PERATURAN GUBERNUR BANTEN

NOMOR 7 TAHUN 2018

TENTANG

TATA KELOLA SISTEM ELEKTRONIK DI LINGKUNGAN

PEMERINTAH PROVINSI BANTEN

DENGAN RAHMAT TUHAN YANG MAHA ESA

GUBERNUR BANTEN,

Menimbang :

a. bahwa untuk mendukung tercapainya rencana strategis pembangunan Pemerintah Daerah di Provinsi Banten, perlu dibangun teknologi informasi dan komunikasi melalui Tata Kelola Sistem Elektronik di Pemerintahan Daerah yang efektif, efisien, transparan, dan terpadu;

b. bahwa kemajuan teknologi informasi dan komunikasi yang sangat pesat memberi peluang pengelolaan data dan informasi yang cepat dan akurat sehingga perlu dimanfaatkan oleh Pemerintah Provinsi Banten dalam melaksanakan tugas dan fungsinya dalam memberikan pelayanan kepada masyarakat;

c. bahwa untuk menyelenggarakan pemerintahan yang baik dan meningkatkan layanan publik yang efektif dan efisien, diperlukan adanya kebijakan dan strategi pengembangan e-government;

d. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b, dan huruf c, perlu menetapkan Peraturan Gubernur tentang Tata Kelola Sistem Elektronik di Lingkungan Pemerintah Provinsi Banten.

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

2. Undang-Undang Nomor 23 Tahun 2000 tentang Pembentukan Provinsi Banten (Lembaran Negara Republik Indonesia Tahun 2000 Nomor 182, Tambahan Lembaran Negara Republik Indonesia Nomor 4010);

3. 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);

4. 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);

5. Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik (Lembaran Negara Republik Indonesia Tahun 2009 Nomor 112, Tambahan Lembaran Negara Republik Indonesia Nomor 5038);

6. 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 2014 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 5679);

7. Peraturan Pemerintah Nomor 61 Tahun 2010 tentang Pelaksanaan Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (Lembaran Negara Republik Indonesia Tahun 2010 Nomor 99, Tambahan Lembaran Negara Republik Indonesia Nomor 5149);
8. 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);
9. Peraturan Menteri Komunikasi dan Informatika Nomor 41/PER/M.KOMINFO/11/2007 tentang Panduan Umum Tata Kelola Teknologi Informasi dan Komunikasi Nasional;
10. Peraturan Menteri Pendayagunaan Aparatur Negara Nomor 35 Tahun 2012 tentang Pedoman Penyusunan Standar Oprasional Prosedur Administrasi Pemerintah;
11. Peraturan Menteri Komunikasi dan Informatika Nomor 23 Tahun 2013 tentang Pengelolaan Nama Domain (Berita Negara Republik Indonesia Tahun 2013 Nomor 1235);
12. Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2015 tentang Register Nama Domain Instansi Penyelenggara Negara;
13. Peraturan Menteri Komunikasi dan Informatika Nomor 10 Tahun 2015 tentang Tata Cara Pendaftaran Sistem Elektronik Instansi Penyelenggara Negara (Berita Negara Republik Indonesia Tahun 2015 Nomor 321);
14. Peraturan Komisi Informasi Nomor 1 Tahun 2010 tentang Standar Layanan Informasi Publik;
15. Peraturan Gubernur Banten Nomor 67 Tahun 2017 tentang Rencana Induk Teknologi Informasi dan Komunikasi Pemerintah Provinsi Banten (Berita Daeah Provinsi Banten Tahun 2017 Nomor 67).

MEMUTUSKAN:

Menetapkan : PERATURAN GUBERNUR TENTANG TATA KELOLA SISTEM ELEKTRONIK DI LINGKUNGAN PEMERINTAH PROVINSI BANTEN.

BAB I

KETENTUAN UMUM

Pasal 1

Dalam Peraturan Gubernur ini yang dimaksud dengan:

1. Daerah adalah Provinsi Banten.
2. Pemerintah Daerah adalah Gubernur sebagai unsur penyelenggara pemerintah daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan daerah otonom.
3. Gubernur adalah Gubernur Banten.
4. Perangkat Daerah adalah unsur pembantu Gubernur dan Dewan Perwakilan Rakyat Daerah dalam penyelenggaraan urusan pemerintahan yang menjadi kewenangan daerah.
5. Dinas adalah Dinas Komunikasi, Informatika, Statistik dan Persandian Provinsi Banten.
6. Teknologi Informasi dan Komunikasi yang selanjutnya disingkat TIK adalah suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan/atau menyebarluaskan informasi.
7. Standar Operasional Prosedur yang selanjutnya disingkat SOP adalah dokumen yang berkaitan dengan prosedur yang dilakukan secara kronologis untuk menyelesaikan suatu pekerjaan yang bertujuan untuk memperoleh hasil kerja yang paling efektif dari para pekerja dengan biaya yang serendah-rendahnya.
8. Penyelenggaraan Teknologi Informasi dan Komunikasi yang selanjutnya disebut *e-Government* adalah pemanfaatan teknologi informasi dan komunikasi dalam proses pemerintahan.
9. Sistem Informasi adalah kesatuan komponen yang terdiri atas lembaga, sumber daya manusia, perangkat keras, perangkat lunak, substansi data dan informasi yang terkait satu sama lain dalam satu mekanisme kerja untuk mengelola data dan informasi.

10. Arsitektur Informasi adalah model informasi organisasi yang mendefinisikan lingkup kebutuhan informasi yang dipetakan ke dalam tata kelola organisasi terkait.
11. Arsitektur Aplikasi adalah model aplikasi organisasi yang mendefinisikan lingkup aplikasi beserta persyaratan dan spesifikasi desain apa saja yang dibutuhkan oleh organisasi untuk mengakomodasi seluruh level tata kelola organisasi seperti transaksional, operasional, pelaporan, analisis, monitoring, dan perencanaan.
12. Arsitektur Infrastruktur TIK adalah topologi, konfigurasi, diagram, dan spesifikasi infrastruktur teknologi beserta pendekatan siklus hidupnya untuk memastikan infrastruktur teknologi yang digunakan organisasi selalu sesuai dengan kebutuhan.
13. Organisasi dan Manajemen adalah struktur organisasi dan deskripsi peran, serta kebijakan dan prosedur untuk menjalankan seluruh proses dalam manajemen TIK.
14. Data adalah kumpulan fakta berupa angka, huruf, gambar, suara, peta, atau citra tentang karakteristik atau ciri-ciri suatu objek.
15. Informasi adalah gabungan, rangkaian dan analisis data yang berbentuk angka, huruf, gambar, suara, peta, atau citra yang telah diolah, yang mempunyai arti, nilai dan makna tertentu.
16. Kode Program adalah suatu rangkaian pernyataan atau deklarasi yang ditulis dalam bahasa pemrograman komputer yang terbaca manusia.
17. Kode Sumber adalah suatu program yang biasanya disimpan dalam satu atau lebih berkas teks, dan dapat pula ditampilkan dalam bentuk cuplikan kode (*code snippet*) yang dicetak pada buku atau media lainnya.
18. Basis Data adalah kumpulan informasi yang disimpan di dalam komputer secara sistematik sehingga dapat diperiksa menggunakan suatu program komputer untuk memperoleh informasi dari basis data tersebut.
19. Infrastruktur Teknologi Informasi dan Komunikasi adalah perangkat keras, piranti lunak sistem operasi dan aplikasi, pusat data serta fasilitas pendukung lainnya, untuk mendukung penyelenggaraan *e-Government*.
20. Pusat data adalah suatu fasilitas yang digunakan untuk menempatkan sistem komputer dan komponen-komponen terkaitnya, seperti sistem telekomunikasi dan sistem repositori.

21. Aplikasi adalah komponen sistem informasi yang digunakan untuk menjalankan fungsi, proses dan mekanisme kerja yang mendukung pelaksanaan *e-Government*.
22. Aplikasi Umum adalah aplikasi *e-Government* yang dapat digunakan oleh seluruh Perangkat Daerah di lingkungan Pemerintah Provinsi Banten.
23. Aplikasi Khusus adalah aplikasi *e-Government* yang digunakan untuk memenuhi kebutuhan Perangkat Daerah tertentu sesuai dengan tugas dan fungsinya.
24. Sumber Daya informatika adalah sumber daya dalam bentuk perangkat keras, piranti lunak, dan sumber daya manusia yang terkait dengan teknologi informasi dan komunikasi.
25. Tata Kelola Sistem Elektronik adalah cara mengatur serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan menyebarkan Informasi elektronik.
26. Repositori adalah sistem pengkoleksian berkas siap pakai dan siap cetak dari berbagai macam sistem informasi dari berbagai unit kerja sehingga dapat diproses menjadi suatu informasi turunan atau agregat secara terintegrasi.
27. Interoperabilitas adalah kemampuan dua sistem atau dua komponen atau lebih untuk bertukar informasi dan untuk menggunakan informasi yang telah dipertukarkan.
28. Penyelenggara Sistem Elektronik yang selanjutnya disebut PSE adalah Perangkat Daerah pemilik sistem informasi sesuai tugas pokok dan fungsinya.
29. Portal *web* adalah kumpulan *situs web* yang berisi informasi elektronik yang dapat diakses publik.
30. Situs *web* adalah kumpulan halaman *web* yang berisi topik yang saling terkait berupa informasi elektronik yang dapat diakses publik.
31. Nama Domain adalah alamat internet penyelenggara negara, orang, badan usaha, dan/atau masyarakat, yang dapat digunakan dalam berkomunikasi melalui internet, yang berupa kode atau susunan karakter yang bersifat unik untuk menunjukkan lokasi tertentu dalam internet.
32. Hak cipta adalah hak eksklusif pencipta yang timbul secara otomatis berdasarkan prinsip deklaratif setelah suatu ciptaan diwujudkan

dalam bentuk nyata tanpa mengurangi pembatasan sesuai dengan ketentuan peraturan perundang-undangan.

33. Akses adalah kegiatan melakukan interaksi dengan sistem elektronik yang berdiri sendiri atau dalam jaringan.
34. *E-Government* adalah pemanfaatan teknologi informasi dan komunikasi dalam proses manajemen pemerintahan untuk meningkatkan efisiensi, efektifitas, transparansi, dan akuntabilitas penyelenggaraan pemerintahan.
35. *Sistem Elektronik* adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan Informasi Elektronik.

Pasal 2

Ruang lingkup Tata Kelola Sistem Elektronik di Lingkungan Pemerintah Daerah ini meliputi:

a. infrastruktur TIK;
b. nama domain dan subdomain Pemerintah Daerah;
c. aplikasi;
d. data dan informasi;
e. portal *web* Pemerintah Daerah;
f. surat elektronik *(e-mail)* Pemerintah Daerah;
g. pusat data dan pusat pemulihan bencana;
h. keterhubungan antar system informasi *(interoperabilitas)*;
i. sumber daya manusia;
j. standar operasional prosedur; dan
k. pembinaan pengawasan.

BAB II

INFRASTRUKTUR TIK

Pasal 3

(1) Infrastruktur TIK yang digunakan dalam *e-Government* harus sesuai dengan standar teknologi, interoperabilitas, dan keamanan informasi.
(2) Standar teknologi sebagaimana dimaksud pada ayat (1) harus memperhatikan teknologi yang terbuka, mudah diperoleh di pasaran,

mudah memperoleh dukungan ketika dibutuhkan, dan mudah dikembangkan (*scalable*).

(3) Standar interoperabilitas sebagaimana dimaksud pada ayat (1) mengacu pada standardisasi format data yang akan dipertukarkan untuk mempermudah dalam hal pengelolaan, pengaksesan data, berbagi data dalam rangka memberikan pelayanan informasi yang lebih efektif dan efisien.

(4) Standar keamanan informasi sebagaimana dimaksud pada ayat (1) tercantum dalam Lampiran I yang merupakan bagian tidak terpisahkan dari Peraturan Gubernur ini.

Pasal 4

(1) Dinas menyediakan, mengelola, dan memelihara infrastruktur TIK yang diperlukan untuk menjamin penyelenggaraan *e-Government*.

(2) Infrastruktur sebagaimana dimaksud pada ayat (1) dimanfaatkan oleh Perangkat Daerah yang terdiri atas:
   a. pusat data dan pusat pemulihan bencana yang selanjutnya disebut *Data Center (DC)* dan *Disaster Recovery Center (DRC)*;
   b. jaringan *backbone* antar Perangkat Daerah;
   c. *router, server,* dan *storage*;
   d. sistem keamanan informasi; dan
   e. *bandwidth*;

(3) *Backup* data ataupun *Disaster Recovery Center* diletakkan dan dikonfigurasi ditempat yang jauh dari pusat data *(data center)* dan risiko terjadinya insiden keamanan informasi.

(4) Dinas berwenang mengatur pemanfaatan internet dan mengendalikan situs yang boleh diakses oleh Perangkat Daerah.

(5) Dinas bisa membuka akses situs yang terlarang apabila ada pengajuan permintaan secara resmi dari Perangkat Daerah dalam rangka melaksanakan pekerjaan sesuai tupoksi Perangkat Daerah.

(6) Seluruh infrastruktur TIK yang diselenggarakan oleh Daerah, hanya bisa dimanfaatkan sebagai sarana bekerja untuk kepentingan kedinasan.

(7) Pengadaan perangkat baru, tambahan, penggantian, harus kompatibel dengan perangkat yang sudah ada.

(8) Hak akses ke data dan keamanan informasi hanya dimiliki oleh Pegawai Negeri Sipil.

(9) Penyediaan dan pengelolaan infrastruktur yang dilaksanakan bisa dilaksanakan oleh pihak ketiga yang berbadan hukum di Indonesia, berdomisili di Indonesia dan memiliki sertifikat ISO 27001.

Pasal 5

(1) Perangkat Daerah dapat menyediakan, mengelola, memanfaatkan dan memelihara infrastruktur TIK sendiri sesuai kebutuhannya.
(2) Infrastruktur yang bisa dikelola oleh Perangkat Daerah diantaranya adalah:
    a. *Local Area Network* (kabel, *switch* dan *wifi*);
    b. perangkat *end user* (laptop, desktop dan alat cetak); dan
    c. keamanan informasi internal Perangkat Daerah.
(3) Setiap kabel data di semua Perangkat Daerah yang menghubungkan jaringan komputer harus diberi label kode alamat antar *node*.

Pasal 6

Perangkat Daerah wajib menginventarisasi seluruh perangkat TIKnya di dalam sistem informasi aset Pemerintah Daerah melalui Badan Pengelolaan Keuangan dan Aset Daerah.

BAB III

NAMA DOMAIN DAN SUBDOMAIN PEMERINTAH DAERAH

Pasal 7

(1) Nama domain resmi Pemerintah Daerah adalah *banten.go.id*.
(2) Penanggung jawab domain Pemerintah Provinsi Daerah sebagaimana dimaksud pada ayat (1) adalah Dinas.
(3) Transisi perubahan domain resmi Pemerintah Daerah sebagaimana dimaksud pada ayat (1) dilaksanakan selama 1 (satu) tahun.

Pasal 8

(1) Nama subdomain dapat digunakan oleh Perangkat Daerah dan Unit Kerja di Pemerintah Daerah serta aplikasi berbasis *web*.
(2) Penggunaan nama subdomain sebagaimana dimaksud pada ayat (1) dikoordinasikan oleh Dinas.

(3) Penanggung jawab subdomain adalah Perangkat Daerah atau Unit Kerja yang mengajukan dan menggunakan nama subdomain.
(4) Penanggung jawab subdomain harus melakukan evaluasi pemanfaatan subdomain untuk memastikan keberlangsungan *website*, aplikasi atau kegiatan yang menggunakan subdomain.

Pasal 9

Nama domain dan sub domain sebagaimana dimaksud dalam Pasal 7 ayat (1) dan Pasal 8 ayat (1) tercantum dalam Lampiran III yang merupakan bagian tidak terpisahkan dari Peraturan Gubernur ini

BAB IV

APLIKASI

Pasal 10

(1) Aplikasi *e-Government* terdiri atas aplikasi umum dan aplikasi khusus.
(2) Aplikasi *e-Government* sebagaimana dimaksud pada ayat (1) harus dilengkapi:
    a. kode program;
    b. basis data; dan
    c. dokumentasi.
(3) Dokumentasi sebagaimana dimaksud pada ayat (2) huruf c paling sedikit terdiri atas identifikasi kebutuhan, desain aplikasi, penjelasan kode program, prosedur standar manual, penjelasan basis data, hak akses, dan kebutuhan sumber daya informatika.
(4) Perangkat lunak yang digunakan oleh Instansi di lingkungan Pemerintah Daerah untuk pelayanan publik wajib:
    a. terdaftar pada Dinas;
    b. terjamin keamanan dan keandalan operasi sebagaimana mestinya;
    c. sesuai dengan ketentuan peraturan perundang-undangan; dan
    d. spesifikasi teknis pengadaan perangkat lunak baru pada setiap Perangkat Daerah wajib dikonsultasikan/dikoordinasikan kepada Dinas.

Pasal 11

(1) Program Aplikasi merupakan komponen sistem informasi yang digunakan untuk menjalankan fungsi, proses, dan mekanisme kerja yang mendukung pelaksanaan *e-Government.*

(2) Program aplikasi sebagaimana dimaksud pada ayat (1) dibangun dan dikembangkan untuk:
   a. dioperasionalkan dalam jaringan dengan mempertimbangkan prinsip interoperabilitas;
   b. program aplikasi dibangun dan dikembangkan menggunakan bahasa pemrograman yang dapat dikoneksikan dengan jaringan;
   c. program aplikasi dibangun dan dikembangkan berdasarkan fungsi dan tugas pokok masing-masing Perangkat Daerah;
   d. meningkatkan produktivitas tugas-tugas operasional dan administratif masing-masing Perangkat Daerah;
   e. program aplikasi pada setiap Perangkat Daerah terintegrasi dalam jaringan lokal yang merupakan bagian integral dari infrastruktur informasi Pemerintah Daerah;
   f. untuk meningkatkan komunikasi, responsivitas pemerintah, dan partisipasi masyarakat dikembangkan aplikasi layanan *on-line* sebagai media interaktif melalui jaringan internet;
   g. setiap *software* aplikasi harus selalu menyertakan prosedur *backup* dan *restore*, serta mengimplementasikan fungsionalitasnya di dalam *software* aplikasi;
   h. Setiap pengoperasian *software* aplikasi harus disertakan dokumentasi sebagai berikut:
      1. dokumentasi hasil aktivitas tahapan-tahapan dalam *System Development Life Cycle (SDLC)*:
      2. manual pengguna, operasi, dukungan teknis, dan administrasi; dan
      3. materi transfer pengetahuan dan materi training.
   i. Semua dokumentasi sebagaimana dimaksud pada huruf h, wajib dikirimkan ke Dinas.

(3) Sistem Basis Data merupakan suatu fasilitas yang digunakan untuk menempatkan sistem komputer dan komponen-komponen terkaitnya, seperti sistem telekomunikasi dan sistem repositori terdiri atas:
   a. basis data sektoral disusun dan dikembangkan oleh Perangkat Daerah guna mendukung penyediaan informasi yang diperlukan untuk kegiatan operasional dalam sektor yang sama;
   b. basis data lintas sektor disusun dan dikembangkan oleh Dinas guna mendukung penyediaan informasi yang diperlukan berbagai sektor;

c. pembangunan dan pengembangan basis data menggunakan data *base server* yang dapat digunakan secara bersama; dan

d. pengamanan basis data dilakukan sesuai dengan sistem dan prosedur teknis dalam sistem komputer.

(4) Manajemen layanan oleh pihak ketiga meliputi:

a. layanan TIK dapat diselenggarakan sebagian atau seluruhnya oleh pihak ketiga, dengan mempertimbangkan faktor-faktor berikut ini:

1. sumber daya internal yang dimiliki oleh institusi pemerintah terkait kurang memungkinkan, untuk mencapai tingkat layanan minimal yang diberikan kepada konsumen (publik atau bisnis);
2. seluruh data yang diolah melalui layanan pihak ketiga adalah data milik institusi pemerintahan terkait, dan pihak ketiga harus menjaga kerahasiaannya serta tidak berhak menggunakannya untuk hal-hal di luar kerja sama dengan institusi pemerintahan.

b. seluruh layanan TIK yang diselenggarakan oleh pihak ketiga harus mematuhi ketentuan-ketentuan operasi sistem sebagai berikut:

1. manajemen tingkat layanan;
2. keamanan informasi dan keberlangsungan sistem;
3. manajemen *software* aplikasi;
4. manajemen infrastruktur; dan
5. manajemen data.

c. secara reguler pihak ketiga penyelenggara layanan TIK harus memberikan laporan atas tingkat kepatuhan terhadap ketentuan-ketentuan operasi sistem sebagaimana dimaksud pada huruf b;

d. pihak institusi pemerintahan yang layanannya diselenggarakan oleh pihak ketiga terkait secara reguler dan insidental dapat melakukan audit atas laporan yang disampaikan oleh pihak ketiga untuk memastikan validitasnya, baik dilakukan secara internal yang melibatkan Dinas atau menggunakan jasa pihak ketiga lain yang independen;

e. penyedia yang mengembangkan perangkat lunak yang khusus dibuat untuk suatu Instansi wajib menyerahkan kode sumber dan dokumentasi atas perangkat lunak kepada Instansi yang bersangkutan.

