TIMUR.**

BAB I
KETENTUAN UMUM
Bagian Kesatu
Batasan, Pengertian dan Definisi
Pasal 1

Dalam Peraturan Gubernur ini yang dimaksud dengan :
1. Daerah adalah Provinsi Nusa Tenggara Timur.
2. Pemerintah Daerah adalah Pemerintah Provinsi Nusa Tenggara Timur.
3. Gubernur adalah Gubernur Nusa Tenggara Timur.
4. Perangkat Daerah yang selanjutnya disingkat PD adalah perangkat daerah lingkup Pemerintah Provinsi Nusa Tenggara Timur.
5. Dinas adalah perangkat daerah tingkat provinsi yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika.
6. Pegawai Aparatur Sipil Negara yang selanjutnya disebut Pegawai Aparatur Sipil Negara adalah Pegawai Negeri Sipil dan Pegawai Pemerintah dengan Perjanjian Kerja yang diangkat oleh pejabat pembina kepegawaian dan diserahi tugas dalam suatu jabatan pemerintahan atau diserahi tugas negara lainnya dan digaji berdasarkan ketentuan peraturan perundang-undangan.
7. Sistem Manajemen Keamanan Informasi yang selanjutnya disingkat SMKI adalah Sistem, metode manajemen untuk melindungi, membangun, mengimplementasikan, mengoperasikan, memonitor, meninjau, memelihara dan meningkatkan Keamanan Informasi berdasarkan pendekatan resiko yang sistimatis.
8. Informasi adalah keterangan, pernyataan, gagasan, dan tanda-tanda yang mengandung nilai, makna, dan pesan, baik data, fakta maupun penjelasannya yang dapat dilihat, didengar, dan dibaca yang disajikan dalam berbagai kemasan dan format sesuai dengan perkembangan teknologi informasi dan komunikasi secara elektronik ataupun non elektronik.
9. Sistem adalah suatu kesatuan yang terdiri dari komponen atau elemen yang dihubungkan bersama untuk memudahkan aliran informasi, materi atau energi untuk mencapai suatu tujuan.
10. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan dan/atau menyebarkan Informasi Elektronik.

11. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek Keamanan Informasi seperti kerahasiaan data, keabsahan data, integritas data, otentikasi, otorisasi dan nirpenyangkalan.
12. Komputer adalah alat untuk memproses data elektronik, mengetik, optik, atau system yang melaksanakan fungsi logika, aritmatika, dan menyimpan.
13. Keamanan Informasi adalah suatu kondisi terjaganya aspek kerahasiaan, integritas keutuhan dan ketersediaan dari informasi.
14. Resiko adalah kejadian atau kondisi yang tidak diinginkan, yang dapat menimbulkan dampak negatif terhadap pencapaian sasaran kinerja pelayanan Sistem Elektronik.
15. Aset Informasi adalah sesuatu yang terdefinisi dan terkelola sebagai suatu unit informasi Teknologi Informasi dan Komunikasi sehingga dapat dipahami, dibagi, dilindungi dan dimanfaatkan bagi penyelenggaraan Sistem Pemerintahan Berbasis Elektronik.
16. Aset Pengolahan dan Penyimpanan Informasi adalah suatu perangkat baik elektronik maupun non-elektronik yang dapat digunakan untuk membuat dan menyunting informasi.
17. Data Center adalah suatu fasilitas untuk menempatkan system komputer dan perangkat-perangkat terkait, seperti Sistem komunikasi data dan penyimpanan data.
18. Standar Nasional Indonesia ISO/IEC 27001 yang selanjutnya disebut ISO adalah badan yanga menetapkan standar internasional yang terdiri dari wakil-wakil dari badan standardisasi nasional setiap negara.
19. Badan Siber dan Sandi Negara yang selanjutnya disingkat BSSN adalah lembaga pemerintah yang menyelenggarakan tugas pemerintahan di bidang keamanan siber dan persandian.
20. Brute Force Attacks adalah upaya mendapatkan akses sebuah akun dengan menebak username dan pasword yang digunakan.
21. Virtual Private Network yang selanjutnya VPN adalah layanan koneksi yang memberikan akses ke website secara aman (secure) dan pribadi (private) dengan mengubah jalur koneksi melalui server dan menyembunyikan pertukaran data yang terjadi.
22. Local Area Network yang selanjutnya disebut LAN adalah suatu jaringan komputer dengan cakupan wilayah jaringan sangat kecil atau terbatas.
23. Wide Area Network yang selanjutnya disingkat WAN adalah jaringan komputer yang membentang di wilayah geografis yang luas, meskipun mungkin terbatas dalam batas-batas Negara dan dapat juga berupa koneksi LAN yang satu ke LAN yang lain.
24. Personal Identification Number yang selanjutnya disingkat PIN adalah sebuah fitur keamanan untuk mengunci atau mengamankan perangkat, akun atau data agar tidak dapat terakses oleh orang lain yang tidak bertanggungjawab.
25. User Identification yang selanjutnya disebut User ID adalah serangkaian huruf yang merupakan tanda pengenal untuk masuk dan mengakses internet.
26. Kode Program adalah suatu rangkaian pernyataan atau deklarasi yang ditulis dalam bahasa pemrograman komputer yang terbaca.
27. Logical adalah metode akses ke Kode Program secara non fisik.
28. Versioning adalah metode yang dibutuhkan setiap kali merilis aplikasi atau software, agar pengguna tahu pada tahap atau versi berapa aplikasi yang sedang dipakai.
29. Hashing adalah suatu kode dari hasil enkripsi yang umumnya terdiri dari huruf maupun angka yang diacak.
30. Hak Akses Khusus adalah hak yang melekat pada individu atau kelompok yang telah mendapat otorisasi untuk dapat mengakses suatu file, data atau program yang tidak dapat diakses oleh orang lain.
31. Anggaran Pendapatan dan Belanja Daerah yang selanjutnya disingkat APBD adalah Anggaran Pendapatan dan Belanja Daerah Provinsi.

Bagian Kedua
Maksud dan Tujuan

Pasal 2

(1) Maksud ditetapkannya Peraturan Gubernur ini adalah sebagai pedoman pengelolaan SMKI dalam rangka pengamanan terhadap seluruh Aset Informasi dan aset pemrosesan Informasi di lingkungan Pemerintah Daerah.
(2) Tujuan ditetapkannya Peraturan Gubernur ini adalah untuk terjaganya kerahasiaan, keaslian, keutuhan, ketersediaan dan kenirsangkalan Informasi di lingkungan Pemerintah Daerah.

Bagian Ketiga
Ruang Lingkup

Pasal 3

Ruang lingkup yang diatur dalam Peraturan Gubernur ini meliputi:
a. Sistem Elektronik;
b. sertifikasi elektronik;
c. Aset Informasi;
d. pengendalian akses informasi;
e. Kriptografi;
f. keamanan fisik dan lingkungan;
g. pengamanan insiden keamanan informasi dan siber; dan
h. monitoring, evaluasi dan pelaporan.

BAB II
SISTEM ELEKTRONIK

Pasal 4

(1) Sistem Elektronik sebagaimana dimaksud dalam Pasal 3 huruf a, terdiri atas :
    a. Sistem Elektronik strategis;
    b. Sistem Elektronik tinggi; dan
    c. Sistem Elektronik rendah.
(2) Sistem Elektronik strategis sebagaimana dimaksud pada ayat (1) huruf a merupakan Sistem Elektronik yang berdampak serius terhadap kepentingan umum, pelayanan publik dan kelancaran penyelenggaraan pemerintahan Daerah.
(3) Sistem Elektronik tinggi sebagaimana dimaksud pada ayat (1) huruf b merupakan Sistem Elektronik yang berdampak terbatas pada kepentingan sektor dan/atau Daerah.
(4) Sistem Elektronik rendah sebagaimana dimaksud pada ayat (1) huruf c merupakan Sistem Elektronik selain Sistem Elektronik strategis dan Sistem Elektronik tinggi sebagaimana dimaksud pada ayat (2) dan ayat (3).

Pasal 5

(1) Penyelenggara Sistem Elektronik yang menyelenggarakan Sistem Elektronik strategis sebagaimana dimaksud dalam Pasal 4 ayat (2) bertanggung jawab untuk menerapkan :
    a. ISO;
    b. standar keamanan lain yang terkait keamanan siber yang ditetapkan oleh BSSN; dan
    c. standar keamanan lain yang terkait dengan keamanan siber yang ditetapkan oleh kementerian atau lembaga lain.

(2) Penyelenggara Sistem Elektronik yang menyelenggarakan Sistem Elektronik tinggi sebagaimana dimaksud dalam Pasal 4 ayat (3) bertanggung jawab untuk menerapkan :
   a. ISO dan/atau standar keamanan lain yang terkait dengan keamanan siber yang ditetapkan oleh BSSN; dan
   b. standar keamanan lain yang terkait dengan keamanan siber yang ditetapkan oleh kementerian atau lembaga.

(3) Penyelenggara Sistem Elektronik yang menyelenggarakan Sistem Elektronik rendah sebagaimana dimaksud dalam Pasal 4 ayat (4) bertanggung jawab untuk menerapkan :
   a. ISO; atau
   b. standar keamanan lain yang terkait dengan keamanan siber yang ditetapkan oleh BSSN.

BAB III
SERTIFIKASI ELEKTRONIK

Pasal 6

Ketentuan mengenai sertifikasi elektronik diatur dengan Peraturan Gubernur.

BAB IV
ASET INFORMASI

Pasal 7

(1) Aset Informasi terdiri atas:
   a. Aset Informasi yang berbentuk fisik, meliputi Informasi yang tercetak, tertulis dan tersimpan dalam bentuk fisik di atas kertas, papan tulis, spanduk atau di dalam buku dan dokumen serta media lain yang serupa; dan
   b. Aset Informasi yang berbentuk elektronik, meliputi Informasi yang tercetak, tertulis dan tersimpan dalam bentuk elektronik pada data base dalam Komputer, Informasi yang ditampilkan pada *website*/layar Komputer dan Informasi yang dikirimkan melalui jaringan telekomunikasi serta media lain yang serupa.

(2) Pengelolaan terhadap Aset Informasi sebagaimana dimaksud pada ayat (1), meliputi kegiatan:
   a. klasifikasi, pelabelan dan penanganan Informasi; dan
   b. penanganan Aset Pengolahan dan Penyimpanan Informasi.

Pasal 8

Dinas menetapkan PD sebagai pemilik Aset Informasi dan perangkat fisik pengolahan Informasi.

Pasal 9

(1) Aset Informasi sebagaimana dimaksud dalam Pasal 8 yang sudah mencapai batas waktu penyimpanan, dihapus oleh PD setelah berkoordinasi dengan Dinas.

(2) Penghapusan Aset Informasi sebagaimana dimaksud pada ayat (1), dilakukan dengan menggunakan metode yang dapat mencegah kebocoran informasi.

Pasal 10

Pegawai Aparatur Sipil Negara dan pihak ketiga yang tidak lagi memiliki hubungan dengan PD atau Pemerintah Daerah wajib mengembalikan Aset Informasi dan Aset Pengolahan dan Penyimpanan Informasi milik PD atau Pemerintah Daerah.

BAB V
PENGENDALIAN AKSES INFORMASI

Pasal 11

(1) PD melakukan pengendalian akses Informasi terhadap Aset Informasi, Aset Pengolahan dan Penyimpanan Informasi PD.
(2) Dalam melakukan pengendalian terhadap akses Informasi sebagaimana dimaksud pada ayat (1), PD memperhatikan hal-hal sebagai berikut:
    a. persyaratan;
    b. jaringan;
    c. pengguna; dan
    d. sistem dan aplikasi.