Pasal 12

(1) Aplikasi *e-Government* harus memenuhi standar pengembangan, interoperabilitas, dan standar keamanan informasi.

(2) Penyelenggara aplikasi pada Perangkat Daerah Pemerintah Provinsi wajib berkoordinasi dengan Dinas dalam perencanaan dan pengembangan aplikasi.
(3) Hak cipta atas aplikasi dan kelengkapannya sebagaimana dimaksud dalam Pasal 10 ayat (1) yang dibangun oleh mitra kerja menjadi milik Pemerintah Daerah.
(4) Aplikasi sebagaimana dimaksud pada ayat (1) yang berbasis *web* harus dipasang pada pusat data Pemerintah Daerah.
(5) Ketentuan mengenai standar pengembangan aplikasi sebagaimana dimaksud pada ayat (1) tercantum dalam Lampiran IV yang merupakan bagian tidak terpisahkan dari Peraturan Gubernur ini.

Pasal 13

(1) Nama domain aplikasi umum sebagaimana dimaksud dalam Pasal 10 ayat (1) yang berbasis *web* menggunakan nama domain sebagaimana dimaksud dalam Pasal 7 ayat (1) diletakkan di depan nama domain Pemerintah Daerah menjadi nama sub domain.
(2) Ketentuan nama domain aplikasi sebagaimana dimaksud pada ayat (1) mengikuti ketentuan dalam Pasal 7 Peraturan Gubernur ini.

BAB V

DATA DAN INFORMASI

Pasal 14

(1) Data dan informasi dalam penyelenggaraan *e-Government* wajib disediakan oleh setiap Perangkat Daerah Pemerintah Daerah.
(2) Data dan informasi sebagaimana dimaksud pada ayat (1) harus memenuhi kaidah struktur data, interoperabilitas kebaruan, keakuratan, kerahasiaan, dan keamanan informasi.
(3) Data dan informasi sebagaimana dimaksud pada ayat (1) dikelola dan dikumpulkan oleh Perangkat Daerah dan Dinas.
(4) Data dan informasi sebagaimana dimaksud pada ayat (1) dapat dimanfaatkan oleh seluruh Perangkat Daerah.

Pasal 15

(1) Data dan informasi sebagaimana dimaksud dalam Pasal 14 ayat (1) merupakan hak cipta Pemerintah Daerah.

(2) Data dan informasi sebagaimana dimaksud dalam Pasal 14 ayat (1) disimpan pada pusat data Pemerintah Daerah.

(3) Pemanfaatan data dan informasi sebagaimana dimaksud dalam Pasal 14 ayat (1) harus berkordinasi dengan Dinas.

(4) Pemanfaatan data dan informasi selain oleh Perangkat Daerah sebagaimana dimaksud dalam Pasal 14 ayat (3) harus berkoordinasi dengan Pejabat Pengelola Informasi dan Dokumentasi Pemerintah Daerah.

BAB VI

PORTAL *WEB* PEMERINTAH DAERAH

Pasal 16

(1) Portal *web* resmi Pemerintah Daerah dikelola oleh Dinas.

(2) Nama domain *website* resmi Pemerintah Daerah adalah *www.banten.go.id*.

(3) Nama sub domain portal resmi Pemerintah Daerah adalah *portal.banten.go.id*.

(4) Situs *web* Perangkat Daerah dikelola oleh setiap Perangkat Daerah.

(5) Nama domain situs *web* Perangkat Daerah di Pemerintah Daerah yang menggunakan nama domain sebagaimana dimaksud pada ayat (1) diletakkan di depan nama domain Pemerintah Daerah menjadi nama sub domain.

(6) Ketentuan mengenai portal *web* dan tata kelola portal *web* sebagaimana dimaksud pada ayat (1), tercantum dalam Lampiran V yang merupakan bagian tidak terpisahkan dari Peraturan Gubernur ini.

Pasal 17

(1) Portal *web* Pemerintah Daerah sebagaimana dimaksud dalam Pasal 16 ayat (1) dilaksanakan oleh setiap Perangkat Daerah.

(2) Setiap Perangkat Daerah dalam mengembangkan situs *web* harus berkordinasi dengan Dinas.

BAB VII

SURAT ELEKTRONIK *(e-Mail)* PEMERINTAH DAERAH

Pasal 18

(1) Alamat surat elektronik resmi Pemerintah Daerah menggunakan nama domain *mail.banten.go.id*.

(2) Akun surat elektronik resmi Pemerintah Daerah menggunakan alamat *@banten.go.id*.

(3) Surat elektronik Pemerintah Daerah diperuntukkan bagi Aparatur Sipil Negara Pemerintah Daerah dengan mengajukan permohonan secara resmi kepada Dinas.
(4) Surat elektronik Pemerintah Daerah sebagaimana dimaksud pada ayat (3) dikelola oleh Dinas.

BAB VIII

PUSAT DATA DAN PUSAT PEMULIHAN BENCANA

Pasal 19

(1) Dinas wajib memiliki rencana keberlangsungan kegiatan untuk menanggulangi gangguan atau bencana sesuai dengan risiko dari dampak yang ditimbulkannya.
(2) Pemerintah Daerah wajib memiliki pusat data (*data center)* dan Pusat Pemulihan Bencana *(Disaster Recovery Center/DRC)* paling lambat Tahun 2019.
(3) Dinas wajib menempatkan pusat data dan pusat pemulihan bencana sebagaimana dimaksud pada ayat (2) di wilayah Daerah.
(4) Pusat data dan pusat pemulihan bencana sebagaimana dimaksud pada ayat (4) digunakan untuk kepentingan penegakan hukum, perlindungan, dan penegakan kedaulatan negara terhadap data warga negaranya.
(5) Pusat data dan pusat pemulihan bencana dikelola oleh Dinas.
(6) Dinas wajib memiliki *Network Operating Center (NOC)* yang merupakan pusat pengendali dan pemantauan seluruh jaringan Pemerintah Daerah.
(7) *Network Operating Center (NOC)* sebagaimana dimaksud pada ayat (6) dikelola oleh Dinas.
(8) Ketentuan mengenai standar pembangunan pusat data *(data center)* dan pusat pemulihan bencana *(Disaster Recovery Center/DRC)* sebagaimana dimaksud pada ayat (3), tercantum dalam Lampiran II yang merupakan bagian tidak terpisahkan dari Peraturan Gubernur ini.

BAB IX

KETERHUBUNGAN ANTAR SISTEM INFORMASI

(INTEROPERABILITAS)

Pasal 20

(1) Ruang lingkup interoperabilitas yaitu untuk setiap Sistem Informasi yang diselenggarakan oleh Pemerintah Daerah.
(2) Kebijakan tentang interoperabilitas ini menjadi tugas pokok Dinas.

(3) Standar Acuan yang digunakan terkait interoperabilitas ini dibuat diubah dan ditetapkan oleh Dinas.

(4) Hal-hal Teknis yang digunakan terkait interoperabilitas ini dibuat diubah dan ditetapkan oleh Dinas.

(5) Pengelolan hak akses untuk setiap *Application Programming Interface (API)* dibuat diubah dan ditetapkan oleh Dinas.

(6) Permohonan Hak Akses untuk setiap *Application Programming Interface (API)* dibuat, diubah, dan ditetapkan oleh Dinas.

(7) Setiap pihak yang terkait berkewajiban menggunakan *standard* yang telah ditetapkan sebagaimana tercantum dalam Lampiran VI yang merupakan bagian tidak terpisahkan dari Peraturan Gubernur ini.

BAB X

SUMBER DAYA MANUSIA

Pasal 21

(1) PSE wajib memiliki Sumber Daya Manusia TIK.

(2) Sumber Daya Manusia TIK dapat menggunakan tenaga non Pegawai Negeri Sipil sesuai dengan standar kompetensi yang dibutuhkan.

(3) Pengembangan kompetensi Sumber Daya Manusia TIK di setiap PSE dilakukan dengan cara antara lain:

a. menaikkan jenjang pendidikan formal;

b. bimbingan teknis; dan

c. pendidikan dan latihan teknis.

(4) Penyelenggaraan pengembangan Sumber Daya Manusia TIK di setiap PSE sebagaimana dimaksud pada ayat (3) dilaksanakan oleh Badan Pengembangan Sumber Daya Manusia Daerah Provinsi Banten.

(5) Dalam hal promosi ataupun mutasi pada setiap Sumber Daya Manusia TIK di PSE, pimpinan Perangkat Daerah menjamin keberlangsungan sistem melalui SOP.

(6) Dinas harus memiliki Sumber Daya Manusia TIK yang memiliki kompetensi sebagai analis sistem sebagai:

a. pelaksana pendampingan pengembangan sistem elektronik di setiap PSE; dan

b. pelaksana evaluasi penyelenggaraan sistem elektronik yang dimiliki oleh Daerah.

BAB XI

STANDAR OPERASIONAL PROSEDUR

Pasal 22

(1) SOP untuk mengatur serangkaian perangkat dan prosedur elektronik, yang berfungsi mempersiapkan, mengumpulkan, dan mengolah informasi elektronik.
(2) SOP disusun oleh Penyelenggara sistem elektronik.
(3) Penyusunan SOP sebagaimana dimaksud pada ayat (2) dikordinasikan pada Dinas.
(4) SOP sebagaimana dimaksud pada ayat (2) ditetapkan oleh Kepala Perangkat Daerah.

Pasal 23

(1) Setiap PSE membuat SOP sesuai sistem elektroniknya.
(2) Setiap proses pembuatan SOP paling sedikit memuat unsur penanggungjawab, waktu, dan urutan serta disahkan oleh kepala Perangkat Daerah.
(3) Setiap SOP yang diterbitkan bisa disosialisasikan dan dilakukan pengawasan pelaksanaannya.
(4) Setiap PSE melakukan peninjauan terhadap SOP dalam satu tahun sekali dan jika perlu dilakukan perbaikan.

BAB XII

PEMBINAAN DAN PENGAWASAN

Pasal 24

(1) Pembinaan, Pengawasan, dan Pengendalian penyelenggaraan *e-Government* dilaksanakan oleh Sekretariat Daerah melalui Dinas dan bisa melibatkan pihak lain sesuai kebutuhan dan peraturan yang berlaku.
(2) Pembinaan sebagaimana dimaksud pada ayat (1) melalui:
a. koordinasi pelaksanaan teknis;

b. pemberian bimbingan dan supervisi teknis berpedoman pada regulasi Pemerintah Pusat, standar Internasional serta kaidah keilmuan terkait pengembangan dan layanan TIK.

(3) Pengawasan sebagaimana dimaksud pada ayat (1) melalui:
   a. pembinaan kesadaran hukum bagi aparatur dan masyarakat;
   b. peningkatan profesionalisme aparatur pelaksana; dan
   c. peningkatan peran dan fungsi pelaporan.

BAB XIII

KETENTUAN PENUTUP

Pasal 25

Peraturan Gubernur ini mulai berlaku pada tanggal diundangkan.

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

Ditetapkan di Serang
pada tanggal 20 Februari 2018

GUBERNUR BANTEN,

ttd

WAHIDIN HALIM

Diundangkan di Serang
pada tanggal 20 Februari 2018

SEKRETARIS DAERAH
PROVINSI BANTEN,

ttd

RANTA SOEHARTA

BERITA DAERAH PROVINSI BANTEN TAHUN 2018 NOMOR 7

Salinan sesuai dengan aslinya
KEPALA BIRO HUKUM

ttd

AGUS MINTONO, SH.M.Si
Pembina Tk. I
NIP. 19680805 199803 1 010

LAMPIRAN I

PERATURAN GUBERNUR BANTEN
NOMOR 7 TAHUN 2018
TENTANG
TATA KELOLA SISTEM ELEKTRONIK DI LINGKUNGAN PEMERINTAH PROVINSI BANTEN

STANDAR KEAMANAN INFORMASI

1. TUJUAN

Standar ini digunakan sebagai pedoman dalam rangka melindungi asset informasi Pemerintah Daerah dari berbagai bentuk ancaman baik dari dalam maupun luar Pemerintah Daerah, yang dilakukan secara sengaja maupun tidak sengaja. Pengamanan dan perlindungan ini diberikan untuk menjamin kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*) aset informasi agar selalu terjaga dan terpelihara dengan baik.

2. RUANG LINGKUP

a. Standard ini berlaku untuk pengelolaan pengamanan seluruh aset informasi Pemerintah Daerah dan dilaksanakan oleh seluruh unit kerja pegawai Pemerintah Daerah baik sebagai pengguna maupun pengelola TIK, dan pihak ketiga di lingkungan Pemerintah Daerah.
b. Aset informasi Pemerintah Daerah adalah aset dalam bentuk:
    1) Seluruh data/dokumen/informasi sebagaimana diatur dalam klasifikasi informasi yang berlaku;
    2) Piranti lunak, meliputi aplikasi, sistem operasi, sistem basis data, dan alat bantu (*tools*) aplikasi;
    3) Aset fisik, meliputi perangkat komputer, perangkat jaringan dan komunikasi, media penyimpanan (*storage*), media lepas pasang (*removable media)*, dan perangkat pendukung (*peripheral*); dan
    4) Aset tak berwujud (*intangible*), meliputi pengetahuan, pengalaman, keahlian, citra, dan reputasi.

3. KEBIJAKAN

a. Setiap Pimpinan Perangkat Daerah dan Unit Kerja bertanggung jawab mengatur penerapan Kebijakan dan Standar Keamanan

Informasi yang ditetapkan dalam Peraturan Gubernur ini di Unit Kerja masing-masing.

b. Perangkat Daerah dan Unit Kerja harus menerapkan Kebijakan dan Standar Keamanan Informasi yang ditetapkan dalam Peraturan Gubernur ini di Unit masing-masing.
c. Setiap Pimpinan Perangkat Daerah dan Unit Kerja bertanggung jawab mengatur pelaksanaan pengamanan dan perlindungan aset informasi di Unit masing-masing dengan mengacu pada Kebijakan dan Standar Keamanan Informasi di Pemerintah Daerah yang ditetapkan dalam Peraturan Gubernur ini.
d. Dinas dan Perangkat Daerah bertanggung jawab meningkatkan pengetahuan, keterampilan, dan kepedulian terhadap keamanan informasi pada seluruh pengguna di lingkungan Perangkat Daerah masing-masing.
e. Dinas dan Perangkat Daerah menerapkan dan mengembangkan manajemen risiko dalam rangka pelaksanaan pengamanan dan perlindungan aset informasi.
f. Pihak ketiga harus bertanggung jawab untuk melindungi kerahasiaan, keutuhan, dan/atau ketersediaan aset informasi Pemerintah Daerah.
g. Dinas dan Perangkat Daerah melakukan evaluasi terhadap pelaksanaan Keamanan Informasi secara berkala untuk menjamin efektivitas dan meningkatkan keamanan informasi.
h. Inspektorat Daerah Provinsi Banten melakukan audit internal Keamanan Informasi di Pemerintah Daerah untuk memastikan pengendalian, proses, dan prosedur Keamanan Informasi dilaksanakan secara efektif sesuai dengan Kebijakan dan Standar Keamanan Informasi di Pemerintah Daerah.
i. Dinas dan Perangkat Daerah menggunakan laporan audit internal Keamanan Informasi untuk meninjau efektivitas penerapan Keamanan Informasi dan melakukan tindak lanjut terhadap temuan auditor.

4. TANGGUNG JAWAB

a. Pihak-pihak yang terkait dalam keamanan informasi terdiri atas:
    1) Pemilik aset informasi adalah Pimpinan Perangkat Daerah yang memiliki kebutuhan akan keamanan informasi untuk mendukung tugas dan fungsinya;

2) Petugas keamanan informasi adalah pegawai Pemerintah Daerah dan/atau Pihak Ketiga yang melaksanakan tanggung jawab terkait keamanan informasi;
3) Tim pengendali mutu keamanan informasi (*information security assurance*) adalah tim yang dibentuk untuk melaksanakan kegiatan penjaminan keamanan informasi;
4) Pengguna adalah pegawai dan bukan pegawai Pemerintah Daerah yang mengakses informasi Pemerintah Daerah.

b. Pemilik aset informasi mempunyai tanggung jawab terhadap:
1) Menetapkan target keamanan informasi setiap tahunnya dan menyusun rencana kerja untuk Pemerintah Daerah, masing-masing Perangkat Daerah, maupun yang bersifat lintas unit;
2) Memastikan efektivitas dan konsistensi penerapan Kebijakan dan Standar Keamanan Informasi di Pemerintah Daerah; dan
3) Melaporkan kinerja penerapan Kebijakan dan Standar Keamanan Informasi di Pemerintah Daerah dan pencapaian target kepada tim pengendali mutu keamanan informasi (*information security assurance)*.

c. Petugas keamanan informasi mempunyai tanggung jawab terhadap:
1) Melaksanakan dan mengawasi penerapan Kebijakan dan Standar Keamanan Informasi di Pemerintah Daerah;
2) Memberi masukan peningkatan terhadap Kebijakan dan Standar Keamanan Informasi di Pemerintah Daerah;
3) Mendefinisikan kebutuhan, merekomendasikan, dan mengupayakan penyelenggaraan pendidikan dan pelatihan keamanan informasi bagi pegawai;
4) Memantau, mencatat, dan menguraikan secara jelas gangguan keamanan informasi yang diketahui atau laporan yang diterima, dan menindaklanjuti laporan tersebut sesuai prosedur pelaporan gangguan keamanan informasi; dan
5) Memberi panduan dan/atau bantuan penyelesaian masalah masalah keamanan informasi.

d. Tim pengendali mutu keamanan informasi (*information security assurance*) mempunyai tanggung jawab terhadap:
1) Pendampingan dan penjaminan keamanan informasi;

2) Penyusunan laporan evaluasi pengendali mutu keamanan informasi (*information security assurance*).

e. Pengguna mempunyai tanggung jawab terhadap pemberian masukan kepada pemilik aset informasi dan petugas keamanan informasi terkait keamanan informasi.

5. STANDAR

a. Standar Keamanan Informasi terdiri atas:
   1) Standar Manajemen Keamanan Informasi;
   2) Standar Pengendalian Pengelolaan Aset Informasi;
   3) Standar Pengendalian Keamanan Sumber Daya Manusia;
   4) Standar Pengendalian Keamanan Fisik dan Lingkungan;
   5) Standar Pengendalian Pengelolaan Komunikasi dan Operasional;
   6) Standar Pengendalian Akses;
   7) Standar Pengendalian Keamanan Informasi dalam Pengadaan, Pengembangan, dan Pemeliharaan Sistem informasi;
   8) Standar Pengendalian Pengelolaan Gangguan Keamanan Informasi;
   9) Standar Pengendalian Keamanan Informasi dalam Pengelolaan Kelangsungan Kegiatan; dan
   10) Standar Pengendalian Kepatuhan.

b. Standar Manajemen Keamanan Informasi
   1) Catatan Penerapan Kebijakan dan Standar Keamanan Informasi di Pemerintah Daerah
      a) Dinas dan Perangkat Daerah harus menggunakan catatan penerapan Kebijakan dan Standar Keamanan Informasi di Pemerintah Daerah untuk mengukur kepatuhan dan efektivitas penerapan keamanan informasi.
      b) Catatan penerapan Kebijakan dan Standar Keamanan Informasi di Pemerintah Daerah harus meliputi:
         1) Formulir-formulir sesuai prosedur operasional yang dijalankan;
         2) Catatan gangguan keamanan informasi;
         3) Catatan dari sistem;

4) Catatan pengunjung di area aman (*secure areas*);
5) Kontrak dan perjanjian layanan;
6) Perjanjian kerahasiaan (*confidentiality agreements*); dan
7) Laporan audit.

2) Penyusunan dokumen pendukung kebijakan keamanan informasi harus memuat:
a) Tujuan dan ruang lingkup dokumen pendukung kebijakan keamanan informasi;
b) Kerangka kerja setiap tujuan sasaran pengendalian keamanan informasi;
c) Metodologi penilaian risiko (*risk assessment*);
d) Penjelasan singkat mengenai standar, prosedur, dan kepatuhan termasuk persyaratan peraturan yang harus dipenuhi, pengelolaan kelangsungan kegiatan, konsekuensi apabila terjadi pelanggaran;
e) Tanggung jawab dari setiap bagian terkait; dan
f) Dokumen referensi yang digunakan dalam menyusun dokumen pendukung kebijakan keamanan informasi.

3) Pengendalian Dokumen
a) Dinas dan Perangkat Daerah harus mengendalikan dokumen keamanan informasi Pemerintah Daerah untuk menjaga kemutakhiran dokumen, efektivitas pelaksanaan operasional, menghindarkan dari segala jenis kerusakan, dan mencegah akses oleh pihak yang tidak berwenang.
b) Dinas dan Perangkat Daerah harus menempatkan dokumen keamanan informasi Pemerintah Daerah di semua area operasional sehingga mudah diakses oleh pengguna di unit kerja masing-masing sesuai peruntukannya.

c. Standar Pengendalian Pengelolaan Aset Informasi
1) Pemilik Aset Informasi menetapkan dan mengkaji secara berkala klasifikasi aset informasi dan jenis perlindungan keamanannya.
2) Pemilik Aset Informasi menetapkan pihak yang berwenang untuk mengakses aset informasi.

3) Dalam pengelolaan aset informasi Pemerintah Daerah, aset informasi diklasifikasikan mengacu kepada peraturan perundang-undangan.

d. Standar Pengendalian Keamanan Sumber Daya Manusia

1) Peran dan tanggung jawab pegawai terhadap keamanan informasi harus menjadi bagian dari penjabaran tugas dan fungsi, khususnya bagi yang memiliki akses terhadap aset informasi;

2) Pimpinan dari pegawai berkeahlian khusus atau yang berada diposisi kunci (*key person*) harus memastikan ketersediaan pengganti pegawai tersebut dengan kompetensi yang setara apabila pegawai yang bersangkutan mutasi/berhenti;

Peran dan tanggung jawab pegawai terhadap keamanan informasi harus menyertakan persyaratan untuk:

a) Melaksanakan dan bertindak sesuai dengan tanggung jawabnya terkait keamanan informasi;

b) Melindungi aset dari akses yang tidak sah, penyingkapan, modifikasi, kerusakan atau gangguan;

c) Melaksanakan proses keamanan atau kegiatan keamanan informasi sesuai dengan peran dan tanggung jawabnya;

d) Melaporkan kejadian, potensi kejadian, atau risiko keamanan informasi sesuai dengan Kebijakan dan Standar Keamanan Informasi di Pemerintah Daerah; dan

e) Peran dan tanggung jawab pegawai terhadap keamanan informasi harus menyertakan persyaratan untuk Pemeriksaan latar belakang calon pegawai dan pihak ketiga Pemerintah Daerah harus memperhitungkan privasi, perlindungan data pribadi dan/atau pekerjaan berdasarkan peraturan perundang-undangan, meliputi:

1) Ketersediaan referensi, dari referensi hubungan kerja, dan referensi pribadi;

2) Pemeriksaan kelengkapan dan ketepatan dari riwayat hidup pemohon;

3) Konfirmasi kualifikasi akademik dan profesional yang diklaim;

4) Pemeriksaan identitas (KTP, paspor atau dokumen sejenis); dan
5) Pemeriksaan lebih rinci, seperti pemeriksaan catatan kriminal.

e. Standar Pengendalian Keamanan Fisik dan Lingkungan

1) Pengamanan Perangkat

a) Penempatan dan perlindungan perangkat

Penempatan dan perlindungan perangkat harus mencakup:

1) Perangkat harus diletakkan pada lokasi yang meminimalkan akses yang tidak perlu ke dalam area kerja;
2) Perangkat pengolah informasi yang menangani informasi sensitif harus diposisikan dan dibatasi arah sudut pandangnya untuk mengurangi risiko informasi dilihat oleh pihak yang tidak berwenang selama digunakan, dan perangkat penyimpanan diamankan untuk menghindari akses oleh pihak yang tidak berwenang;
3) Perangkat yang memerlukan perlindungan khusus seperti perangkat cetak khusus, perangkat jaringan di luar ruang server harus terisolasi;
4) Langkah-langkah pengendalian dilakukan untuk meminimalkan risiko potensi ancaman fisik, seperti pencurian, api, bahan peledak, asap, air termasuk kegagalan penyediaan air, debu, getaran, efek kimia, gangguan pasokan listrik, gangguan komunikasi, radiasi elektromagnetis, dan perusakan;
5) Kondisi lingkungan, seperti suhu dan kelembaban harus dimonitor untuk mencegah perubahan kondisi yang dapat mempengaruhi pengoperasian perangkat pengolah informasi;
6) Perlindungan petir harus diterapkan untuk semua bangunan dan filter perlindungan petir harus dipasang untuk semua jalur komunikasi dan listrik; dan

7) Perangkat pengolah informasi sensitif harus dilindungi untuk meminimalkan risiko kebocoran informasi.

b) Penyediaan perangkat pendukung

Perangkat pendukung harus dipasang untuk menjamin beroperasinya perangkat pengolah informasi dan secara berkala harus diperiksa dan diuji ulang kinerjanya.

c) Pengamanan kabel

Perlindungan keamanan kabel mencakup:

1) Pemasangan kabel sumber daya listrik dan kabel telekomunikasi ke perangkat pengolah informasi selama memungkinkan harus terletak di bawah tanah, atau menerapkan alternatif perlindungan lain yang memadai;
2) Pemasangan kabel jaringan harus dilindungi dari penyusupan yang tidak sah atau kerusakan, misalnya dengan menggunakan *conduit* atau menghindari rute melalui area publik;
3) Pemisahan antara kabel sumber daya listrik dengan kabel telekomunikasi untuk mencegah interferensi;
4) Penandaan/penamaan kabel dan perangkat harus diterapkan secara jelas untuk memudahkan penanganan kesalahan;
5) Penggunaan dokumentasi daftar panel *patch* diperlukan untuk mengurangi kesalahan; dan
6) Pengendalian untuk sistem informasi yang sensitif harus mempertimbangkan:
   a) Penggunaan *conduit*;
   b) Penggunaan ruangan terkunci pada tempat inspeksi dan titik pemutusan kabel;
   c) Penggunaan rute alternatif dan/atau media transmisi yang menyediakan keamanan yang sesuai;
   d) Penggunaan kabel fiber optik;
   e) Penggunaan lapisan elektromagnet untuk melindungi kabel;

f) Inisiasi penghapusan teknikal (*technical sweeps*) dan pemeriksaan secara fisik untuk peralatan yang tidak diotorisasi saat akan disambungkan ke kabel; dan

g) Penerapan akses kontrol ke panel *patch* dan ruangan kabel.

d) Pemeliharaan perangkat

1) Perangkat harus dipelihara secara berkala untuk menjamin ketersediaan, keutuhannya (*integrity*), dan fungsinya.

2) Perangkat harus dipelihara sesuai dengan petunjuk manualnya. Untuk pemeliharaan yang dilakukan oleh pihak ketiga, harus diadakan Perjanjian Tingkat Layanan (*Service Level Agreement*/SLA) yang mendefinisikan tingkat pemeliharaan yang disediakan dan tingkat kinerja yang harus dipenuhi pihak ketiga.

3) Pemeliharaan terhadap perangkat keras atau piranti lunak dilakukan hanya oleh pegawai yang berwenang.

4) Dalam hal pemeliharaan perangkat tidak dapat dilakukan di tempat, maka pemindahan perangkat harus mendapatkan persetujuan Pejabat yang berwenang, dan terhadap data yang memiliki klasifikasi sangat rahasia dan rahasia yang disimpan dalam perangkat tersebut harus dipindahkan terlebih dahulu.

5) Otorisasi penggunaan perangkat harus dilakukan secara tertulis dan data-data yang terkait dengan aset informasi yang digunakan, seperti nama pemakai aset, lokasi, dan tujuan penggunaan aset, harus dicatat dan disimpan.

e) Pengamanan perangkat di luar Pemerintah Daerah

Penggunaan perangkat yang dibawa ke luar dari Pemerintah Daerah harus disetujui oleh Pejabat yang berwenang.

f) Pengamanan penggunaan kembali atau penghapusan/pemusnahan perangkat

Perangkat pengolah informasi penyimpan data yang sudah tidak digunakan harus disanitasi (*sanitized*) sebelum digunakan kembali atau dihapuskan/dimusnahkan

2) Pengamanan Area
   a) Seluruh pegawai, pihak ketiga, dan tamu yang memasuki lingkungan Pemerintah Daerah harus mematuhi aturan yang berlaku di Pemerintah Daerah.
   b) Dinas dan Perangkat Daerah menyimpan perangkat pengolah informasi di ruangan khusus yang dilindungi dengan pengamanan fisik yang memadai antara lain pintu elektronik, sistem pemadam kebakaran, alarm bahaya, dan perangkat pemutus aliran listrik;
   c) Akses ke ruang server, data center, dan area kerja yang berisikan aset informasi yang memiliki klasifikasi sangat rahasia dan rahasia harus dibatasi dan hanya diberikan kepada pegawai yang berwenang;
   d) Pihak ketiga yang memasuki ruang server, pusat data *(data center)*, dan area kerja yang berisikan aset informasi yang memiliki klasifikasi sangat rahasia dan rahasia harus didampingi pegawai Dinas dan/atau Perangkat Daerah sepanjang waktu kunjungan. Waktu masuk dan keluar serta maksud kedatangan harus dicatat dalam buku catatan kunjungan;
   e) Kantor, ruangan, dan perangkat yang berisikan aset informasi yang memiliki klasifikasi sangat rahasia dan rahasia harus dilindungi secara memadai;
   f) Pegawai dan pihak ketiga tidak diizinkan merokok, makan, minum di ruang server, dan pusat data *(data center)*; dan
   g) Area keluar masuk barang dan area publik harus selalu dijaga, diawasi dan dikendalikan, dan jika memungkinkan disterilkan dari perangkat pengolah informasi untuk menghindari akses oleh pihak yang tidak berwenang.

3) Pengamanan Kantor, Ruangan, dan Fasilitas

   Pengamanan kantor, ruangan, dan fasilitas mencakup:

a) Pengamanan kantor, ruangan, dan fasilitas harus sesuai dengan peraturan dan standar keamanan dan keselamatan kerja yang berlaku;
b) Fasilitas utama harus ditempatkan khusus untuk menghindari akses publik;
c) Pembatasan pemberian identitas atau tanda-tanda keberadaan aktivitas pengolahan informasi; dan
d) Direktori dan buku telepon internal yang mengidentifikasi lokasi perangkat pengolah informasi tidak mudah diakses oleh publik.

4) Perlindungan terhadap Ancaman Eksternal dan Lingkungan

Perlindungan terhadap ancaman eksternal dan lingkungan harus mempertimbangkan:

a) Bahan-bahan berbahaya atau mudah terbakar harus disimpan pada jarak yang aman dari area aman (*secure areas*);
b) Perlengkapan umum, seperti alat tulis, tidak boleh disimpan di dalam area aman (*secure areas*);
c) Perangkat *fallback* dan media cadangan (*media backup*) harus diletakkan pada jarak yang aman untuk menghindari kerusakan dari bencana yang mempengaruhi fasilitas utama; dan
d) Perangkat pemadam kebakaran harus disediakan dan diletakkan di tempat yang tepat dan aman.

f. Standar Pengendalian Pengelolaan Komunikasi dan Operasional

1) Dokumentasi Prosedur Operasional harus mencakup:

a) Tata cara pengolahan dan penanganan informasi;
b) Tata cara menangani kesalahan-kesalahan atau kondisi khusus yang terjadi beserta pihak yang harus dihubungi bila mengalami kesulitan teknis;
c) Cara memfungsikan kembali perangkat dan cara mengembalikan perangkat ke keadaan awal saat terjadi kegagalan sistem;
d) Tata cara pencadangan (*backup*) dan penyimpanan ulang (*restore*); dan

e) Tata cara pengelolaan jejak audit (*audit trails*) pengguna dan catatan kejadian/kegiatan sistem.

2) Pemisahan Perangkat Pengembangan dan Operasional harus mempertimbangkan:
   a) Pengembangan dan operasional piranti lunak harus dioperasikan di sistem atau prosesor komputer dan domain atau direktori yang berbeda;
   b) Instruksi Kerja (*working instruction*) rilis dari pengembangan piranti lunak ke operasional harus ditetapkan dan didokumentasikan;
   c) Penjalan kode program (*compiler*), penyunting (*editor*), dan alat bantu pengembangan lain tidak boleh diakses dan sistem operasional ketika tidak dibutuhkan;
   d) Lingkungan sistem pengujian harus diusahakan sama dengan lingkungan sistem operasional;
   e) Pengguna harus menggunakan profil pengguna yang berbeda untuk sistem pengujian dan sistem operasional, serta aplikasi harus menampilkan pesan identifikasi dari sistem untuk mengurangi risiko kesalahan; dan
   f) Data yang memiliki klasifikasi sangat rahasia dan rahasia tidak boleh disalin ke dalam lingkungan pengujian sistem.

3) Pemantauan dan Pengkajian Layanan Pihak Ketiga
   Pemantauan dan pengkajian layanan dari pihak ketiga, serta laporan dan catatan dari pihak ketiga mencakup proses sebagai berikut:
   a) Pemantauan tingkat kinerja layanan untuk memastikan kesesuaian kepatuhan dengan perjanjian;
   b) Pengkajian laporan layanan pihak ketiga dan pengaturan pertemuan berkala dalam rangka pembahasan perkembangan layanan sebagaimana diatur dalam perjanjian kesepakatan;
   c) Pemberian informasi tentang gangguan keamanan informasi dan pengkajian informasi ini bersama pihak ketiga sebagaimana diatur dalam perjanjian kesepakatan;

d) Pemeriksaan jejak audit pihak ketiga dan pencatatan peristiwa keamanan, masalah operasional, kegagalan, dan gangguan yang terkait dengan layanan yang diberikan; dan
e) Penyelesaian dan pengelolaan masalah yang teridentifikasi.

4) Pengelolaan Keamanan Jaringan mencakup:
a) Pemantauan kegiatan pengelolaan jaringan untuk menjamin bahwa perangkat jaringan digunakan secara efektif dan efisien;
b) Pengendalian dan pengaturan tentang penyambungan atau perluasan jaringan internal atau eksternal Pemerintah Daerah;
c) Pengendalian dan pengaturan akses ke sistem jaringan internal atau eksternal Pemerintah Daerah;
d) Pencatatan informasi pihak ketiga yang diizinkan mengakses ke jaringan Pemerintah Daerah dan menerapkan pemantauan serta pencatatan kegiatan selama menggunakan jaringan.
e) Pemutusan layanan tanpa pemberitahuan sebelumnya jika terjadi gangguan keamanan informasi;
f) Perlindungan jaringan dari akses yang tidak berwenang mencakup:
1) Penetapan untuk penanggung jawab pengelolaan jaringan dipisahkan dari pengelolaan perangkat pengolah informasi;
2) Penerapan pengendalian khusus untuk melindungi keutuhan informasi yang melewati jaringan umum antara lain dengan penggunaan enkripsi dan tanda tangan elektronik (*digital signature*); dan
3) Pendokumentasian arsitektur jaringan seluruh komponen perangkat keras jaringan dan piranti lunak.
g) Penerapan fitur keamanan layanan jaringan mencakup:
1) Teknologi keamanan seperti autentikasi, enkripsi, dan pengendalian sambungan jaringan;

2) Parameter teknis yang diperlukan untuk koneksi aman dengan layanan jaringan sesuai dengan keamanan dan aturan koneksi jaringan; dan
3) Prosedur untuk penggunaan layanan jaringan yang membatasi akses ke layanan jaringan atau aplikasi.

h) Pertukaran Informasi
1) Prosedur pertukaran informasi bila menggunakan perangkat komunikasi elektronik, mencakup:
a) Perlindungan pertukaran informasi dari pencegatan, penyalinan, modifikasi, kesalahan penjaluran (*missrouting*), dan perusakan;
b) Pendeteksian dan perlindungan terhadap kode berbahaya yang dapat dikirim melalui penggunaan komunikasi elektronik;
c) Perlindungan informasi elektronik dalam bentuk lampiran (*attachment*) yang memiliki klasifikasi sangat rahasia dan rahasia;
d) Pertimbangan risiko terkait penggunaan perangkat komunikasi nirkabel.
2) Pertukaran informasi yang tidak menggunakan perangkat komunikasi elektronik, mengacu pada ketentuan yang berlaku;
3) Pengendalian pertukaran informasi bila menggunakan perangkat komunikasi elektronik, mencakup:
a) Pencegahan terhadap penyalahgunaan wewenang pegawai dan pihak ketiga yang dapat membahayakan Organisasi;
b) Penggunaan teknik kriptografi;
c) Penyelenggaraan penyimpanan dan penghapusan/pemusnahan untuk semua korespondensi kegiatan, termasuk pesan, yang sesuai dengan ketentuan yang berlaku;
d) Larangan meninggalkan informasi sensitif pada perangkat pengolah informasi;
e) Pembatasan penerusan informasi secara otomatis;

f) Pembangunan kepedulian atas ancaman pencurian informasi, misalnya terhadap:
   1) Pengungkapan informasi sensitif untuk menghindari mencuri dengar saat melakukan panggilan telepon;
   2) Akses pesan di luar kewenangannya;
   3) Pemrograman mesin faksimili baik sengaja maupun tidak sengaja untuk mengirim pesan ke nomor tertentu;
   4) Pengiriman dokumen dan pesan ke tujuan yang salah.

4) Pembangunan kepedulian atas pendaftaran data demografis, seperti alamat surat elektronik atau informasi pribadi lainnya untuk menghindari pengumpulan informasi yang tidak sah; dan
5) Penyediaan informasi internal Pemerintah Daerah bagi masyarakat umum harus disetujui oleh pemilik informasi dan sesuai dengan ketentuan yang berlaku.

i) Pemantauan

Prosedur pemantauan penggunaan sistem pengolah informasi ditetapkan untuk menjamin agar kegiatan akses yang tidak sah tidak perIu terjadi. Prosedur ini mencakup pemantauan:

1) Kegagalan akses (*access failures*);
2) Pola-pola masuk (*log-on*) yang mengindikasikan penggunaan yang tidak wajar;
3) Alokasi dan penggunaan hak akses khusus (*privileged access capability*);
4) Penelusuran transaksi dan pengiriman dokumen (*file*) tertentu yang mencurigakan; dan
5) Penggunaan sumber daya sensitif.

g. Standar Pengendalian Akses

1) Persyaratan untuk Pengendalian Akses

Perangkat Daerah harus menyusun, mendokumentasikan, dan mengkaji ketentuan akses ke aset informasi berdasarkan

kebutuhan organisasi dan persyaratan keamanan. Persyaratan untuk pengendalian akses mencakup:

a) Penentuan kebutuhan keamanan dari pengolah aset informasi; dan
b) Pemisahan peran pengendalian akses, seperti administrasi akses dan otorisasi akses.

2) Pengelolaan Akses Pengguna

Dinas dan Perangkat Daerah harus menyusun prosedur pengelolaan hak akses pengguna sesuai dengan peruntukannya. Prosedur pengelolaan akses pengguna harus mencakup:

a) Penggunaan akun yang unik untuk mengaktifkan pengguna agar terhubung dengan sistem informasi atau layanan, dan pengguna dapat bertanggung jawab dalam penggunaan sistem informasi atau layanan tersebut. Penggunaan akun khusus hanya diperbolehkan sebatas yang diperlukan untuk kegiatan atau alasan operasional, dan harus disetujui Pejabat yang berwenang serta didokumentasikan;
b) Pemeriksaan bahwa pengguna memiliki otorisasi dari pemilik sistem untuk menggunakan sistem informasi atau layanan, dan jika diperlukan harus mendapat persetujuan yang terpisah dari Pejabat yang berwenang;
c) Pemeriksaan bahwa tingkat akses yang diberikan sesuai dengan tujuan kegiatan dan konsisten dengan Kebijakan dan Standar Keamanan Informasi di lingkungan Pemerintah Daerah;
d) Pemberian pernyataan tertulis kepada pengguna tentang hak aksesnya dan meminta pengguna menandatangani pernyataan ketentuan akses tersebut;
e) Pemastian penyedia layanan tidak memberikan akses kepada pengguna sebelum prosedur otorisasi telah selesai;
f) Pemeliharaan catatan pengguna layanan yang terdaftar dalam menggunakan layanan;

g) Penghapusan atau penonaktifan akses pengguna yang telah berubah tugas dan/atau fungsinya, setelah penugasan berakhir atau mutasi;
h) Pemeriksaan, penghapusan, serta penonaktifan akun secara berkala dan untuk pengguna yang memiliki lebih dari 1 (satu) akun; dan
i) Pemastian bahwa akun tidak digunakan oleh pengguna lain.

3) Pengelolaan Hak Akses Khusus (*privilege management*)

Dinas dan Perangkat Daerah harus membatasi dan mengendalikan penggunaan hak akses khusus. Pengelolaan hak akses khusus harus mempertimbangkan:

a) Hak akses khusus setiap sistem dari pabrikan perlu diidentifikasi untuk dialokasikan/diberikan kepada pengguna yang terkait dengan produk, seperti sistem operasi, sistem pengelolaan basis data, aplikasi;
b) Hak akses khusus hanya diberikan kepada pengguna sesuai dengan peruntukkannya berdasarkan kebutuhan dan kegiatan tertentu;
c) Pengelolaan proses otorisasi dan catatan dari seluruh hak akses khusus yang dialokasikan/diberikan kepada pengguna. Hak akses khusus tidak boleh diberikan sebelum proses otorisasi selesai;
d) Pengembangan dan penggunaan sistem rutin (misal *job scheduling*) harus diutamakan untuk menghindari kebutuhan dalam memberikan hak akses khusus secara terus menerus kepada pengguna;
e) Hak akses khusus harus diberikan secara terpisah dari akun yang digunakan untuk kegiatan umum, seperti akun administrator sistem (*system administrator*), administrator basis data (*database administrator*), dan administrator jaringan (*network administrator*).