Pasal 12

Persyaratan sebagaimana dimaksud dalam Pasal 11 ayat (2) huruf a, meliputi:

a. akses ke Aset Informasi, Aset Pengolahan dan Penyimpanan Informasi PD harus dikendalikan dengan menggunakan metode pengendalian akses yang memadai;
b. pemberian hak akses dikelola secara formal pada seluruh siklusnya, mulai dari proses pengajuan, persetujuan dan pencabutan serta dilaksanakan oleh para pihak terkait sesuai jenjang kewenangannya;
c. pengguna yang mengakses sistem Informasi dalam lingkungan Pemerintah Daerah harus mengautentikasi dirinya dengan menggunakan kombinasi User ID dan informasi autentikasi pribadi seperti Pasword atau PIN;
d. pemberian akses kepada pengguna perlu mempertimbangkan:
    1. klasifikasi dari informasi;
    2. kritikalitas dari aset yang digunakan untuk mendukung operasional bisnis;
    3. prasyarat hukum dan ketentuan peraturan perundang-undangan, kontraktual serta keamanan yang relevan; dan
    4. didasarkan atas prinsip *need to know* dan *need to use* yaitu disesuaikan dengan kebutuhan pekerjaan dan operasional di lingkungan Pemerintah Daerah.
e. tata cara pemberian akses harus dikembangkan dan didokumentasikan oleh setiap pemilik Sistem dalam bentuk daftar atau matriks akses;
f. peninjauan oleh PD terhadap tata cara pemberian akses harus dilakukan terhadap aset/Sistem secara berkala tergantung tingkat kritikalisasi Sistem tersebut;
g. peninjauan terhadap hak akses pengguna harus didokumentasikan secara formal; dan
h. setiap penyimpangan yang ditemukan dalam proses peninjauan harus segera diperbaiki dengan cara menyesuaikan atau mencabut hak akses yang menyimpang.

Pasal 13

Penggunaan jaringan sebagaimana dimaksud dalam Pasal 11 ayat (2) huruf b, memperhatikan hal-hal sebagai berikut:

a. penggunaan layanan jaringan *(network services)* hanya diperbolehkan secara terbatas sesuai kebutuhan dan kepentingan PD;

b. jaringan komunikasi dalam lingkungan PD harus dipisahkan ke dalam domain jaringan yang terpisah sesuai dengan kebutuhan PD dan operasional dalam rangka mengamankan jaringan internal PD dan aset dalam jaringan;
c. akses secara *remote* ke jaringan internal PD dari jaringan publik harus sangat dibatasi baik dari perangkat yang digunakan maupun waktu untuk kebutuhan *troubleshooting* dan harus dilakukan melalui secure channel antara lain dengan menggunakan teknologi LAN maupun WAN VPN; dan
d. pemberian akses pengguna terhadap jaringan, baik dilakukan melalui mekanisme formal.

Pasal 14

(1) Pengguna sebagaimana dimaksud dalam Pasal 11 ayat (2) huruf c, harus memenuhi ketentuan sebagai berikut:
   a. pengguna harus menyampaikan identitas kepada PD untuk kepentingan manajemen identitas meliputi proses pendaftaran dan terminasi pengguna, dengan ketentuan:
      1. identitas pengguna *(user account)* harus unik, melekat ke setiap individu tunggal sehingga setiap tindakan pengguna dapat dipertanggungjawabkan;
      2. tidak diijinkan menggunakan satu identitas pengguna secara bersama-sama oleh lebih dari satu individu, kecuali untuk tujuan tertentu yang sebelumnya harus mendapatkan persetujuan dari pihak berwenang;
      3. memastikan secara berkala bahwa tidak ada identitas pengguna yang terduplikasi atau *redundan* sehingga seluruh identitas pengguna aktif adalah sesuai dengan data pegawai aktif pada PD.
   b. pendaftaran, modifikasi dan pencabutan hak akses pengguna mencakup proses pembuatan User ID, memberikan hak akses kepada *User* ID dan mencabut hak akses dan User ID;
   c. pendaftaran, modifikasi dan pencabutan hak akses pengguna sebagaimana dimaksud pada huruf b harus disetujui oleh atasan dari pengguna hak akses dan PD dan/atau Sistem yang diberikan sesuai dengan aturan pemberian akses;
   d. identitas pengguna harus diotorisasi secara formal oleh pejabat berwenang pada PD;
   e. identitas pengguna pada Sistem, seperti User ID, harus bersifat unik untuk memungkinkan mengidentifikasi dan meminta pertanggungjawaban pengguna;
   f. pemberian informasi autentikasi pengguna yang bersifat rahasia harus dilakukan melalui proses formal yang mencakup:
      1. informasi autentikasi perdana yang diberikan untuk pertama kalinya adalah bersifat sementara, dimana pengguna wajib menggantinya pada kesempatan pertama mengakses Sistem atau aplikasi; dan
      2. informasi autentikasi bawaan *(default)* dari penyedia barang/jasa harus segera diganti pada saat instalasi Sistem atau aplikasi.
   g. PD harus melakukan peninjauan secara berkala atas seluruh hak akses pengguna dan peninjauan insidental yang dilakukan pada saat:
      1. terjadinya proses kepegawaian, seperti promosi, mutasi dan pemberhentian; dan
      2. terjadinya perubahan struktur organisasi.
   h. Hak Akses Khusus dari Sistem informasi pada PD harus dibatasi kepada Aparatur Sipil Negara dan pihak ketiga yang terotorisasi;