4) Kajian Hak Akses Pengguna

Kajian hak akses pengguna harus mempertimbangkan:

a) Hak akses pengguna harus dikaji paling sedikit 6 (enam) bulan sekali atau setelah terjadi perubahan pada sistem, atau struktur Organisasi;
b) Hak akses khusus harus dikaji paling sedikit 6 (enam) bulan sekali dalam jangka waktu lebih sering dibanding jangka waktu pengkajian hak akses pengguna, atau apabila terjadi perubahan pada sistem, atau struktur Organisasi;
c) Pemeriksaan hak akses khusus harus dilakukan secara berkala, untuk memastikan pemberian hak akses khusus telah diotorisasi.

5) Pengendalian Akses Jaringan
a) Menerapkan prosedur otorisasi untuk pemberian akses ke jaringan dan layanan jaringan;
b) Menerapkan teknik autentikasi akses dari koneksi eksternal, seperti teknik kriptografi; dan
c) Melakukan penghentian isolasi layanan jaringan pada area jaringan yang mengalami gangguan keamanan informasi.

6) Pemisahan dalam Jaringan
Melakukan pemisahan dalam jaringan antara lain:
a) Pemisahan berdasarkan kelompok layanan informasi, pengguna, dan aplikasi; dan
b) Pemberian akses jaringan kepada tamu, hanya dapat diberikan akses terbatas misalnya internet dan/atau surat elektronik tanpa bisa terhubung ke jaringan internal Pemerintah Daerah.

7) Perangkat Kerja Bergerak dan Jarak Jauh (*Mobile Computing* dan *Teleworking*)
a) Penggunaan perangkat kerja bergerak dan jarak jauh (*mobile computing* dan *teleworking*) harus mempertimbangkan:
1) Memenuhi keamanan informasi dalam penentuan lokasi;
2) Menjaga keamanan akses;
3) Menggunakan anti kode berbahaya (*malicious code*);
4) Memakai piranti lunak berlisensi;

5) Mendapat persetujuan Pejabat yang berwenang/atasan langsung pegawai; dan

6) Pencabutan hak akses dan pengembalian fasilitas perangkat jarak jauh (*teleworking*) apabila kegiatan telah selesai.

h. Standar Pengendalian Keamanan Informasi dalam Pengadaan, Pengembangan, dan Pemeliharaan Sistem Informasi

1) Spesifikasi kebutuhan perangkat pengolah informasi yang dikembangkan baik oleh internal atau pihak ketiga harus didokumentasikan secara formal.

2) Pengolahan Data pada Aplikasi

a) Pemeriksaan data masukan harus mempertimbangkan:

1) Penerapan masukan rangkap (*dual input*) atau mekanisme pengecekan masukan Iainnya untuk mendeteksi kesalahan sebagai berikut:

a) Diluar rentang/batas nilai-nilai yang diperbolehkan;

b) Karakter tidak valid dalam field data;

c) Data hilang atau tidak lengkap;

d) Melebihi batas atas dan bawah volume data; dan

e) Data yang tidak diotorisasi dan tidak konsisten.

2) Pengkajian secara berkala terhadap isi field kunci (*key field*) atau dokumen (*file*) data untuk mengkonfirmasi keabsahan dan integritas data;

3) Memeriksa dokumen cetak (*hard copy*) untuk memastikan tidak adanya perubahan data masukan yang tidak melalui otorisasi;

4) Menampilkan pesan yang sesuai dalam menanggapi kesalahan validasi;

5) Prosedur untuk menguji kewajaran dari data masukan;

6) Menguraikan tanggung jawab dari seIuruh pegawai yang terkait dalam proses perekaman data; dan

7) Sistem mampu membuat dan mengeluarkan catatan aktivitas terkait proses perekaman data.

b) Menyusun daftar pemeriksaan (*check list*) yang sesuai, mendokumentasikan proses pemeriksaan, dan menyimpan hasilnya secara aman. Proses pemeriksaan mencakup:
   1) Pengendalian sesi (*session*) atau tumpak (*batch*), untuk mencocokkan data setelah perubahan transaksi;
   2) Pengendalian saldo (*balancing*) untuk memeriksa data sebelum dan sesudah transaksi;
   3) Validasi data masukan yang dihasilkan sistem;
   4) Keutuhan dan keaslian data yang diunduh/diunggah (*download/upload*);
   5) *Hash tools* dari rekaman (*record*) dan dokumen (*file*);
   6) Aplikasi berjalan sesuai dengan rencana dan waktu yang ditentukan;
   7) Program dijalankan dalam urutan yang benar dan menghentikan sementara jika terjadi kegagalan sampai masalah diatasi; dan
   8) Sistem mampu membuat dan mengeluarkan catatan aktivitas pengelolaan internal.

c) Pemeriksaan data keluaran harus mempertimbangkan:
   1) Kewajaran dari data keluaran yang dihasilkan;
   2) Pengendalian rekonsiliasi data untuk memastikan kebenaran pengolahan data;
   3) Menyediakan informasi yang cukup untuk pengguna atau sistem pengolahan informasi untuk menentukan akurasi, kelengkapan, ketepatan, dan klasifikasi informasi;
   4) Prosedur untuk menindaklanjuti validasi data keluaran;
   5) Menguraikan tanggung jawab dari seluruh pegawai yang terkait proses data keluaran; dan
   6) Sistem mampu membuat dan mengeluarkan catatan aktivitas dalam proses validasi data keluaran.

3) Pengendalian dan Penggunaan Kriptografi

Pengembangan dan penerapan sistem kriptografi untuk perlindungan informasi harus mempertimbangkan:

a) Kondisi dari suatu kegiatan yang menentukan bahwa informasi harus dilindungi, seperti risiko kegiatan, media pengiriman informasi, tingkat perlindungan yang dibutuhkan;
b) Tingkat perlindungan yang dibutuhkan harus diidentifikasi berdasarkan penilaian risiko, antara lain jenis, kekuatan, dan kualitas dari algoritma enkripsi yang akan digunakan;
c) Keperluan enkripsi untuk perlindungan informasi sangat rahasia, rahasia, dan terbatas yang melalui perangkat bergerak *(mobile computing)*, media lepas pasang *(removable media)*, atau jalur komunikasi;
d) Pengelolaan kunci kriptografi (*kriptografi key*), seperti perlindungan kunci kriptografi (*kriptografi key*), pemulihan informasi ter-enkripsi dalam hal kehilangan atau kerusakan kunci kriptografi (*kriptografi key*); dan
e) Dampak penggunaan informasi ter-enkripsi, seperti pengendalian terkait pemeriksaan suatu konten, kecepatan pemrosesan pada sistem.

4) Keamanan Dokumen (*File*) Sistem
a) Pengembangan prosedur pengendalian piranti lunak pada sistem operasional harus mempertimbangkan:
1) Proses pemutakhiran piranti lunak operasional, aplikasi, kumpulan program (*library program*) hanya boleh dilakukan oleh administrator sistem terlatih setelah melalui proses otorisasi;
2) Sistem operasional hanya berisi program aplikasi yang dapat dieksekusi (*executable*) yang telah diotorisasi, tidak boleh berisi kode program (*source code*) atau penjalan kode program (*compiler*);
3) Aplikasi dan piranti lunak sistem operasi hanya dapat diimplementasikan setelah melewati proses pengujian yang ekstensif;
4) Sistem pengendalian konfigurasi harus digunakan untuk mengendalikan seluruh piranti lunak yang

telah diimplementasikan beserta dokumentasi sistem;

5) *Strategi rollback* harus tersedia sebelum suatu perubahan diimplementasikan;
6) Catatan audit harus dipelihara untuk menjaga kemutakhiran catatan (*library*) program operasional;
7) Versi terdahulu dari suatu aplikasi harus tetap disimpan untuk keperluan kontinjensi; dan
8) Versi lama dari suatu piranti lunak harus diarsip, bersama dengan informasi terkait dan prosedur, parameter, konfigurasi rinci, dan piranti lunak pendukung.

b) Perlindungan terhadap sistem pengujian data harus mempertimbangkan:
   1) Prosedur pengendalian akses yang berlaku pada sistem aplikasi operasional, harus berlaku juga pada sistem aplikasi pengujian;
   2) Proses otorisasi setiap kali informasi/data operasional digunakan pada sistem pengujian;
   3) Penghapusan informasi/data operasional yang digunakan pada sistem pengujian segera setelah proses pengujian selesai; dan
   4) Pencatatan jejak audit penggunaan informasi/data operasional.

c) Pengendalian akses ke kode program (*source code*) harus mempertimbangkan:
   1) Kode program (*source code*) tidak boleh disimpan pada sistem operasional;
   2) Pengelolaan kode program (*source code*) dan catatan (*library*) harus mengikuti prosedur yang telah ditetapkan;
   3) Pengelola TIK tidak boleh memiliki akses yang tidak terbatas ke kode program (*source code*) dan catatan (*library*);
   4) Proses pemutakhiran kode program (*source code*) dan item terkait, serta pemberian kode program (*source*

code) kepada programmer hanya dapat dilakukan setelah melalui proses otorisasi;

5) Daftar (*listing*) program harus disimpan dalam area aman (*secure areas*);
6) Catatan audit dari seluruh akses ke kode program (*source code*) library harus dipelihara; dan
7) Pemeliharaan dan penyalinan kode program (*source code*) library harus mengikuti prosedur pengendalian perubahan.

5) Keamanan dalam proses pengembangan dan pendukung (*support proceses*)
   a) Prosedur pengendalian perubahan sistem operasi dan piranti lunak, mencakup:
      1) Memelihara catatan persetujuan sesuai dengan kewenangannya;
      2) Memastikan permintaan perubahan diajukan oleh pihak yang berwenang;
      3) Melakukan kaji ulang (*revieu*) untuk memastikan bahwa tidak ada penurunan kualitas prosedur pengendalian dan integritas akibat permintaan perubahan;
      4) Melakukan identifikasi terhadap piranti lunak, informasi, basis data, dan perangkat keras yang perlu diubah;
      5) Mendapatkan persetujuan formal dari pihak yang berwenang sebelum pelaksanaan perubahan;
      6) Memastikan pihak yang berwenang menerima perubahan yang diminta sebelum dilakukan implementasi;
      7) Memastikan bahwa dokumentasi sistem mutakhir dan dokumen versi sebelumnya diarsip;
      8) Memelihara versi perubahan aplikasi;
      9) Memelihara jejak audit perubahan aplikasi;
      10) Memastikan dokumentasi penggunaan dan prosedur telah diubah sesuai dengan perubahan yang dilaksanakan; dan

11) Memastikan bahwa implementasi perubahan dilakukan pada waktu yang tepat dan tidak menganggu kegiatan.

b) Prosedur kajian teknis aplikasi setelah perubahan sistem operasi dan/atau piranti lunak, mencakup:
   1) Melakukan kaji ulang untuk memastikan bahwa tidak ada penurunan kualitas prosedur pengendalian dan integritas akibat permintaan perubahan;
   2) Memastikan rencana dan anggaran yang mencakup kaji ulang dan pengujian sistem dari perubahan sistem operasi;
   3) Memastikan pemberitahuan perubahan sistem informasi dilakukan dalam jangka waktu yang tepat untuk memastikan tes dan kaji ulang telah dilaksanakan sebelum implementasi; dan
   4) Memastikan bahwa perubahan telah diselaraskan dengan rencana kelangsungan kegiatan.

c) Kebocoran informasi

   Pengendalian yang dapat diterapkan untuk membatasi risiko kebocoran informasi, antara lain:
   1) Melakukan pemantauan terhadap sistem dan aktivitas pegawai dan pihak ketiga, sesuai dengan ketentuan yang berlaku; dan
   2) Melakukan pemantauan terhadap aktivitas penggunaan komputer personal (*desktop*) dan perangkat bergerak (*mobile*).

d) Pengembangan piranti lunak oleh pihak ketiga harus mempertimbangkan:
   1) Perjanjian lisensi, kepemilikan kode program (*source code*), dan Hak Atas Kekayaan Intelektual (HAKI);
   2) Perjanjian *escrow*;
   3) Hak untuk melakukan audit terhadap kualitas dan akurasi pekerjaan;
   4) Persyaratan kontrak mengenai kualitas dan fungsi keamanan aplikasi;

5) Uji coba terhadap aplikasi untuk memastikan tidak terdapat kode berbahaya (*malicious code*) sebelum implementasi.

e) Pengelolaan Kerentanan Teknis, mencakup:

1) Penunjukan fungsi dan tanggung jawab yang terkait dengan pengelolaan kerentanan teknis termasuk di dalamnya pemantauan kerentanan, penilaian risiko kerentanan, patching, registrasi aset, dan koordinasi dengan pihak terkait;
2) Pengidentifikasian sumber informasi yang dapat digunakan untuk meningkatkan kepedulian terhadap kerentanan teknis;
3) Penentuan rentang waktu untuk melakukan aksi terhadap munculnya potensi kerentanan teknis. Apabila terjadi kerentanan teknis yang butuh penanganan maka harus diambil tindakan sesuai kontrol yang telah ditetapkan atau melaporkan kejadian tersebut melalui pelaporan kejadian dan kelemahan keamanan informasi;
4) Pengujian dan evaluasi penggunaan *patch* sebelum proses instalasi untuk memastikan *patch* dapat bekerja secara efektif dan tidak menimbulkan risiko yang lain. Apabila *patch* tidak tersedia, harus melakukan hal sebagai berikut:
   a) Mematikan layanan (*services*) yang berhubungan dengan kerentanan;
   b) Menambahkan pengendalian akses seperti *firewall*;
   c) Meningkatkan pengawasan untuk mengidentifikasi atau mencegah terjadinya serangan atau kejadian;
   d) Meningkatkan kepedulian terhadap kerentanan teknis;
5) Penyimpanan catatan audit (*audit log*) yang memuat prosedur dan langkah-langkah yang telah diambil;

6) Pemantauan dan evaluasi terhadap pengelolaan kerentanan teknis harus dilakukan secara berkala; dan
7) Pengelolaan kerentanan teknis diutamakan terhadap sistem informasi yang memiliki tingkat risiko tinggi.

i. Standar Pengendalian Pengelolaan Gangguan Keamanan Informasi

1) Pelaporan Kejadian dan Kelemahan Keamanan Informasi

a) Gangguan keamanan informasi antara lain:
1) Hilangnya layanan, perangkat, atau fasilitas TIK;
2) Kerusakan fungsi sistem atau kelebihan beban;
3) Perubahan sistem di luar kendali;
4) Kerusakan fungsi piranti lunak atau perangkat keras;
5) Pelanggaran akses ke dalam sistem pengolah informasi TIK;
6) Kelalaian manusia; dan
7) Ketidaksesuaian dengan ketentuan yang berlaku.

b) Pegawai dan pihak ketiga harus melaporkan kepada Dinas dan Perangkat Daerah sesegera mungkin pada saat menemui kelemahan atau terjadi gangguan keamanan informasi dalam sistem atau layanan TIK Pemerintah Daerah.

c) Pelaporan gangguan harus mencakup:
1) Proses umpan balik yang sesuai untuk memastikan bahwa pihak yang melaporkan kejadian keamanan informasi mendapatkan pemberitahuan penanganan masalah;
2) Formulir laporan gangguan keamanan informasi untuk mendukung tindakan pelaporan dan membantu pelapor mengingat kronologis kejadian keamanan informasi;
3) Perilaku yang benar dalam menghadapi gangguan keamanan informasi, antara lain:
a) Mencatat semua rincian penting gangguan dengan segera, seperti jenis pelanggaran, jenis

kerusakan, pesan pada layar, atau anomali sistem; dan

b) Segera melaporkan gangguan ke pihak berwenang sebelum melakukan tindakan penanganan sendiri.

d) Sebagai referensi yang digunakan dalam proses penanganan pelanggaran disiplin bagi pegawai dan pihak ketiga yang melakukan pelanggaran keamanan informasi.

2) Pengelolaan Gangguan Keamanan Informasi dan Perbaikannya

a) Dinas dan Perangkat Daerah masing-masing harus menyusun prosedur dan menguraikan tanggung jawab pegawai, terkait dalam rangka memastikan gangguan keamanan informasi dapat ditangani secara cepat dan efektif;

b) Prosedur pengelolaan gangguan keamanan informasi harus mempertimbangkan:

1) Prosedur yang harus ditetapkan untuk menangani berbagai jenis gangguan keamanan informasi, antara lain:

a) Kegagalan sistem informasi dan hilangnya layanan;

b) Serangan program yang membahayakan (*malicious code*);

c) Serangan *denial* of *service*;

d) Kesalahan akibat data tidak lengkap atau tidak akurat;

e) Pelanggaran kerahasiaan dan keutuhan; dan

f) Penyalahgunaan sistem informasi.

2) Untuk melengkapi rencana kontijensi, prosedur harus mencakup:

a) Analisis dan identifikasi penyebab gangguan;

b) Mengkarantina atau membatasi gangguan;

c) Perencanaan dan pelaksanaan tindakan korektif untuk mencegah gangguan berulang;

d) Komunikasi dengan pihak-pihak yang terkena dampak pemulihan gangguan; dan
e) Pelaporan tindakan ke pihak berwenang.

3) Jejak audit dan bukti serupa harus dikumpulkan dan diamankan untuk:
a) Analisis masalah internal;
b) Digunakan sebagai bukti forensik yang berkaitan dengan potensi pelanggaran kontrak atau peraturan atau persyaratan dalam hal proses pidana atau perdata; dan
c) Digunakan sebagai bahan tuntutan ganti rugi pada pihak ketiga yang menyediakan piranti lunak dan layanan.

4) Tindakan untuk memulihkan keamanan dari pelanggaran dan perbaikan kegagalan sistem harus dikendalikan secara hati-hati dan formal, prosedur harus memastikan bahwa:
a) Hanya pegawai yang sudah diidentifikasi dan berwenang yang diizinkan akses langsung ke sistem dan data;
b) Semua tindakan darurat yang diambil, didokumentasikan secara rinci;
c) Tindakan darurat dilaporkan kepada pihak berwenang; dan
d) Keutuhan sistem dan pengendaliannya dikonfirmasikan dengan pihak-pihak terkait sesegera mungkin.

c) Peningkatan penanganan gangguan keamanan informasi

1) Seluruh gangguan keamanan informasi yang terjadi dan tindakan mengatasinya harus dicatat dalam suatu basis data dan/atau buku catatan pelaporan gangguan keamanan informasi, dan akan menjadi masukan pada proses peningkatan penanganan gangguan keamanan informasi;
2) Seluruh catatan gangguan keamanan informasi akan dievaluasi dan dianalisis untuk perbaikan dan

pencegahan agar gangguan keamanan informasi tidak terulang.

d) Pengumpulan bukti pelanggaran

Dinas teknis yang membidangi Komunikasi dan Informatika dan Perangkat Daerah harus mengumpulkan, menyimpan, dan menyajikan bukti pelanggaran terhadap Kebijakan dan Standar Keamanan Informasi di Pemerintah Daerah.

j. Standar Pengendalian Keamanan Informasi dalam Pengelolaan Kelangsungan Kegiatan

1) Perangkat Daerah harus mengelola proses kelangsungan kegiatan pada saat keadaan darurat di Perangkat Daerah masing-masing;

2) Perangkat Daerah harus menyusun dan menerapkan Rencana Kelangsungan Kegiatan untuk menjaga dan mengembalikan kegiatan operasional dalam jangka waktu yang disepakati dan level yang dibutuhkan;

3) Perangkat Daerah harus memelihara dan memastikan rencana-rencana yang termuat dalam Rencana Kelangsungan Kegiatan masih sesuai, dan mengidentifikasi prioritas untuk kegiatan uji coba;

4) Perangkat Daerah harus melakukan uji coba Rencana Kelangsungan Kegiatan secara berkala untuk memastikan Rencana Kelangsungan Kegiatan dapat dilaksanakan secara efektif;

5) Pengelolaan Kelangsungan Kegiatan pada saat Keadaan Darurat.

Komponen yang harus diperhatikan dalam mengelola proses kelangsungan kegiatan:

a) Identifikasi risiko dan analisis dampak yang diakibatkan pada saat terjadi keadaan darurat;

b) Identifikasi seluruh aset informasi yang menunjang proses kegiatan kritikal;

c) Identifikasi sumber daya, mencakup biaya, struktur organisasi, teknis pelaksanaan, pegawai, dan pihak ketiga;

d) Memastikan keselamatan pegawai dan perlindungan terhadap perangkat pengolah informasi dan aset organisasi;
e) Penyusunan dan pendokumentasian Rencana Kelangsungan Kegiatan sesuai dengan Rencana Strategi (Renstra) Pemerintah Daerah; dan
f) Pelaksanaan uji coba dan pemeliharaan Rencana Kelangsungan Kegiatan secara berkala.

6) Proses identifikasi risiko mengikuti ketentuan mengenai Penerapan Manajemen Risiko di Pemerintah Daerah;
7) Proses analisis dampak kegiatan harus melibatkan pemilik proses bisnis dan dievaluasi secara berkala;
8) Penyusunan Rencana Kelangsungan Kegiatan mencakup:
a) Prosedur saat keadaan darurat, mencakup tindakan yang harus dilakukan serta pengaturan hubungan dengan pihak berwenang;
b) Prosedur *fallback*, mencakup tindakan yang harus diambil untuk memindahkan kegiatan kritikal atau layanan pendukung ke lokasi kerja sementara, dan mengembalikan operasional kegiatan kritikal dalam jangka waktu sesuai dengan standar ketersediaan data yang ditetapkan;
c) Prosedur saat kondisi telah normal (*resumption*), adalah tindakan mengembalikan kegiatan operasional ke kondisi normal;
d) Jadwal uji coba, mencakup langkah-langkah, dan waktu pelaksanaan uji coba serta proses pemeliharaannya;
e) Pelaksanaan pelatihan dan sosialisasi dalam rangka meningkatkan kepedulian dan pemahaman proses kelangsungan kegiatan dan memastikan proses kelangsungan kegiatan dilaksanakan secara efektif;
f) Tanggung jawab dan peran setiap Petugas Pelaksana Pengelolaan Proses Kelangsungan;
g) Daftar kebutuhan aset informasi kritikal dan sumber daya untuk dapat menjalankan prosedur saat keadaan

darurat, *fallback*, dan saat kondisi telah normal (*resumption*).

9) Uji Coba Rencana Kelangsungan Kegiatan harus dilaksanakan untuk memastikan setiap rencana yang disusun dapat dilakukan/dipenuhi pada saat penerapannya. Kegiatan uji coba Rencana Kelangsungan Kegiatan ini mencakup:
   a) Simulasi terutama untuk Petugas Pelaksana Pengelolaan Proses Kelangsungan Kegiatan;
   b) Uji coba pemulihan (*recovery*) sistem informasi untuk memastikan sistem informasi dapat berfungsi kembali;
   c) Uji coba proses pemulihan (*recovery*) di lokasi kerja sementara untuk menjalankan proses bisnis secara paralel;
   d) Uji coba terhadap perangkat dan layanan yang disediakan oleh pihak ketiga; dan
   e) Uji coba keseluruhan mulai dari organisasi, petugas, peralatan, perangkat, dan prosesnya.

k. Standar Pengendalian Kepatuhan

1) Kepatuhan terhadap peraturan perundang-undangan yang terkait keamanan informasi
   a) Seluruh pegawai dan pihak ketiga harus menaati peraturan perundangan yang terkait dengan keamanan informasi;
   b) Dinas dan Perangkat Daerah harus mengidentifikasi, mendokumentasikan, dan memelihara kemutakhiran semua peraturan perundangan yang terkait dengan sistem keamanan informasi;
   c) Hak Atas Kekayaan Intelektual
      Piranti lunak yang dikelola Dinas dan Perangkat Daerah harus mematuhi ketentuan penggunaan lisensi. Penggandaan piranti lunak secara tidak sah tidak diizinkan dan merupakan bentuk pelanggaran;
   d) Perlindungan terhadap rekaman
      Rekaman milik Pemerintah Daerah harus dilindungi dari kehilangan, kerusakan atau penyalahgunaan.
   e) Pengamanan data

Dinas dan Perangkat Daerah melindungi kepemilikan dan kerahasiaan data. Data hanya digunakan untuk kepentingan yang dibenarkan oleh peraturan perundang-undangan dan kesepakatan.

2) Kepatuhan Teknis

Dinas dan Perangkat Daerah harus melakukan pemeriksaan kepatuhan teknis secara berkala untuk menjamin efektivitas standar dan prosedur keamanan informasi yang ada di area operasional.

3) Audit Sistem Informasi

a) Pengendalian audit sistem informasi Dinas dan Perangkat Daerah bersama dengan Inspektorat Jenderal harus membuat perencanaan persyaratan, ruang lingkup, dan kegiatan audit yang melibatkan pemeriksaan sistem operasional untuk mengurangi kemungkinan risiko gangguan yang bisa terjadi terhadap kegiatan Pemerintah Daerah selama proses audit.

b) Perlindungan terhadap alat bantu (*tools*) audit sistem informasi Penggunaan alat bantu (baik piranti lunak maupun perangkat keras) untuk mengetahui kelemahan keamanan, memindai (*scanning*) kata sandi, atau untuk melemahkan dan menerobos sistem keamanan informasi tidak diizinkan kecuali atas persetujuan Pimpinan Dinas dan Perangkat Daerah.

c) Proses audit sistem informasi harus memperhatikan hal berikut:

1) Persyaratan audit harus disetujui oleh Pimpinan Perangkat Daerah;
2) Ruang lingkup pemeriksaan/audit harus disetujui dan dikendalikan oleh pihak berwenang;
3) Pemeriksaan piranti lunak dan data harus dibatasi untuk akses baca saja (*read-only*);
4) Selain akses baca saja hanya diizinkan untuk salinan dari dokumen (*file*) sistem yang diisolasi, yang harus dihapus bila audit telah selesai, atau diberikan perlindungan yang tepat jika ada kewajiban untuk

menyimpan dokumen (*file*) tersebut di bawah persyaratan dokumentasi audit;

5) Sumber daya untuk melakukan pemeriksaan harus secara jelas diidentifikasi dan tersedia;
6) Persyaratan untuk pengolahan khusus atau tambahan harus diidentifikasi dan disepakati;
7) Semua akses harus dipantau dan dicatat untuk menghasilkan jejak audit, dan untuk data dan sistem informasi sensitif harus mempertimbangkan pencatatan waktu (*timestamp*) pada jejak audit;
8) Semua prosedur, persyaratan, dan tanggung jawab harus didokumentasikan; dan
9) Auditor harus independen dari kegiatan yang diaudit.

4) Kepatuhan terhadap Hak Kekayaan Intelektual

Hal yang perIu diperhatikan dalam melindungi segala materi yang dapat dianggap kekayaan intelektual meliputi:

a) Mendapatkan piranti lunak hanya melalui sumber yang dikenal dan memiliki reputasi baik, untuk memastikan hak cipta tidak dilanggar;
b) Memelihara daftar aset informasi sesuai persyaratan untuk melindungi hak kekayaan intelektual;
c) Memelihara bukti kepemilikan lisensi, cakram utama (master disk), buku manual, dan lain sebagainya;
d) Menerapkan pengendalian untuk memastikan jumlah pengguna tidak melampaui lisensi yang dimiliki;
e) Melakukan pemeriksaan bahwa hanya piranti lunak dan produk berlisensi yang dipasang;
f) Patuh terhadap syarat dan kondisi untuk piranti lunak dan informasi yang didapat dari jaringan publik;
g) Dilarang melakukan duplikasi, konversi ke format lain atau mengambil dari rekaman komersial (*film* atau *audio*), selain yang diperbolehkan oleh Undang-Undang Hak Cipta; dan
h) Tidak menyalin secara penuh atau sebagian buku, artikel, laporan, atau dokumen lainnya, selain yang diizinkan oleh Undang-Undang Hak Cipta.

5) Kepatuhan terhadap Kebijakan dan Standar

Hal yang perlu dilakukan jika terdapat ketidakpatuhan teknis meliputi:

a) Menentukan dan mengevaluasi penyebab ketidakpatuhan;
b) Menentukan tindakan yang perlu dilakukan berdasarkan hasil evaluasi agar ketidakpatuhan tidak terulang kembali;
c) Menentukan dan melaksanakan tindakan perbaikan yang sesuai; dan
d) Mengkaji tindakan perbaikan yang dilakukan.

6) Kepatuhan Teknis

Sistem informasi harus diperiksa secara berkala untuk memastikan pengendalian perangkat keras dan piranti lunak telah diimplementasikan secara benar. Kepatuhan teknis juga mencakup pengujian penetrasi (*penetrating testing*) untuk mendeteksi kerentanan dalam sistem, dan memeriksa pengendalian akses untuk mencegah kerentanan tersebut telah diterapkan.

6. ISTILAH YANG DIGUNAKAN

1. Akun adalah identifikasi pengguna yang diberikan oleh unit Pengelola TIK, bersifat unik dan digunakan bersamaan dengan kata sandi ketika akan memasuki sistem TIK.
2. Akun khusus adalah akun yang diberikan oleh unit Pengelola TIK sesuai kebutuhan tetapi tidak terbatas pada pengelolaan TIK (baik berupa aplikasi atau sistem), dan kelompok kerja (baik berupa acara kedinasan, tim, atau unit kerja).
3. Aset fisik adalah jenis aset yang memiliki wujud fisik, misalnya perangkat komputer, perangkat jaringan dan komunikasi, media lepas pasang *(removable media)*, dan perangkat pendukung lainnya.
4. Aset tak berwujud adalah jenis aset yang tidak memiliki wujud fisik, misalnya pengetahuan, pengalaman, keahlian, citra, dan reputasi. Aset ini mempunyai umur lebih dari satu tahun (aset tidak lancar) dan dapat diamortisasi selama periode pemanfaatannya, yang biasanya tidak lebih dari empat puluh tahun.

5. *Conduit* adalah sebuah tabung atau saluran untuk melindungi kabel yang biasanya terbuat dari baja.
6. Data adalah catatan atas kumpulan fakta yang mempunyai arti baik secara kualitatif maupun kuantitatif.
7. *Denial of service* adalah suatu kondisi dimana sistem tidak dapat memberikan layanan secara normal, yang disebabkan oleh suatu proses yang tidak terkendali baik dari dalam maupun dari luar sistem.
8. Direktori adalah hirarki atau *tree structure*.
9. Informasi adalah hasil pemrosesan, manipulasi, dan pengorganisasian data yang dapat disajikan sebagai pengetahuan. Catatan: dalam penggunaannya, data dapat berupa informasi yang menjadi data baru, sebaliknya informasi dapat berfungsi sebagai data untuk menghasilkan informasi baru.
10. *Fallback* adalah suatu tindakan pembalikan/menarik diri dari posisi awal.
11. Fasilitas adalah sarana untuk melancarkan pelaksanaan fungsi atau mempermudah sesuatu.
12. Fasilitas utama adalah sarana utama gedung atau bangunan, seperti pusat control listrik, CCTV.
13. Hak akses khusus adalah akses terhadap sistem informasi sensitif, termasuk di dalamnya dan tidak terbatas pada sistem operasi, perangkat penyimpanan *(storage devices)*, dokumen pada *server (file server)*, dan aplikasi-aplikasi sensitif, hanya diberikan kepada pengguna yang membutuhkan dan pemakaiannya terbatas dan dikontrol.
14. *Hash totals* adalah nilai pemeriksa kesalahan yang diturunkan dari penambahan satu himpunan bilangan yang diambil dari data (tidak harus berupa data numerik) yang diproses atau dimanipulasi dengan cara tertentu.
15. Jejak audit *(audit trails)* adalah urutan kronologis catatan audit yang berkaitan dengan pelaksanaan suatu kegiatan.
16. Kata sandi adalah serangkaian kode yang dibuat pengguna, bersifat rahasia dan pribadi yang digunakan bersamaan dengan Akun Pengguna.

17. Keamanan informasi adalah perlindungan aset informasi dari berbagai bentuk ancaman untuk memastikan kelangsungan kegiatan, menjamin kerahasiaan, keutuhan, dan ketersediaan aset informasi.
18. Koneksi eksternal *(remote access)* adalah suatu akses jaringan komunikasi dari luar organisasi ke dalam organisasi.
19. *Kriptografi* adalah ilmu yang mempelajari cara menyamarkan informasi dan mengubah kembali bentuk tersamar tersebut ke informasi awal untuk meningkatkan keamanan informasi. Dalam *kriptografi* terdapat dua konsep utama yakni enkripsi dan dekripsi.
20. Kode berbahaya *(malicious code)* adalah semua macam program yang membahayakan termasuk makro atau *script* yang dapat diesekusi dan dibuat dengan tujuan untuk merusak sistem komputer.
21. Cakram utama *(master disk)* adalah media yang digunakan sebagai sumber dalam melakukan instalasi piranti lunak.
22. Perangkat bergerak *(mobile computing)* adalah penggunaan perangkat komputasi yang dapat dipindah *(portabel)* misalnya komputer jinjing *(notebook)* dan telepon selular untuk melakukan akses, pengolahan data dan penyimpanan.
23. Pemilik aset informasi adalah unit kerja yang memiliki kewenangan terhadap aset informasi.
24. Perangkat jaringan adalah peralatan jaringan komunikasi data seperti *modem, hub, switch, router*, dan lain-lain.
25. Piranti lunak adalah kumpulan beberapa perintah yang dieksekusi oleh mesin komputer dalam menjalankan pekerjaannya.
26. Perangkat pendukung adalah peralatan pendukung untuk menjamin beroperasinya perangkat keras dan perangkat jaringan serta untuk melindunginya dari kerusakan. Contoh perangkat pendukung adalah *Uninterruptible Power Supply (UPS)*, pembangkit tenaga listrik/generator, antena komunikasi.
27. Perangkat pengolah informasi adalah setiap sistem pengolah informasi, layanan atau infrastruktur. Contoh perangkat pengolah informasi adalah komputer, faksimili, telepon, mesin *fotocopy*.
28. Perjanjian *escrow* adalah perjanjian dengan pihak ketiga atau pembuat aplikasi untuk memastikan apabila pihak ketiga tersebut

tidak beroperasi/bangkrut (mengalami *failure*) maka Pemerintah Daerah berhak untuk mendapatkan kode program *(source code)*.

29. Perjanjian kerahasiaan adalah perikatan antara para pihak yang mencantumkan bahan rahasia, pengetahuan, atau informasi yang mana pihak-pihak ingin berbagi satu sama lain untuk tujuan tertentu, tetapi ingin membatasi akses dengan pihak lain.
30. Pihak berwenang adalah pihak yang mempunyai kewenangan terkait suatu hal, seperti kepolisian, instansi pemadam kebakaran, dan penyedia jasa telekomunikasi/internet.
31. Pihak ketiga adalah semua unsur di Iuar pengguna unit TIK Pemerintah Daerah yang bukan bagian dari Pemerintah Daerah, misal mitra kerja Pemerintah Daerah (seperti: konsultan, penyedia jasa komunikasi, pemasok dan pemelihara perangkat pengolah informasi), dan Pemerintah Daerah/lembaga lain.
32. Proses pendukung *(support processes)* adalah proses-proses penunjang yang mendukung suatu proses utama yang terkait. Contoh proses pendukung dalam pengembangan *(development)* adalah proses pengujian piranti lunak, proses perubahan piranti lunak.
33. Rencana *Kontijensi* adalah suatu rencana ke depan pada keadaan yang tidak menentu dengan skenario, tujuan, teknik, manajemen, pelaksanaan, serta sistem penanggulangannya telah Ditentukan secara bersama untuk mencegah dan mengatasi keadaan darurat.
34. *Rollback* adalah mengembalikan sebuah sistem mekanisme ke kondisi yang semula digunakan sebelum untuk perubahan diimplementasikan. Mekanisme ini biasanya terdapat pada sistem basis data.
35. *Routing* adalah sebuah mekanisme yang digunakan untuk mengarahkan dan menentukan rute/jalur yang akan dilewati paket dari satu perangkat ke perangkat yang berada di jaringan lain.
36. Sanitasi adalah proses penghilangan informasi yang disimpan secara permanen dengan menggunakan medan magnet besar atau perusakan fisik.
37. Manajemen Keamanan Informasi adalah sistem manajemen yang meliputi kebijakan, organisasi, perencanaan, penangung jawab,

proses, dan sumber daya yang mengacu pada pendekatan risiko bisnis untuk menetapkan, mengimplementasikan, mengoperasikan, memantau, mengevaluasi, mengelola, dan meningkatkan keamanan informasi.

38. Sanitasi *(sanitized)* adalah proses pembersihan data dan informasi sehingga tidak ada data dan informasi yang dapat diambil kembali dari perangkat keras tersebut.
39. Sistem informasi adalah serangkaian perangkat keras, piranti lunak, sumber daya manusia, serta prosedur dan/atau aturan yang diorganisasikan secara terpadu untuk mengolah data menjadi inforrnasi yang berguna untuk rnencapai suatu tujuan.
40. Sistem TIK adalah sistem operasi, sistem surat elektronik, sistem aplikasi, sistem basis data, sistem jaringan intranet/internet, dan sebagainya.
41. Administrator sistem *(system administrator)* adalah akun khusus untuk mengelola sistem informasi.
42. Perangkat jarak jauh *(teleworking)* adalah penggunaan teknologi telekomunikasi untuk memungkinkan pegawai bekerja di suatu lokasi yang berada di luar kantor untuk mengakses jaringan internal.

GUBERNUR BANTEN,

ttd

WAHIDIN HALIM

Salinan sesuai dengan aslinya
KEPALA BIRO HUKUM

ttd

AGUS MINTONO, SH.M.Si
Pembina Tk. I
NIP. 19680805 199803 1 010

LAMPIRAN II
PERATURAN GUBERNUR BANTEN
NOMOR 7 TAHUN 2018
TENTANG
TATA KELOLA SISTEM ELEKTRONIK DI LINGKUNGAN PEMERINTAH PROVINSI BANTEN

PUSAT DATA *(DATA CENTER)*

1. TUJUAN

   Standard ini bertujuan untuk mengatur penyelenggaraan pusat data *(data center)* di lingkungan Pemerintah Daerah.

2. RUANG LINGKUP

   Standard ini berlaku untuk penyelenggaraan pusat data *(data center)*, di lingkungan Pemerintah Daerah yang dilaksanakan secara internal dan/atau menggunakan pihak ketiga .

3. KEBIJAKAN

   a. Pemerintah Daerah menyediakan fasilitas berupa pusat data *(data center)* untuk pengelolaan *e-Government*;
   b. Penyelenggara pusat data *(data center)* Pemerintah Daerah dilakukan secara terpusat oleh Dinas;
   c. Dinas menyediakan layanan penempatan (*hosting*) *portal web* (*website*) dan aplikasi berbasis *web* kepada setiap Perangkat Daerah;
   d. Dinas menyediakan layanan pencadangan sistem (*system backup*) untuk aplikasi yang bersifat umum dan aplikasi khusus untuk Perangkat Daerah;
   e. Dinas menyediakan seluruh fasilitas, infrastruktur teknologi informasi (*server*, sistem operasi, penyimpanan (*storage*), cadangan (*backup*), perangkat jaringan) dan sistem keamanan pusat data (*data center*) untuk memfasilitasi layanan penempatan (*hosting*);

f. Pemilik aplikasi bertanggung jawab akan pengelolaan aplikasi, validitas data, dan pengelolaan hak aksesnya.

g. Dalam keadaan pemilik aplikasi kehilangan hak akses, Dinas dapat membuat hak akses baru berdasarkan surat resmi pemilik aplikasi;

h. Dinas berhak melakukan pengujian aplikasi yang akan ditempatkan (*hosting*) sesuai dengan standar keamanan informasi yang telah ditetapkan;

i. Seluruh peralatan, baik perangkat keras maupun piranti lunak termasuk di dalamnya data dan aplikasi, yang berada di dalam pusat data (*data center*) menjadi milik Pemerintah Daerah dan tidak boleh digunakan di luar Pemerintah Daerah tanpa izin dari Kepala Dinas teknis yang membidangi Komunikasi dan Informatika.

4. TANGGUNG JAWAB

a. Pihak-pihak yang terkait dalam penyelenggaraan pusat data (*data center*) terdiri atas:

1) Pemilik aplikasi adalah Pimpinan Perangkat Daerah atau Pejabat di Pemerintah Daerah yang membutuhkan aplikasi untuk mendukung tugas dan fungsinya;

2) Penyelenggara pusat data (*data center*) adalah Dinas dan/atau pihak ketiga yang melaksanakan pengembangan, pengelolaan, dan penyelenggaraan pusat data (*data center*);

3) Tim *quality assurance* (penjaminan mutu) penyelenggaraan pusat data (*data center*) adalah tim yang ditunjuk oleh pemilik aplikasi untuk melaksanakan kegiatan penjaminan mutu dalam penyelenggaraan pusat data (*data center*) di luar tim penyelenggara pusat data (*data center*);

4) Pengguna adalah pegawai Pemerintah Daerah.

b. Pemilik aplikasi mempunyai tanggung jawab terhadap:

1) Pemberian persetujuan:

a) Dokumen analisis dan spesifikasi kebutuhan *server* serta perubahannya;

b) Dokumen rancangan tingkat tinggi (*high level design*) dan rancangan rinci (*detail design*);

c) Dokumentasi penyelenggaraan aplikasi yang ditempatkan *(hosting)* di pusat data (*data center*).

2) Pemberian masukan kepada penyelenggara pusat data (*data center*) terkait penyelenggaraan aplikasi yang ditempatkan (*hosting*) di pusat data (*data center*);

3) Menjamin aplikasi yang akan ditempatkan (*hosting*) di pusat data (*data center*) telah bebas dari *bug* dan *error*;

4) Melakukan perbaikan aplikasi apabila ditemukan *bug* dan *error* pada aplikasi yang ditempatkan (*hosting*) di pusat data (*data center*).

c. Penyelenggara pusat data (*data center*) mempunyai tanggung jawab terhadap:

1) Penyelenggaraan pusat data (*data center*) sesuai Kebijakan dan Standar pusat data (*data center*) di Pemerintah Daerah;

2) Tindak lanjut masukan dari pemilik aplikasi yang ditempatkan (*hosting*) di pusat data (*data center*);

3) Penyusunan laporan status dan kemajuan pelaksanaan penyelenggaraan pusat data (*data center*) secara berkala kepada pemilik aplikasi.

d. Tim pengendali mutu (*quality assurance*) pengembangan aplikasi mempunyai tanggung jawab terhadap:

1) Pendampingan dan penjaminan mutu dalam penyelenggaraan pusat data (*data center*) secara berkala;

2) Penyusunan laporan pengendali mutu (*quality assurance*) secara berkala.

e. Pengguna mempunyai tanggung jawab terhadap pemberian masukan kepada pemilik aplikasi terkait penyelenggaraan pusat data (*data center*).