i. Hak Akses Khusus sebagaimana dimaksud pada huruf h harus disetujui dan didokumentasikan secara formal;
j. alokasi Hak Akses Khusus sebagaimana dimaksud pada huruf i harus ditinjau secara berkala dan setiap kali terdapat perubahan dalam status penggunaan akses; dan
k. jejak audit untuk Hak Akses Khusus pada Sistem informasi di lingkungan PD harus diaktifkan.

(2) Setiap penyimpangan yang ditemukan dalam proses peninjauan sebagaimana dimaksud pada ayat (1) huruf j, harus segera diperbaiki dengan menyesuaikan atau menghapus Hak Akses Khusus yang menyimpang.

(3) Hak Akses Khusus sebagaimana dimaksud pada ayat (2), harus dialokasikan secara individual dan tidak dibagikan untuk menjamin akuntabilitas dari pengguna.

(4) Dalam hal Hak Akses Khusus sebagaimana dimaksud pada ayat (3) tidak bisa dialokasikan secara individual maka Dinas mengimplementasikan kontrol tambahan untuk menghindari penyalahgunaan.

Pasal 15

(1) Dalam menggunakan User ID dan Pasword, pengguna sebagaimana dimaksud dalam Pasal 14 bertanggung jawab untuk:
a. menjaga kerahasiaan dan keamanan Pasword pribadi atau kelompok serta informasi autentikasi rahasia lainnya;
b. segera mengganti informasi autentikasi rahasia jika terindikasi bahwa informasi tersebut telah diketahui oleh orang lain;
c. Pasword yang diberikan untuk pertama kali bersifat sementara dan pengguna wajib menggantinya pada kesempatan pertama saat mengakses Sistem atau aplikasi;
d. melakukan pergantian pasword paling rendah 3 (tiga) bulan sekali;
e. Pasword yang pernah digunakan sebelumnya tidak boleh digunakan kembali sampai setelah 3 (tiga) siklus pergantian Pasword;
f. prosedur login dari Sistem harus dapat menjamin keamanan dari Pasword dengan cara:
   1. tidak menampilkan Pasword yang dimasukan; dan
   2. tidak menyediakan pesan bantuan pada saat proses login yang dapat membantu pengguna yang tidak berwenang.
g. menggunakan kata sandi yang berbeda untuk keperluan kedinasan dan pribadi.

(2) Pasword sebagaimana dimaksud pada ayat (1), harus memiliki karakteristik sebagai berikut :
a. memiliki panjang minimum 8 (delapan) karakter;
b. mengandung kombinasi huruf besar, huruf kecil dan nomor;
c. tidak terdiri dari kata atau nomor yang mudah ditebak; dan
d. tidak terdiri dari informasi pribadi.