5. STANDAR

a. Pedoman penyelenggaraan pusat data (*data center*) terdiri atas:

1) Persyaratan disain teknis dan implementasi;

2) Persyaratan operasi;

3) Persyaratan keberlangsungan kegiatan.

b. Persyaratan disain teknis dan implementasi pusat data (*data center*) paling sedikit harus memenuhi aspek-aspek sebagai berikut:

1) Lokasi

a) Bangunan harus berada pada lokasi yang aman berdasar kajian indeks rawan bencana Indonesia;
b) Bangunan harus mempunyai akses jalan yang cukup dan fasilitas parkir;
c) Lokasi sebaiknya berada di kawasan yang memiliki temperatur sekitar yang rendah dan menghindari kawasan yang memiliki kelembaban tinggi.

2) Persyaratan Bangunan dan Arsitektur
a) Ruang komputer tidak berada di bawah area perpipaan (*plumbing*) seperti kamar mandi, toilet, dapur, laboratorium dan ruang mekanik kecuali jika sistem pengendalian air disiapkan;
b) Tiap jendela ruang komputer yang menghadap ke sinar matahari harus ditutup untuk mencegah paparan panas;
c) Bangunan harus memiliki area bongkar muat yang memadai untuk menangani penghantaran barang/peralatan.

3) Persyaratan Kontrol Akses dan Keamanan
a) Setiap jendela yang memungkinkan akses langsung ke pusat data (*data center*), diberi pengaman fisik;
b) Pusat data (*data center*) harus diamankan selama 24 jam dengan paling sedikit satu orang petugas per siklus kerja (*shift*);
c) Perangkat sistem pemantau visual (seperti CCTV) harus dipasang untuk memantau dan merekam setiap aktivitas pada ruang *Server*, ruang mekanik dan kelistrikan, ruang telekomunikasi dan kawasan kantor;
d) Akses ke dalam ruang *Server* menggunakan perangkat yang dikendalikan dengan mekanisme otentikasi (seperti pin, kartu gesek, kartu nirkontak atau akses biometrik). Tamu/pengunjung harus dilengkapi dengan tanda masuk dan tanda pengenal untuk dapat masuk ke ruang *Server*, ruang mekanikal dan kelistrikan, ruang telekomunikasi dan kawasan kantor. Setiap orang yang masuk ke dalam ruangan sebagaimana

dimaksud di atas harus memiliki izin dan didampingi oleh pemilik aplikasi dan Dinas teknis yang membidangi Komunikasi dan Informatika.

4) Peringatan Kebakaran, Deteksi Asap, dan Pemadam Kebakaran (*Fire Precautions, Smoke Detection and Fire Suppression*)
   a) Jumlah dan lokasi pintu darurat kebakaran sesuai dengan peraturan perundang-undangan;
   b) Pintu darurat kebakaran dapat dibuka ke arah luar;
   c) Lampu darurat dan tanda keluar diletakkan pada lokasi sesuai dengan peraturan perundang-undangan;
   d) Titik panggil manual harus dipasang sesuai dengan peraturan perundang-undangan;
   e) Dinding dan pintu ke ruang komputer, ruang mekanikal dan kelistrikan, ruang telekomunikasi dan kawasan kritikal lainnya memiliki tingkat terbakar (*fire-rating*) sesuai dengan peraturan perundang-undangan;
   f) Ruang komputer harus diproteksi dengan sistem deteksi asap. Seluruh sistem deteksi asap bangunan harus diintegrasikan ke satu alarm bersama;
   g) Catatan pemeliharaan yang mencakup seluruh aspek yang berkaitan dengan deteksi api dan pemadaman harus tersedia untuk keperluan pemeriksaan;
   h) Bukti pelatihan staf pada simulasi pengendalian kebakaran harus tersedia;
   i) Ruang pusat data (*data center*) harus dilindungi dengan sistem pemadam kebakaran. Sistem pemadam kebakaran otomatis harus dapat diaktifkan secara manual;
   j) Alat pemadam kebakaran harus ditempatkan sesuai ketentuan peraturan perundang-undangan;
   k) Semua tanda peringatan kebakaran harus ditempatkan pada posisinya sesuai ketentuan peraturan perundang-undangan;
   l) Seluruh sistem pendeteksi dan pemadam kebakaran harus didesain dan dipasang oleh petugas yang

memiliki kualifikasi dan didesain sesuai standar internasional/nasional atau regulasi nasional;

m) Jika ruang *server*, ruang telekomunikasi, dan ruang mekanikal dan kelistrikan memiliki sistem pemadam api otomatis (*sprinkler*), maka sistem tersebut harus tipe *pre-action*;

n) Jika ruang atau bangunan yang berdekatan dengan lokasi pusat data (*data center*) tidak memiliki sistem pemadam api otomatis (*sprinkler*), maka risiko kebakaran harus dikaji.

5) Penyediaan Catu Daya

a) Kabel daya masuk ke dalam bangunan pusat data (*data center*) dan diterminasi di ruang kendali penyambungan listrik yang handal yang berisikan seluruh penyambungan dan pengukuran yang penting;

b) Daya listrik utama paling sedikit 20% lebih besar dari proyeksi beban puncak dimana pusat data (*data center*) berada;

c) Tersedianya catu daya listrik alternatif (seperti generator *standby*) dengan kapasitas yang memadai untuk operasional paling sedikit 3 jam selama kejadian gangguan listrik utama;

d) Perangkat TIK harus diproteksi dengan *Uninterruptible Power Supply* (UPS) atau catu daya cadangan lainnya;

e) Kapasitas penyimpanan energi UPS atau catu daya cadangan lainnya harus memadai untuk memasok beban TIK sehingga cukup waktu bagi catu daya alternatif mencapai keadaan tunak (*steady state*) untuk memikul beban perangkat TIK;

f) Kapasitas UPS harus lebih besar dari proyeksi beban puncak perangkat TIK. Kapasitas beban rata-rata tidak lebih besar dari 80% kapasitas UPS;

g) UPS memiliki sistem pelaporan dan pemantauan kinerja serta sistem peringatan;

h) UPS yang digunakan telah memiliki jaminan dari pabrikan untuk dapat berfungsi sesuai spesifikasinya;

i) Bangunan harus dilengkapi dengan sistem proteksi petir;

j) Kabel komunikasi tembaga dari luar gedung diproteksi dengan peredam tegangan lebih (*surge suppressor*) sebelum ke ruang pusat data (*data center*);

k) ruang pusat data (*data center*) memiliki terminal pembumian (*grounding*) tembaga yang menjadi titik acuan pembumian ruangan tersebut.

6) Penyediaan Sistem Pendingin dan Ventilasi

a) Ruang pusat data *(data center)* dijaga dan dikendalikan temperatur dan kelembaban ruangnya sesuai dengan kebutuhan operasional normal perangkat TIK yang paling peka;

b) Peralatan pengkondisian udara harus dihubungkan ke catu daya utama dan (didukung oleh catu daya alternatif). Jika ruang komputer menggunakan sistem ventilasi detektor asap harus terpasang pada saluran udara masuk, dan harus dapat menghentikan udara masuk jika asap terdeteksi.

7) Penyediaan Sistem Pengkabelan dan Manajemen Kabel

a) Sistem pengkabelan yang digunakan untuk konektivitas ke setiap rak sesuai dengan standar nasional/internasional;

b) Seluruh pengkabelan interior dengan tipe tidak mudah terbakar (*low flammability*);

c) Setiap rak memiliki akses ke sistem saluran kabel, di atas atau di bawahnya, yang memungkinkan kabel-kabel dapat ditata secara baik antar rak;

d) Kabel daya satu fase dan kabel data tembaga harus dipisahkan paling sedikit 20 cm;

e) Kabel daya tiga fase dan kabel data tembaga harus dipisahkan paling sedikit 60 cm;

f) Kabel yang melewati dinding dilindungi terhadap bahaya api sesuai ketentuan peraturan perundang-undangan.

g) Kabel tidak boleh diletakkan di pintu, lantai, atau digantung antar rak;

h) Setiap kabel memiliki label identifikasi yang unik pada kedua ujung awal dan akhir, jika perlu terdapat data pemilik;

i) Setiap rak peralatan memiliki label identifikasi, jika perlu terdapat data pemilik;

j) Kabel input telekomunikasi eksternal dihubungkan di area atau ruang telekomunikasi tersendiri;

k) Jika area telekomunikasi terpisah dari pusat data (*data center*) maka harus memiliki sistem pengkondisi udara, proteksi kebakaran, kelistrikan yang sama dengan standar ruang pusat data (*data center*);

l) Seluruh item perangkat logam berisi kabel harus dibumikan *(grounded)*.

8) Sistem Manajemen Bangunan dan Pemantauan

a) Ruang pusat data (*data center*) memiliki paling sedikit satu sensor temperatur ruang dan satu sensor kelembaban ruang;

b) Ruang telekomunikasi dan ruang mekanikal dan kelistrikan memiliki sebuah sensor temperatur dan sensor kelembaban ruang.

c. Persyaratan operasi pusat data *(data center)* paling sedikit harus memenuhi aspek sebagai berikut:

1) Tata Kerja dalam Bangunan

a) Pusat data (*data center*) memiliki satu area bongkar muat barang;

b) Seluruh peralatan dibongkar atau dikemas dan dirakit di area tertentu dan tidak dilakukan di dalam ruang komputer;

c) Ruang kendali disediakan untuk melakukan fungsi pemantauan dan pengendalian.

2) Dokumentasi Manajemen Operasi

a) Manual operasi umum diperlukan dan harus mencakup seluruh persyaratan operasi pusat data (*data center*);

b) Seluruh perangkat utama seperti pengkondisi udara, UPS, generator, dan lain sebagainya harus terdapat dalam pencatatan aset:
   1) Lokasi;
   2) Nomor seri;
   3) Data pengadaan;
   4) Kontak rinci pabrikan;
   5) Tanggal kalibrasi jika diperlukan.
c) Seluruh konfigurasi dan prosedur operasi harus didokumentasikan termasuk di dalamnya:
   1) Perubahan konfigurasi;
   2) *Set-point default*.
d) Informasi dokumentasi lokasi meliputi:
   1) Bangunan dan lantai;
   2) Lokasi rak dan item utama dari perangkat;
   3) Denah rak;
   4) Interkonektivitas fisik dan logik dari peralatan.
e) Daftar kontak harus tersedia dan mencatat seluruh staf pusat data (*data center*), tugas dan tanggung jawab staf pusat data (*data center*), pemasok, perusahaan pemelihara pusat data (data center), dan layanan darurat;
f) Pusat data (*data center*) memiliki panduan keamanan operasi yang merinci hal-hal seperti:
   1) Prosedur pencegahan kebakaran;
   2) Penggunaan listrik secara aman;
   3) Penggunaan perangkat transmisi data optik;
   4) Pengangkatan beban berat.
g) Prosedur tertulis harus tersedia dan mudah diakses untuk menjelaskan secara rinci status peringatan dan bagaimana gangguan sistem ditangani oleh staf pusat data (*data center*).

3) Prosedur Pemeliharaan
   a) Setiap staf pusat data (*data center*) dan/atau kontraktor yang bertugas dalam pemeliharaan harus dapat menunjukkan kompetensinya;

b) Setiap peralatan yang membutuhkan pemeliharaan harus memiliki catatan pemeliharaan yang merinci peralatan, tanggal pemeliharaan, hasil dan kontak rinci.

d. Persyaratan keberlangsungan kegiatan pusat data (*data center*) paling sedikit harus memenuhi aspek sebagai berikut:

1) Manajemen Risiko

a) Pusat data (*data center*) harus memiliki kajian analisa risiko yang meliputi risiko yang mungkin terjadi, dampak, dan strategi mengurangi risiko, antara lain:
   1) Lokasi: kebakaran, banjir;
   2) Pegawai: penyakit epidemic;
   3) Komunikasi: kerusakan kabel utama.

b) Seluruh perangkat kritis seperti status UPS, kondisi gangguan, dan lain-lain harus dipantau.

2) Penanganan Insiden

a) Setiap gangguan kritis dan berhentinya layanan harus dapat disampaikan kepada pengguna pusat data *(data center)* secepatnya;

b) Setiap gangguan dan berhentinya layanan dapat disampaikan kepada Dinas teknis yang membidangi Komunikasi dan Informatika oleh pengguna pusat data (*data center*);

c) Pihak manajemen harus menelaah setiap insiden sebagai berikut:
   1) Insiden yang terjadi;
   2) Dimana terjadi;
   3) Kapan terjadi;
   4) Dampak terhadap penyediaan layanan;
   5) Bagaimana mengatasinya;
   6) Perubahan apa yang perlu dilakukan untuk menghindari terjadinya insiden serupa.

d) Memiliki peringatan tertulis yang merinci apa saja dampak kehilangan daya mendadak dan menyeluruh pada perangkat TIK serta petunjuk tertulis bagaimana proses *restart* ditangani;

e) Efek dari terputusnya aliran daya harus disimulasi secara regular untuk membuktikan UPS dan menghidupkan (*startup*) generator dapat beroperasi dengan baik;

f) Pada setiap siklus kerja (*shift*) harus diidentifikasi oleh petugas yang bertanggung jawab untuk memberikan tanggapan terhadap setiap insiden/bencana.

3) Pusat Pemulihan Bencana (*Disaster Recovery Center*)
   a) Penyelenggara pusat data (*data center*) harus memiliki fasilitas sistem cadangan (*backup system*);
   b) Penempatan fasilitas Pusat Pemulihan Bencana harus mempertimbangkan:
      1) jarak terhadap lokasi Pusat Data (*data center*) yang meminimalkan risiko;
      2) biaya yang layak; dan
      3) Memenuhi *Service Level Agreement (SLA)* yang disyaratkan.

6. ISTILAH YANG DIGUNAKAN
   a. Pusat data *(data center)* adalah suatu fasilitas yang digunakan untuk menempatkan sistem elektronik dan komponen terkaitnya untuk keperluan penempatan, penyimpanan, dan pengolahan data.
   b. Pusat pemulihan bencana *(disaster recovery center)* adalah fasilitas sistem cadangan *(backup system)* pusat data *(data center)* yang terdiri dari perangkat keras dan piranti lunak untuk mendukung kegiatan operasional Pemerintah Daerah secara berkesinambungan ketika pusat data *(data center)* mati/rusak karena bencana.

GUBERNUR BANTEN,

ttd

WAHIDIN HALIM

Salinan sesuai dengan aslinya
KEPALA BIRO HUKUM

ttd

AGUS MINTONO, SH.M.Si
Pembina Tk. I
NIP. 19680805 199803 1 010

LAMPIRAN III
PERATURAN GUBERNUR BANTEN
NOMOR 7 TAHUN 2018
TENTANG
TATA KELOLA SISTEM ELEKTRONIK DI LINGKUNGAN PEMERINTAH PROVINSI BANTEN

NAMA DOMAIN DAN SUBDOMAIN

1. TUJUAN

Standar ini menjadi pedoman bagi penyelenggara *portal web (website)* dan/atau aplikasi berbasis *web* di Pemerintah Daerah. Kebijakan ini sesuai dengan ketentuan Kementerian Komunikasi dan Informatika.

2. RUANG LINGKUP

Ruang lingkup dari penataan domain dan subdomain meliputi *website* Perangkat Daerah dan Unit Kerja, aplikasi berbasis web, dan kegiatan Pemerintah Daerah yang dituangkan dalam tampilan (*website*).

Setiap pengajuan nama subdomain harus disampaikan kepada Dinas teknis yang membidangi Komunikasi dan Informatika disertai dengan data penanggung jawab *website*, aplikasi berbasis *web* serta pemilik kegiatan.

3. KEBIJAKAN

a. Setiap Pimpinan Perangkat Daerah bertanggung jawab dalam memantau dan mengawasi penggunaan subdomain di lingkungan Perangkat Daerah masing-masing.
b. Setiap Pimpinan Perangkat Daerah bertanggung jawab dan mengetahui terhadap penambahan dan perubahan nama subdomain di lingkungan Perangkat Daerah masing-masing, dalam hal ini meliputi penambahan, perubahan, dan penghapusan subdomain.
c. Domain dan subdomain yang sudah dibuat menjadi milik Pemerintah Daerah dan tidak boleh digunakan di luar Pemerintah Daerah tanpa izin dari pejabat yang berwenang.

4. SISTEM PENAMAAN DOMAIN *(DOMAIN NAME SERVER (DNS))*

a. Pengertian DNS:

1) DNS adalah sistem basis data terdistribusi (*distribute database system*) yang digunakan untuk pencarian nama komputer di jaringan yang menggunakan TCP/IP (*Transmission Control Protocol/ Internet Protocol*);
2) DNS merupakan sebuah *aplikasi service* yang bisa digunakan di internet seperti peramban *web browser* atau surat elektronik yang menerjemahkan sebuah nama domain ke alamat *IP* (*IP address*). Contoh : yahoo.com 68.142.197.64.

b. Struktur DNS

DNS merupakan sebuah hierarki pengelompokan domain berdasarkan nama yang terbagi menjadi beberapa bagian, yakni:

1) Domain Tingkat Pertama (*Root Domain*)
   a) Domain Level Global (*Generic/ Global Top Level Domain* (gTLD))
      Contoh: .com, .net, .org, .ac, .web, .go;
   b) Domain Level Negara (*Country Code Top Level Domain* (ccTLD))
      Contoh: .sg, .au, .id;
2) Domain Tingkat Kedua (*Second Level Domain*)
   Contoh: *banten.go.id*;
3) Domain Tingkat Ketiga (*Third Level Domain* (subdomain))
   Contoh: *diskominfo.banten.go.id*.

5. SISTEM PENAMAAN DOMAIN *(DOMAIN NAME SERVER (DNS))*

a. Pengelolaan Penamaan Domain meliputi:
   1) Pendaftaran;
   2) Penggunaan;
   3) Penonaktifan;
   4) Perpanjangan;
   5) Penunjukan pejabat;
   6) Perubahan nama domain;
   7) *Server* nama domain.

b. Nama domain yang dimaksud di atas dibiayai oleh Anggaran Pemerintah Daerah.

c. Seluruh situs *web* (*website*) Perangkat Daerah dan Unit Kerja serta aplikasi berbasis *web* pada Pemerintah Daerah harus menjadi subdomain dari nama domain Pemerintah Daerah.

6. SUBDOMAIN DI PEMERINTAH PROVINSI BANTEN

a. Yang berhak mendapatkan nama subdomain:
   1) Perangkat Daerah dan Unit Kerja di Pemerintah Daerah;
   2) Pelayanan publik di Pemerintah Daerah;
   3) Kegiatan Pemerintah Daerah;
   4) Aplikasi berbasis *web*.

b. Permohonan mendapatkan nama subdomain. Mengajukan permohonan melalui Dinas dengan mencantumkan dan melampirkan:
   1) Surat permohonan nama subdomain layanan publik/domain khusus;
   2) Peraturan perundang-undangan yang menjadi penyelenggaraan pelayanan publik/penyelenggaraan dasar kegiatan Pemerintah Daerah;
   3) Surat keterangan mengenai pelayanan publik/kegiatan berskala nasional atau internasional;
   4) Penunjukan pejabat nama subdomain:
      a) Surat penunjukan pejabat nama subdomain;
      b) Kartu PNS atau kartu identitas pegawai tetap.

c. Nama subdomain yang diajukan harus terdiri dari karakter yang dapat berupa nama, singkatan nama atau akronim dari nama resmi instansi, nomenklatur pelayanan publik, nama kegiatan Pemerintah Daerah, dan aplikasi berbasis *web*.

d. Penataan subdomain untuk Perangkat Daerah dan Unit Kerja di bawahnya:
   1) Perangkat Daerah : *eselonII.banten.go.id*;
   2) Unit Kerja : *eselonII.banten.go.id/eselonIII*;
   3) Unit Eselon IV : e*selonII.banten.go.id/eselonIII/produk*.

e. Penataan subdomain untuk kegiatan Pemerintah Daerah:
   1) Kegiatan Skala Nasional/Internasional: *kegiatan.banten.go.id*;
   2) Kegiatan Internal Pemerintah Daerah Tingkat Perangkat Daerah:

eselonII.banten.go.id/kegiatan;

3) Kegiatan Internal Pemerintah Daerah Tingkat Unit Kerja: *eselonII.banten.go.id/eselonIII/kegiatan*;

f. Penataan subdomain untuk aplikasi berbasis *web:*

1) Digunakan oleh publik: *aplikasi.banten.go.id*;

2) Digunakan di lingkungan Pemerintah Daerah: *aplikasi.banten.go.id/kegiatan*;

3) Digunakan di lingkungan Perangkat Daerah/Unit Kerja/khusus: *aplikasi.eselonII.banten.go.id*.

g. Nama subdomain Perangkat Daerah di Pemerintah Daerah:

1.	Biro Administrasi Rumah Tangga Pimpinan	biroaprt.banten.go.id
2.	Biro Infrastruktur dan Sumber Daya Alam	biroisd.banten.go.id
3.	Biro Administrasi Pembangunan Daerah	biroadpem.banten.go.id
4.	Biro Perekonomian	biroekonomi.banten.go.id
5.	Biro Pemerintahan	biropemerintahan.banten.go.id
6.	Biro Hukum	birohukum.banten.go.id
7.	Biro Organisasi	biroorganisasi.banten.go.id
8.	Biro Kesejahteraan Rakyat	birokesra.banten.go.id
9.	Biro Umum	biroumum.banten.go.id
10.	DPRD Provinsi Banten	http://dprd-banten.go.id/
11.	Dinas Perpustakaan dan Kearsipan	dpk.banten.go.id
12.	Dinas Pemberdayaan Perempuan, Perlindungan Anak, Kependudukan dan Keluarga Berencana	dp3akkb.banten.go.id

13.	Dinas Lingkungan Hidup dan Kehutanan	dlhk.banten.go.id
14.	Dinas Ketahanan Pangan	disketapang.banten.go.id
15.	Dinas Perumahan Rakyat dan Kawasan Permukiman	perkim.banten.go.id
16.	Dinas Pekerjaan Umum dan Penataan Ruang	dpupr.banten.go.id
17.	Dinas Kesehatan	dinkes.banten.go.id
18.	Dinas Pendidikan dan Kebudayaan	dindikbud.banten.go.id
19.	Dinas Kepemudaan dan Olah Raga	dispora.banten.go.id
20.	Dinas Pertanian	dispertan.banten.go.id
21.	Dinas Kelautan dan Perikanan	dkp.banten.go.id
22.	Dinas Penanaman Modal dan Pelayanan Terpadu Satu Pintu	dpmptsp.banten.go.id
23.	Dinas Komunikasi, Informatika, Statistik dan Persandian	diskominfo.banten.go.id
24.	Dinas Pemberdayaan Masyarakat dan Desa	dpmd.banten.go.id
25.	Dinas Perhubungan	dishub.banten.go.id
26.	Dinas Energi dan Sumberdaya Mineral	desdm.banten.go.id
27.	Dinas Perindustrian dan Perdagangan	http://disperindag.banten.go.id /
28.	Dinas Pariwisata	dispar.banten.go.id
29.	Dinas Sosial	dinsos.banten.go.id
30.	Dinas Tenaga Kerja dan Transmigrasi	disnakertrans.banten.go.id
31.	Dinas Koperasi, Usaha Kecil dan Menengah	dinkopukm.banten.go.id
32.	Inspektorat	inspektorat.banten.go.id
33.	Badan Pengelolaan Keuangan dan Aset Daerah	bpkad.banten.go.id
34.	Badan Kepegawaian Daerah	bkd.banten.go.id
35.	Badan Pengembangan Sumber Daya Manusia	bpsdmd.banten.go.id

36.	Badan Kesatuan Bangsa dan Politik	kesbangpol.banten.go.id
37.	Badan Pendapatan Daerah	bapenda.banten.go.id
38.	Badan Perencanaan Pembangunan Daerah	bappeda.banten.go.id
39.	Badan Penanggulangan Bencana Daerah	bpbd.banten.go.id
40.	Badan Penghubung	penghubung.banten.go.id
41.	Satuan Polisi Pamong Praja (SATPOLPP) Provinsi Banten	satpolpp.banten.go.id

h. Ketentuan lain yang harus diikuti bagi seluruh Perangkat Daerah di Pemerintah Daerah

1) Seluruh basis data (*data base*) dan *website*/aplikasi berbasis *web* harus disimpan pada *server* yang berada di pusat data (*data center*) Pemerintah Daerah;
2) Perangkat Daerah wajib melakukan pembinaan dan pengawasan terhadap unit kerja di bawahnya;
3) Jika terjadi gangguan jaringan komunikasi dan keamanan menjadi tanggung jawab Dinas untuk melakukan perbaikan;
4) Jika terjadi gangguan terkait data dan informasi menjadi tanggung jawab Perangkat Daerah pemilik data dan informasi tersebut dan akan dibantu oleh Dinas dalam melakukan perbaikan.

GUBERNUR BANTEN,

ttd

WAHIDIN HALIM

Salinan sesuai dengan aslinya
KEPALA BIRO HUKUM

ttd

AGUS MINTONO, SH.M.Si
Pembina Tk. I
NIP. 19680805 199803 1 010

LAMPIRAN IV
PERATURAN GUBERNUR BANTEN
NOMOR 7 TAHUN 2018
TENTANG
TATA KELOLA SISTEM ELEKTRONIK DI LINGKUNGAN PEMERINTAH PROVINSI BANTEN

STANDAR PENGEMBANGAN APLIKASI

1. TUJUAN

Standar ini digunakan sebagai pedoman dalam pengembangan aplikasi di Pemerintah Daerah agar pelaksanaan pengembangan aplikasi efektif dan efisien.

2. RUANG LINGKUP

Standar ini berlaku untuk pengembangan aplikasi di Pemerintah Daerah yang dilaksanakan secara internal dan/atau menggunakan pihak ketiga, yang mencakup komponen sistem aplikasi, basis data, dan jaringan.

3. KEBIJAKAN

a. Aplikasi harus dikembangkan oleh pemilik proses bisnis sesuai dengan tugas dan fungsinya;
b. Pemilik proses bisnis bertanggung jawab atas aplikasi yang dikembangkan;
c. Penyelenggara pengembangan aplikasi adalah pihak yang ditunjuk oleh pemilik proses bisnis untuk mengembangkan aplikasi mulai dari perencanaan hingga implementasinya;
d. Setiap Pimpinan Perangkat Daerah bertanggung jawab dalam penerapan Kebijakan dan Standar Pengembangan Aplikasi di Perangkat Daerah masing-masing;
e. Perangkat Daerah harus menerapkan Kebijakan dan Standar Pengembangan Aplikasi di Perangkat Daerah masing-masing;
f. Setiap Pimpinan Perangkat Daerah bertanggung jawab dalam membangun kompetensi pengembangan aplikasi bagi

pejabat/staf di Perangkat Daerah masing-masing untuk mendukung kelancaran pengembangan aplikasi;

g. Setiap kegiatan pengembangan aplikasi harus dibentuk tim pengembangan aplikasi yang sekurang-kurangnya terdiri atas: manajer proyek, sistem analis, pemilik proses bisnis, penguji aplikasi, dan pemrogram (*programmer*);

h. Perangkat Daerah harus berkoordinasi dengan Dinas selama proses pengembangan aplikasi sampai dengan operasionalisasi aplikasi;

i. Dinas sebagai pengatur, pembina dan pengawas TIK di Pemerintah Daerah memiliki kewenangan untuk memastikan bahwa proses pengembangan telah sesuai dengan kebijakan dan standar pengembangan aplikasi;

j. Aplikasi yang telah dikembangkan untuk kepentingan Pemerintah Daerah dan Perangkat Daerah harus ditempatkan di pusat data *(data center)* Pemerintah Daerah yang dikelola oleh Dinas teknis yang membidangi Komunikasi dan Informatika;

k. Aplikasi yang sudah dikembangkan menjadi milik Pemerintah Daerah dan tidak boleh digunakan di luar Pemerintah Daerah tanpa izin dari pejabat yang berwenang.

4. TANGGUNG JAWAB

a. Pihak-pihak yang terkait dalam pengembangan aplikasi terdiri atas:

1) Pemilik proses bisnis adalah Pimpinan Perangkat Daerah atau Pejabat di Pemerintah Daerah yang memiliki kebutuhan akan adanya aplikasi untuk mendukung berjalannya tugas dan fungsi;

2) Pengembang aplikasi adalah pegawai pada Perangkat Daerah di Pemerintah Daerah dan/atau Pihak Ketiga yang melaksanakan pengembangan aplikasi;

3) Tim pengendalian mutu (*quality assurance*) adalah tim yang ditunjuk oleh pemilik proses bisnis untuk melaksanakan kegiatan pengendalian mutu dalam pengembangan aplikasi di luar tim pengembang aplikasi;

4) Pengguna aplikasi;

5) Dinas.

b. Pemilik proses bisnis mempunyai tanggung jawab terhadap:

1) Pemberian persetujuan:
   a) Dokumen analisis dan spesifikasi kebutuhan aplikasi serta perubahannya;
   b) Dokumen rancangan tingkat tinggi (*high level design*) dan rancangan rinci (*detail design*);
   c) Dokumentasi pengembangan aplikasi; dan
   d) Dokumen rencana dan skenario pengujian.
2) Pelaksanaan *User Acceptance Test* (UAT);
3) Memastikan bahwa aplikasi yang akan ditempatkan (*hosting*) di pusat data (*data center*) sudah bebas *bug* dan *error*;
4) Pemeriksaan dan penandatanganan berita acara analisis hasil pengujian dan juga berita acara hasil tinjauan pasca implementasi aplikasi; dan
5) Memberi masukan kepada pengembang aplikasi terkait pengembangan dan penyempurnaan aplikasi.
6) Melakukan evaluasi pasca implementasi dan melaporkan hasilnya ke Dinas.

c. Pengembang aplikasi mempunyai tanggung jawab terhadap:

1) Pelaksanaan siklus pengembangan aplikasi sesuai kebijakan dan standar siklus pengembangan aplikasi di Pemerintah Daerah;
2) Tindak lanjut masukan dari pemilik proses bisnis terkait pengembangan dan penyempumaan aplikasi;
3) Pemeriksaan dan penandatanganan berita acara analisis hasil pengujian dan juga berita acara hasil tinjauan pasca implementasi aplikasi;
4) Penyusunan laporan status dan kemajuan pelaksanaan pengembangan aplikasi secara berkala serta pelaporan kepada pemilik proses bisnis;
5) Penyusunan laporan terkait perubahan pengembangan aplikasi berdasarkan hasil UAT serta pelaporan kepada pemilik proses bisnis; dan

6) Penyusunan dokumentasi yang merupakan keluaran pada semua tahapan pengembangan aplikasi

d. Tim pengendalian mutu (*quality assurance*) mempunyai tanggung jawab terhadap:
   1) Pendampingan dan pengendalian mutu dalam pengembangan aplikasi;
   2) Penyusunan laporan pengendalian mutu (*quality assurance*) dalam setiap tahapan pengembangan aplikasi;
   3) Pelaksanaan *User Acceptance Test* (UAT).

e. Pengguna dapat memberi masukkan kepada pemilik proses bisnis terkait pengembangan dan penyempurnaan aplikasi

f. Dinas mempunyai tanggung jawab terhadap:
   1) Pendampingan dalam pelaksanaan pengendalian mutu dalam pengembangan aplikasi;
   2) Persetujuan dalam penyusunan laporan pengendalian mutu (*quality assurance*) dalam setiap tahapan pengembangan aplikasi;
   3) Pengaturan, pembinaan, dan pengawasan pelaksanaan pengembangan aplikasi di Pemerintah Daerah;
   4) Memastikan bahwa pengembangan aplikasi baik proses maupun produk yang dihasilkan sesuai dengan standar aplikasi yang berlaku di Pemerintah Daerah yang ditetapkan oleh Dinas;
   5) Terlibat dalam proses pengujian aplikasi;
   6) Memastikan tidak terjadi redundansi pengembangan aplikasi untuk produk aplikasi sejenis;
   7) Melakukan monitoring dan evaluasi proses pengembangan aplikasi dan melaporkan kepada Gubernur setiap akhir tahun anggaran.

5. STANDAR

a. Siklus pengembangan aplikasi terdiri atas:
   1) Proses analisis kebutuhan aplikasi, merupakan proses untuk mengumpulkan dan menganalisis spesifikasi kebutuhan bisnis dan aplikasi secara rinci;

2) Proses perancangan aplikasi, merupakan proses penyusunan rancangan aplikasi berdasarkan analisis kebutuhan aplikasi dan hasilnya akan digunakan sebagai acuan dalam proses pengembangan aplikasi;
3) Proses pengkodean (*coding*) aplikasi, merupakan proses yang dilaksanakan untuk membangun aplikasi sesuai dengan kebutuhan berdasarkan rancangan aplikasi;
4) Proses pengujian aplikasi, merupakan proses yang dilaksanakan untuk menguji aplikasi yang telah dikembangkan;
5) Proses implementasi aplikasi, merupakan proses penerapan aplikasi yang telah dikembangkan pada lingkungan operasional; dan
6) Proses tinjauan pasca implementasi aplikasi, merupakan proses evaluasi yang dilaksanakan sebagai bahan pembelajaran untuk pengembangan aplikasi selanjutnya.

b. Proses analisis kebutuhan aplikasi
1) Proses analisis kebutuhan aplikasi meliputi kegiatan
a) Pengumpulan, analisis, penyusunan, dan pendokumentasian spesifikasi kebutuhan bisnis dan aplikasi yang mencakup:
1) Kebutuhan aplikasi termasuk fungsi kemampuan yang diinginkan, target kinerja, tingkat keamanan, dan kebutuhan spesifik lainnya;
2) Identifikasi dan analisis risiko teknologi serta rencana mitigasi;
3) Deskripsi aplikasi yang sudah ada (jika ada), dan analisis kesenjangannya (*gap analysis*) dari target aplikasi yang diinginkan;
4) Target waktu pengembangan aplikasi;
5) Konsep dasar operasional aplikasi;
6) Rencana kapasitas (*capacity planning*);
7) Infrastruktur pendukung.
b) Pendokumentasian perubahan analisis dan spesifikasi kebutuhan aplikasi yang terjadi dalam proses ini.
2) Proses analisis kebutuhan aplikasi menghasilkan keluaran:

a) Dokumen analisis dan spesifikasi kebutuhan aplikasi; dan
b) Dokumen perubahan analisis dan perubahan spesifikasi kebutuhan aplikasi.

c. Proses Perancangan Aplikasi

1) Sistem aplikasi dan basis data, meliputi kegiatan:

a) Penyusunan dan pendokumentasian rancangan tingkat tinggi dengan mengacu pada dokumen yang mencakup:
   1) Kebutuhan informasi dan struktur informasi;
   2) Pemetaan hak akses atas informasi oleh peran-peran yang terlibat; dan
   3) Infrastruktur pendukung yang mencakup jaringan komunikasi, *server, workstation,* perangkat pendukung, piranti lunak, dan media penyimpanan data.
b) Penyusunan dan pendokumentasian rancangan rinci yang mencakup:
   1) Rancangan kebutuhan sistem aplikasi dan basis data serta infrastruktur pendukung dengan mengacu pada rancangan tingkat tinggi;
   2) Rancangan antarmuka pengguna (*user interface*)/rancangan tampilan memasukkan data (*data entry screen design*), pencarian (*inquiry*), menu bantuan, dan navigasi dari layar ke layar sesuai dengan tingkatan pengguna dan pemisahan fungsi tugas (*segregation of duties*);
   3) Rancangan proses waktu nyata (*real-time processing*) dan/atau proses bertahap (*batch processing*);
   4) Rancangan laporan dan dokumen keluaran;
   5) Formulir pracetak (*pre-printed form*) (jika dibutuhkan) serta distribusinya sesuai dengan tingkatan pengguna dan pemisahan fungsi tugas;
   6) Rancangan antarmuka (*interface*) untuk integrasi dengan aplikasi yang lain (jika dibutuhkan);
   7) Rancangan konversi dan/atau migrasi data (jika dibutuhkan);

8) Rancangan kendali internal (*internal control*) yang diperlukan dalam kegiatan antara lain validasi, otorisasi dan, jejak audit (*audit trail*); dan
9) Rancangan keamanan logika (*logic*).

2) Sistem jaringan pendukung aplikasi, meliputi kegiatan:
a) Penyusunan dan pendokumentasian rancangan tingkat tinggi dengan mengacu pada dokumen yang mencakup:
1) Gambaran secara garis besar mengenai penempatan aplikasi sistem jaringan yang ada dan rencana penempatan aplikasi dalam sistem jaringan; dan
2) Gambaran integrasi antara aplikasi dengan sistem jaringan.
b) Penyusunan dan pendokumentasian rancangan rinci yang mencakup:
1) Rancangan kebutuhan sistem jaringan dengan mengacu pada rancangan tingkat tinggi pengembangan aplikasi;
2) Rancangan kapasitas mengacu pada rencana kapasitas (*capacity planning*) dan/atau kebutuhan dukungan sistem jaringan terhadap aplikasi;
3) Rancangan integrasi aplikasi dengan sistem jaringan yang sudah ada;
4) Rancangan keamanan aplikasi dalam sistem jaringan yang meliputi keamanan fisik maupun logika (*logic*); dan
5) Rancangan penempatan dan pemasangan sesuai dengan Kebijakan dan Standar Keamanan Aplikasi di Pemerintah Daerah.
c) Menghasilkan keluaran:
1) Dokumen rancangan tingkat tinggi; dan
2) Dokumen rancangan rinci.

d. Proses Pengkodean (*coding*) Aplikasi
1) Sistem aplikasi dan basis data, meliputi kegiatan:
a) Pelaksanaan Pengkodean (*coding*) aplikasi dan basis data sesuai dengan rancangan rinci yang telah disetujui;

b) Pengelolaan perubahan dalam pengkodean (*coding*) aplikasi dan basis data;
c) Penyusunan dokumentasi pengkodean (*coding*) aplikasi dan basis data yang terdiri atas:
   1) Formulir perubahan dan rencana dan laporan hasil pengembangan;
   2) Kode program (*source code*) disertai dengan penjelasannya.
d) Pengendalian terhadap kode program (*source code*) yang sesuai dengan Kebijakan dan Standar Keamanan Aplikasi di Pemerintah Daerah.

2) Sistem jaringan pendukung aplikasi, meliputi kegiatan:
   a) Pelaksanaan pengembangan sistem jaringan pendukung aplikasi sesuai dengan rancangan rinci yang telah disetujui;
   b) Pengelolaan perubahan sistem jaringan akibat adanya proses pengembangan sistem aplikasi;
   c) Penyusunan dokumentasi pengembangan sistem jaringan pendukung aplikasi:
      1) Formulir perubahan;
      2) Rencana dan laporan hasil pengembangan jaringan terkait pengembangan aplikasi;
      3) Dokumentasi setiap tahapan pengembangan sistem jaringan pendukung aplikasi;
      4) Petunjuk instalasi sistem jaringan pendukung aplikasi;
      5) Petunjuk teknis pengoperasian dan pemeliharaan sistem jaringan pendukung aplikasi; dan
      6) Materi pelatihan.
   d) Pengendalian konfigurasi perangkat jaringan yang sesuai dengan Kebijakan dan Standar Keamanan Aplikasi di Pemerintah Daerah;
   e) Menghasilkan keluaran:
      1) Sistem aplikasi dan basis data, serta sistem jaringan pendukung aplikasi sesuai dengan rancangan rinci; dan

2) Dokumentasi pengembangan aplikasi.

e. Proses Pengujian Aplikasi

1) Proses pengujian aplikasi meliputi kegiatan:

a) Penyusunan rencana dan skenario untuk setiap jenis pengujian yang mencakup:

1) Tujuan dan sasaran;
2) Strategi dan metode, termasuk langkah-Iangkah alternatif apabila aplikasi gagal dalam pengujian;
3) Ruang lingkup;
4) Asumsi dan batasan;
5) Jadwal;
6) Pihak pelaksana dan kompetensi yang dibutuhkan;
7) Alat bantu;
8) Skenario dengan mempertimbangkan risiko teknologi yang telah diidentifikasi;
9) Kriteria penerimaan (*acceptance criteria*); dan
10) Sumber daya yang diperlukan, termasuk penyiapan lingkungan pengujian yang mencerminkan lingkungan operasional.

b) Pelaksanaan setiap jenis pengujian dengan mengacu pada rencana dan skenario. Jenis pengujian terdiri dari:

1) Pengujian unit (*unit testing*);
2) Pengujian sistem (*system testing*);
3) Pengujian integrasi (*integration testing*); dan
4) UAT.

c) Pelaksanaan analisis hasil pengujian.

2) Proses pengujian aplikasi menghasilkan keluaran:

a) Dokumen rencana dan skenario pengujian;
b) Dokumen hasil pengujian;
c) Dokumen analisis hasil pengujian.

f. Proses Implementasi Aplikasi

1) Proses implementasi aplikasi meliputi kegiatan:

a) Penyusunan rencana implementasi aplikasi di lingkungan operasional yang mencakup sekurang-kurangnya:

1) Kebutuhan sumber daya;

2) Urutan langkah implementasi dari komponen aplikasi;
3) Pemindahan perangkat lunak dari/atau perangkat keras dari lingkungan pengujian ke lingkungan operasional;
4) *Fall-backplan* dan/atau *backup plan* untuk mengantisipasi kegagalan dalam implementasi aplikasi; dan
5) Jadwal pelatihan dan pengajar.

b) Implementasi aplikasi dilakukan sesuai rencana implementasi dengan memperhatikan kebijakan dan standar manajemen rilis yang akan ditetapkan dalam ketentuan tersendiri;
c) Pelaksanaan pelatihan dan transfer pengetahuan;
d) Pendampingan dalam pengoperasian aplikasi dalam kurun waktu tertentu; dan
e) Serah terima aplikasi berikut dokumentasinya kepada pemilik proses bisnis.