Pasal 16

(1) Dalam mengelola Sistem dan aplikasi sebagaimana dimaksud dalam Pasal 11 ayat (2) huruf d, PD harus:
a. memastikan bahwa Sistem dan aplikasi yang dikelola memiliki fasilitas manajemen hak akses pengguna, manajemen kata sandi yang baik serta mekanisme autentikasi pengguna yang aman;
b. fasilitas manajemen hak akses pengguna sebagaimana dimaksud pada huruf a harus mampu membatasi akses Informasi sesuai ketugasannya *(role based access control)*;

c. fasilitas manajemen kata sandi sebagaimana dimaksud pada huruf a, harus dapat memastikan bahwa kata sandi yang dihasilkan berkualitas, dengan cara:
   1. menegakkan akuntabilitas pengguna melalui penggunaan identitas pengguna tunggal untuk setiap individu;
   2. memberikan fasilitas penggantian kata sandi mandiri;
   3. membantu memberikan rekomendasi kata sandi yang berkualitas;
   4. mewajibkan pengguna untuk mengganti kata sandi pada saat pertama kali login;
   5. mewajibkan pengguna untuk mengganti kata sandi secara berkala;
   6. menyimpan riwayat kata sandi pengguna dan mencegah agar pengguna tidak menggunakan kata sandi yang sebelumnya telah digunakan;
   7. tidak menampilkan kata sandi saat sedang dientrikan; dan
   8. kata sandi yang disimpan dan ditransmisikan harus terlindungi (dienkripsi).

d. mekanisme autentikasi pengguna perlu dirancang agar meminimalisir peluang terjadinya akses yang tidak sah, dengan cara:
   1. kata sandi tidak ditransmisikan melalui jaringan secara teks terang;
   2. memiliki mekanisme penguncian Sistem sementara sebagai perlindungan terhadap Brute Force Attacks;
   3. adanya pencatatan terhadap seluruh upaya autentifikasi yang sukses dan gagal; dan
   4. adanya pembatasan jumlah akses pengguna yang sama secara simultan.

e. penggunaan program penggunaan khusus dalam operasional Sistem pada PD harus mempertimbangkan keamanan yaitu penggunaan program utility khusus seperti Sistem monitoring yang dapat mengambil alih kendali Sistem/aplikasi atau mendapatkan hak akses khusus pada Sistem/aplikasi harus sangat dibatasi berdasarkan kebutuhan operasional pengguna;

f. memastikan bahwa Kode Program dikelola dan disimpan secara memadai, baik yang dikembangkan oleh internal PD maupun yang dikembangkan oleh penyedia jasa aplikasi; dan

g. bersama penyedia jasa aplikasi meninjau kembali perjanjian kerja sama dalam hal terdapat pengembangan terhadap aplikasi yang ada.

(2) Untuk mencegah akses tanpa izin ke Kode Program sebagaimana dimaksud pada ayat (1) huruf f, PD melakukan pengendalian.

(3) Pengendalian sebagaimana dimaksud pada ayat (2), dilakukan dengan:
   a. tidak menyimpan Kode Program pada Sistem operasional;
   b. menyimpan Kode Program pada lokasi fisik yang aman dari ancaman akses tanpa izin maupun ancaman kerusakan karena kondisi lingkungan;
   c. membatasi akses secara fisik maupun *Logical* ke Kode Program;
   d. Kode Program hanya diberikan kepada pengembang dan personil yang berwenang; dan
   e. mengimplementasikan metode *Versioning* dan proses manajemen perubahan untuk menjamin integritas dari Kode Program aplikasi.

BAB VI
KRIPTOGRAFI

Pasal 17

(1) Teknologi Kriptografi digunakan dalam pengolahan dan penyimpanan Informasi di lingkungan Pemerintah Daerah.
(2) Penggunaan teknologi Kriptografi dalam pengolahan dan penyimpanan Informasi sebagaimana dimaksud pada ayat (1), diatur sebagai berikut:
   a. kontrol Kriptografi dapat digunakan untuk menjamin kerahasiaan, keaslian dan/atau integritas, autentikasi, otorisasi dan nirpenyangkalan dari Informasi sensitif di lingkungan PD;
   b. kontrol Kriptografi dapat mencakup namun tidak terbatas pada:
      1. enkripsi Informasi dan jaringan komunikasi;
      2. pemeriksaan integritas informasi, seperti *Hashing*;
      3. autentikasi identitas; dan
      4. tanda tangan elektronik (digital *signatures).*
   c. implementasi dari kontrol Kriptografi harus mempertimbangkan klasifikasi dari informasi yang akan diamankan;
   d. pemilihan kontrol Kriptografi harus mempertimbangkan :
      1. jenis dari kontrol Kriptografi;
      2. kekuatan dari algoritma Kriptografi; dan
      3. panjang dari kunci Kriptografi.
   e. implementasi dari kontrol Kriptografi harus secara berkala ditinjau untuk memastikan kecukupan dan kesesuaian dari kontrol tersebut dalam mengamankan kerahasiaan dan integritas dari Informasi;
   f. pengelolaan dari kunci Kriptografi harus dikendalikan secara ketat dan dibatasi hanya pada personil yang terotorisasi; dan
   g. pengelolaan dari kunci Kriptografi didasarkan pada prinsip *dual custody* (suatu pekerjaan dilakukan secara bersama-sama) untuk mengurangi Resiko penyalahgunaan.

BAB VII
KEAMANAN FISIK DAN LINGKUNGAN

Pasal 18

(1) Pengelolaan keamanan fisik dan lingkungan dilakukan di area kerja dan penyimpanan perangkat pengolahan dan penyimpanan Informasi.
(2) Penyimpanan perangkat pengolahan dan penyimpanan Informasi sebagaimana dimaksud pada ayat (1) terdiri atas:
   a. Data *Center*;
   b. ruang arsip; dan
   c. perangkat lainnya dengan peruntukan yang sama.

BAB VIII
PENANGANAN INSIDEN KEAMANAN INFORMASI DAN SIBER

Pasal 19

(1) Penanganan insiden Keamanan Informasi dan siber meliputi :
   a. tanggung jawab PD dan prosedur penanganan insiden;
   b. pelaporan atas kejadian insiden Keamanan Informasi dan siber;
   c. pelaporan atas penanganan insiden Keamanan Informasi dan siber; dan
   d. pelaporan atas kelemahan Keamanan Informasi.
(2) Penanganan insiden Keamanan Informasi sebagaimana dimaksud pada ayat (1), dilakukan untuk merespon insiden Keamanan Informasi dan siber yang terjadi pada PD secara cepat, efektif dan efisien.

(3) Dalam merespon insiden Keamanan Informasi dan siber yang terjadi pada PD sebagaimana dimaksud pada ayat (2), Pemerintah Daerah membentuk Tim Tanggap Insiden Keamanan.

BAB IX
MONITORING DAN EVALUASI

Pasal 20

(1) Dinas melakukan monitoring dan evaluasi terhadap pelaksanaan SMKI di lingkungan Pemerintah Daerah.
(2) Monitoring dan evaluasi sebagaimana dimaksud pada ayat (1) dilakukan dalam bentuk penilaian terhadap kesesuaian antara implementasi pelaksanaan SMKI dengan program/kegiatan yang telah ditetapkan.

BAB X
PEMBIAYAAN

Pasal 21

Segala biaya yang dikeluarkan sebagai akibat ditetapkannya Peraturan Gubernur ini dibebankan pada APBD.

BAB XI
KETENTUAN PENUTUP

Pasal 22

Peraturan Gubernur ini mulai berlaku pada tanggal diundangkan.

Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Gubernur ini dengan penempatannya dalam Berita Daerah Provinsi Nusa Tenggara Timur.

Ditetapkan di Kupang
pada tanggal 1 APRIL 2021
GUBERNUR NUSA TENGGARA TIMUR,

VIKTOR BUNGTILU LAISKODAT

Diundangkan di Kupang
pada tanggal 1 APRIL 2021
SEKRETARIS DAERAH
PROVINSI NUSA TENGGARA TIMUR,

BENEDIKTUS POLO MAING

BERITA DAERAH PROVINSI NUSA TENGGARA TIMUR TAHUN 2021
NOMOR 019