2) Proses implementasi aplikasi menghasilkan keluaran:
a) Dokumen rencana implementasi aplikasi;
b) Dokumen implementasi/rilis aplikasi;
c) Laporan pelaksanaan pelatihan;
d) Berita acara serah terima aplikasi;
e) Petunjuk instalasi sistem aplikasi dan basis data;
f) Petunjuk instalasi dan pengoperasian perangkat pendukung (jika dibutuhkan);
g) Payung hukum beserta petunjuk teknis yang selaras dengan proses bisnis; dan
h) Materi pelatihan.

3) Proses tinjauan pasca implementasi aplikasi meliputi kegiatan:
a) Pelaksanaan evaluasi yang dijadikan bahan pembelajaran untuk pengembangan aplikasi selanjutnya yang mencakup:
1) Pencapaian tujuan pengembangan aplikasi; dan
2) Pelaksanaan pengembangan aplikasi.

b) Penyusunan hasil tinjauan pasca implementasi aplikasi ke dalam dokumen tinjauan pasca implementasi aplikasi.

4) Proses tinjauan pasca implementasi aplikasi menghasilkan keluaran:
   a) Laporan evaluasi pasca implementasi aplikasi;
   b) Dokumen tinjauan pasca implementasi aplikasi.

g. Pengendalian Mutu
   1) Pengendalian mutu meliputi kegiatan:
      a) Menyusun rencana pengendalian mutu pengembangan aplikasi;
      b) Melaksanakan pengendalian mutu pengembangan aplikasi melalui evaluasi/audit; dan
      c) Melaporkan hasil kegiatan pengendalian mutu.
   2) Menghasilkan keluaran berupa laporan pengendalian mutu.

h. Standar keamanan aplikasi yang dikembangkan harus mengacu pada Kebijakan dan Standar Keamanan Informasi di Pemerintah Daerah.

6. ISTILAH YANG DIGUNAKAN

a. *Backup Plan* adalah rencana pemulihan sistem ke kondisi semula sebelum terjadi permasalahan terkait proses implementasi.

b. *Fall-backplan* adalah merupakan rencana alternatif (yang menghilangkan dampak negatif) apabila terjadi kegagalan di dalam implementasi TIK.

c. Pengujian integrasi *(integration testing)* adalah pengujian integrasi dari unit-unit dalam suatu aplikasi yang sudah teruji dalam pengujian unit *(unit testing)*.

d. Jejak audit *(audit trail)* adalah urutan kronologis catatan audit yang berkaitan dengan pelaksanaan suatu kegiatan.

e. *Joint Application Development (JAD)* adalah pengembangan aplikasi yang dilaksanakan secara bersama-sama oleh pengembang aplikasi di Pemerintah Daerah dan pengembang aplikasi dari Pihak Ketiga.

f. Konsep dasar operasional adalah dokumen yang menjelaskan karakteristik kuantitatif dan kualitatif suatu sistem yang dibutuhkan dari sudut pandang calon pengguna aplikasi.

g. Penerimaan Kriteria *(acceptance criteria)* adalah serangkaian persyaratan yang harus dipenuhi oleh suatu produk sehingga produk tersebut dapat diterima oleh pengguna. Kriteria penerimaan harus dapat memastikan suatu produk berfungsi sesuai dengan kebutuhan.

h. Rancangan tingkat tinggi *(high level design)* adalah suatu *overview* terhadap aplikasi yang memperlihatkan gambaran menyeluruh dari suatu aplikasi.

i. Siklus pengembangan aplikasi disebut juga sebagai *System Development Life Cycle (SDLC)* adalah siklus pengembangan aplikasi terdiri dari proses analisis kebutuhan, proses perancangan, proses pengembangan, proses pengujian, proses implementasi, dan proses tinjauan pasca implementasi aplikasi yang dapat dilaksanakan oleh internal, pihak ketiga, atau melalui *Joint Application Development (JAD)*.

j. Pengujian sistem *(system testing)* adalah pengujian perangkat keras/lunak yang baru terhadap aplikasi yang sudah terpasang. Pengujian ini bertujuan untuk melihat apakah perangkat keras/Iunak yang baru dapat berintegrasi dengan baik dengan aplikasi yang sudah ada.

k. Pengujian unit *(unit testing)* adalah pengujian masing-masing unit dalam komponen suatu rilis untuk memastikan bahwa setiap unit bekerja dengan baik sesuai dengan fungsinya.

l. *User Acceptance Test (UAT)* adalah uji penerimaan yang dilakukan dengan persetujuan pemilik proses bisnis dengan menugaskan tim *quality assurance* beserta pengguna. Suatu aplikasi dikatakan dapat diterima apabila telah lulus dari UAT. UAT terdiri dari uji penerimaan sistem *(system acceptance testing)*, uji penerimaan contoh *(pilot acceptance test)*, uji setiap fase pengembangan *(roll-out)*, dan pengujian akhir *(final acceptance test)*.

GUBERNUR BANTEN,

ttd

WAHIDIN HALIM

Salinan sesuai dengan aslinya
KEPALA BIRO HUKUM

ttd

AGUS MINTONO, SH.M.Si
Pembina Tk. I
NIP. 19680805 199803 1 010

LAMPIRAN V
PERATURAN GUBERNUR BANTEN
NOMOR 7 TAHUN 2018
TENTANG
TATA KELOLA SISTEM ELEKTRONIK DI LINGKUNGAN PEMERINTAH PROVINSI BANTEN

TATA KELOLA PORTAL WEB

1. UMUM

   Tata kelola *website* merupakan kebijakan terkait dalam penyelenggaraan *website* khususnya pengelolaan *website* di Pemerintah Daerah baik Perangkat Daerah atau Unit Kerja. Tata kelola ini untuk dijadikan sebagai pedoman bagi pengelola *website* di Pemerintah Daerah agar mudah dalam melakukan koordinasi dan komunikasi.

   Standard ini berlaku bagi seluruh pengelola *website* yang dilaksanakan oleh seluruh Perangkat Daerah di Pemerintah Daerah.

2. RUANG LINGKUP

   Ruang lingkup dari tata kelola *website* meliputi penetapan penanggung jawab pengelola *website* dan konten pada Perangkat Daerah dan Unit Kerja di Pemerintah Daerah.

3. KEBIJAKAN

   a. Setiap Pimpinan Perangkat Daerah bertanggung jawab dalam memantau dan mengawasi pembuatan dan pengembangan *website* di Perangkat Daerah masing-masing.

   b. Setiap Pimpinan Perangkat Daerah bertanggung jawab dan mengetahui terhadap penambahan dan perubahan *website* di Perangkat Daerah masing-masing, dalam hal ini meliputi penambahan, perubahan, dan penghapusan *website*.

c. *website* yang sudah dibuat menjadi milik Pemerintah Daerah dan tidak boleh digunakan di luar Pemerintah Daerah tanpa izin dari pejabat yang berwenang.

4. TANGGUNG JAWAB

Pihak-pihak yang terkait dalam pembuatan dan pengembangan *website* terdiri dari:

a. Penanggungjawab *website* adalah Perangkat Daerah di lingkungan Pemerintah Daerah;

b. Penanggungjawab *website* harus melakukan pemutakhiran konten *website* secara rutin atau setiap ada perubahan pada kontennya;

c. Penanggungjawab *website* melakukan evaluasi terhadap *website* yang telah dibangun untuk memastikan keberlangsungan *website* tersebut;

d. Pengguna adalah publik baik eksternal maupun internal Pemerintah Daerah.

5. *PLATFORM WEBSITE*

a. Penyelenggara *website*

Pemeliharaan infrastruktur *website* Pemerintah Daerah dilakukan secara berkelanjutan dan menjadi tanggung jawab Dinas.

Penyediaan jaringan teknologi informasi dan komunikasi di Pemerintah Daerah disiapkan dan dikelola oleh Dinas. Pemanfaatan jaringan teknologi informasi dan komunikasi ini dilaksanakan di seluruh Perangkat Daerah Pemerintah Daerah yang tersebar di seluruh wilayah Daerah.

Secara umum pengelolaan infrastruktur jaringan teknologi informasi dan komunikasi dan *website* Pemerintah Daerah melibatkan antara lain:

1) Dinas;
   a) Penanggungjawab jaringan teknologi informasi dan komunikasi *website* Pemerintah Daerah dan Perangkat Daerah;
   b) Penanggung jawab sistem *website* Pemerintah Daerah (*banten.go.id*);
   c) Penanggung jawab sistem *website* seluruh Perangkat Daerah di lingkungan Pemerintah Daerah.
2) Seksi informasi dan komunikasi publik Dinas.
   a) Penanggungjawab konten *website* Pemerintah Daerah (banten.go.id):
      1) berita utama Pemerintah Daerah;
      2) galeri foto dan video Pemerintah Daerah;
      3) saran dan Pengaduan;
      4) layanan informasi publik;
      5) pelayanan publik.
   b) Pengelola tayangan:
      1) Pengumuman;
      2) agenda kegiatan Pimpinan;
      3) tayangan informasi Pemerintah Daerah di luar berita dan publikasi;
      4) kontributor konten *website* Pemerintah Daerah (*banten.go.id*).
   c) Penanggungjawab konten portal *web (website)* Sekretariat Daerah Provinsi Banten:
      1) Berita Sekretariat Daerah Provinsi Banten;
      2) Galeri foto dan video Sekretariat Daerah Provinsi Banten;
      3) Kontributor konten lainnya.
3) Perangkat Daerah
   a) Penanggungjawab berita dan konten *website* Perangkat Daerah;

b) Kontributor konten portal web (website) Pemerintah Daerah.

4) Unit Kerja

a) Penanggungjawab berita dan konten portal *web (website)* Unit Kerja;

b) Kontributor konten portal *web (website)* Pemerintah Daerah.

Tata Kelola *website* meliputi perencanaan, pembuatan dan pengembangan, dukungan piranti keras, dan piranti lunak serta sumber daya manusia. Tata kelola ini diperlukan guna menjaga kinerja *website* Pemerintah Daerah, sehingga jika terjadi masalah dapat segera diatasi.

Matriks tugas dan tanggung jawab pemeliharaan *website* Pemerintah Daerah

		Tugas	Pelaksana
Top Level Management and Policy maker/Pembuat kebijakan			
1	Pengelola web utama (*Webmaster*)	Menentukan kebijakan, mengelola dan menjaga *website*	Dinas teknis yang membidangi Komunikasi dan Informatika
2	Administrator *web* (*Web Administrator*)	Proses Manajemen	Dinas teknis yang membidangi Komunikasi dan Informatika, Penanggung jawab portal *web (website)* Unit Organisasi, dan Unit Kerja
3	Administrator Konten (*Content Administrator*)	Penentuan kebijakan konten	Dinas teknis yang membidangi Komunikasi dan Informatika (Seksi informasi dan komunikasi publik)
Content Management/Pengelola konten *web*			
4	Penulis (*Author*)	Membangun konten *website*	Dinas teknis yang membidangi Komunikasi dan Informatika, Penanggungjawab *website* Perangkat Daerah, dan Unit Kerja
5	Penyunting (*Editor*)	Merawat konten *Website*	Dinas teknis yang membidangi Komunikasi dan Informatika, Penanggungjawab *website* Perangkat Daerah, dan Unit Kerja

6	Pengembang *web* (*Web Developer*)	Desain *website*	
a	Arsitek *web* (*Web Architect*)	Desain *website*	Dinas teknis yang membidangi Komunikasi dan Informatika
b	Pemogram *web* (*Web Programmer*)	Membuat aplikasi	Dinas teknis yang membidangi Komunikasi dan Informatika
c	Administrator Basis Data (*Database Administrator*)	Merancang basis data *(database)* aplikasi	Dinas teknis yang membidangi Komunikasi dan Informatika, Penanggungjawab portal web *(website)* Perangkat Daerah, dan Unit Kerja
d	*Desainer grafis/Desainer multimedia (Graphic Designer/Multi-media Designer)*	Membuat grafis, gambar, tipografi, animasi, dan multimedia	Dinas teknis yang membidangi Komunikasi dan Informatika

5) Pengelola *web* utama *(webmaster)*

Pengelola *web* utama *(webmaster)* bertanggung jawab sebagai berikut:

a) Merencanakan, mengembangkan, mengelola, dan mengevaluasi *website* secara berkelanjutan;
b) Menyusun Prosedur Operasional Standar Pengelolaan *website*;
c) Menetapkan persyaratan teknis *website*;
d) Menentukan situs terkait;
e) Memberikan pelayanan dan perawatan yang berkaitan dengan *website*.

6) Administrator *web (web Administrator*)

Administrator *web* (*web Administrator*) bertanggung jawab sebagai berikut:

a) Membantu *webmaster* dalam merencanakan, mengembangkan, mengelola, dan mengevaluasi *website* secara berkelanjutan serta menyusun Prosedur Operasional Standar;
b) Mengelola hak akses pengguna ke *website*;
c) Melakukan koordinasi dengan Perangkat Daerah dan Unit Kerja terkait dalam pengelolaan *website*;
d) Melakukan cadangan (*back up*) sistem dan data.

7) Administrator konten (*content administrator*)

Administrator konten (*content administrator*) bertanggung jawab sebagai berikut:

a) Membuat, menyiapkan, dan mengelola konten baru untuk setiap Perangkat Daerah dan unit kerja;
b) Menyusun Prosedur Operasional Standar penyusunan konten *website*.

8) Penulis (*author*)

Penulis (*author*) bertanggung jawab menyusun konten *website*.

9) Penyunting (*editor*)

Penyunting (*editor*) bertanggung jawab atas kelayakan konten *website*.

10) Pengembang *web (web developer*)

Pengembang *web (web developer*) bertanggung jawab sebagai berikut:

a) Merencanakan dan membangun dalam pengembangan *website*;
b) Membuat Petunjuk Teknis Penggunaan *website*.

<u>Pengembang *web* (*web developer*) terdiri atas:</u>

a) Arsitek *web* (*web architect*)

Arsitek *web* (*web architect*) bertanggung jawab sebagai berikut:

1) Membuat rancangan dan menentukan struktur bagian-bagian *website* yang akan dibuat;

2) Menentukan skema/hierarki tautan (*link-link*) yang akan dibuat, dan layanan yang akan diberikan ke publik serta menentukan pola *website*.

b) Pemogram *web* (*web programmer*)

Pemogram *web* (*web programmer*) bertanggung jawab sebagai berikut:

1) Membuat dan melakukan pengaturan (*setup*) layanan interaktif dalam lingkungan *website*;
2) Menjalankan program-program yang ada dalam *website*.

c) Administrator basis data (*database administrator*)

Administrator basis data (*database administrator*) bertanggung jawab merancang dan mengelola sistem basis data (*database*).

d) Desainer Grafis/Desainer Multimedia (*Graphic Designer/Multimedia Designer*)

Desainer Grafis/Desainer Multimedia (*Graphic Designer/Multimedia Designer* bertanggung jawab menciptakan hasil visualisasi dari suatu ide ke dalam bentuk grafis, gambar, tipografi, animasi, dan multimedia.

b. Pengelola Portal *Web (Website)* Pemerintah Daerah

Susunan dan tugas pokok serta fungsi pengelola *website* Pemerintah Daerah ditetapkan oleh Gubernur.

GUBERNUR BANTEN,

ttd

WAHIDIN HALIM

Salinan sesuai dengan aslinya
KEPALA BIRO HUKUM

ttd

AGUS MINTONO, SH.M.Si
Pembina Tk. I
NIP. 19680805 199803 1 010

LAMPIRAN VI
PERATURAN GUBERNUR BANTEN
NOMOR 7 TAHUN 2018
TENTANG
TATA KELOLA SISTEM ELEKTRONIK DI LINGKUNGAN PEMERINTAH PROVINSI BANTEN

KETERHUBUNGAN ANTAR SISTEM INFORMASI
(INTEROPERABILITAS)

1. UMUM

Interoperabiltas yang dalam IEEE *Standard Computer Dictionary* didefinisikan sebagai *"The ability of two or more systems or components to exchange information and to use the information that has been exchanged"*, secara teknis menggambarkan kemampuan 2 (dua) atau lebih sistem untuk saling tukar menukar data atau informasi dan saling dapat mempergunakan data atau informasi yang dipertukarkan tersebut.

Interoperabilitas bukanlah berarti penentuan atau penyamaan penggunaan platform perangkat keras, atau perangkat lunak semisal *operating system* tertentu misalnya, bukan pula berarti penentuan atau penyeragaman *data base* yang akan dipergunakan dalam penyimpanan data, dan juga bukan berarti penentuan atau penyeragaman penggunaan bahasa pemrograman dalam pengembangan sistem informasi pemerintahan. Interoperabilitas harus dapat dicapai dalam keragaman penggunaan perangkat keras dan perangkat lunak baik *operating system, data base* dan bahasa pemrograman yang tersedia saat ini dan khususnya yang telah dipergunakan di berbagai instansi pemerintahan baik pusat ataupun daerah. *Interoperabilitas* dalam keragaman ini hanya dapat dicapai melalui standarisasi format pertukaran data, yang secara teknis saat ini banyak dilakukan dengan menggunakan basis JSON, XML atau CSV. Setiap pihak yang terkait berkewajiban menggunakan standard yang telah ditetapkan sebagai acuan bersama.

2. RUANG LINGKUP

Ruang lingkup dari keterhubungan antar sistem meliputi:

a. *Interoperabilitas* pada sistem informasi *Government to Government (G2G), Government to Employee (G2E), Government to Citizen (G2C), Government to Business (G2B)* ; dan

b. *Interoperabilitas* dengan memanfaatkan format dokumen terbuka.

c. *Interoperabilitas* teknis: memastikan bahwa data dapat terkirim pada pihak-pihak yang berkepentingan, terlepas dari terstruktur atau tidaknya data yang dikirimkan tersebut.

d. *Interoperabilitas* semantik: memastikan bahwa data dipahami secara sama oleh pihak-pihak yang berkepentingan, terlepas dari mekanisme pengirimannya.

e. *Interoperabilitas* proses: memastikan bahwa data terkirim pada saat yang tepat, dalam urutan yang tepat, dalam satu kerangka koordinasi kerja antara pihak-pihak yang berkepentingan.

f. Untuk implementasi yang optimal dalam satu lingkungan kerja, ketiga klasifikasi interoperabilitas tersebut harus terwujud.

3. KEBIJAKAN

a. Setiap Perangkat Daerah yang ada di lingkungan Pemerintah Daerah wajib memiliki skema data pada sistem informasi yang dimilikinya dalam rangka untuk kemudahan interoperabilitas dan teknologinya ditentukan oleh Dinas;

b. Perangkat Daerah dapat menyesuaikan atau mengacu pada skema data yang teknologinya ditentukan oleh Dinas (sesuai rujukan ketentuan Internasional) dari masing-masing instansi terkait;

c. Peraturan dan kebijakan yang dikeluarkan oleh Pemerintah Daerah berkaitan interoperabilitas harus mengacu dan selaras dengan peraturan dan kebijakan nasional tentang *e-Government*;

d. Jenis data yang terbuka dan tertutup akan ditentukan oleh Dinas;

e. Transaksi data untuk interoperabilitas dilakukan dalam format terbuka yang teknologinya ditentukan oleh Dinas.

4. STANDARD ACUAN

a. Standardisasi dalam *interoperabilitas* bukanlah penyeragaman penggunaan perangkat keras ataupun perangkat lunak yang akan dipergunakan;

b. Standardisasi dalam *interoperabilitas* lebih mengarah pada Standardisasi format data-data yang akan dipertukarkan;

c. Data dapat dipertukarkan terlepas dari *platform* yang dipergunakan di setiap intansi pengguna *(platform independen)*;

d. Pertukaran data dapat dilakukan dengan mempergunakan berbagai macam protokol pertukaran data yang tersedia;

e. Pemrosesan data yang dipertukarkan dapat dilakukan baik secara otomatis maupun otomatis dengan persetujuan operator;

f. Pengelolaan data lebih *fleksible*, lebih *cost* efektif dan tidak perlu mempergunakan perangkat yang *proprietary*.

5. TEKNIS

a. Setiap Pengelola Sistem Elektronik wajib membuat *Application Programming Interface (API)* pada sistem informasi yang digunakannya;

b. *Application Programming Interface (API)* yang dibuat harus mendapat persetujuan Dinas;

c. Setiap *Application Programming Interface (API)* yang dibuat harus disertai dengan dokumentasi lengkap dan contoh penggunaanya.

d. Alamat untuk mempublikasikan *Application Programming Interface (API)* ditentukan oleh Dinas;

6. HAK AKSES

a. Setiap Pengelola Sistem Elektronik yang menyediakan *Application Programming Interface (API)* pada sistem informasi yang digunakannya wajib menggunakan pengamanan terhadap pengguna yang menggunakan *Application Programming Interface (API)* tersebut;

b. Pengamanan yang paling sederhana terhadap *Application Programming Interface (API)* yang dapat digunakan adalah dengan menggunakan *API KEY* atau *API TOKEN*;

c. Tingkat pengamanan yang digunakan dapat diubah oleh Dinas sesuai dengan tingkat perkembangan teknologi informatika;

7. PERMOHONAN HAK AKSES

a. Setiap Pengelola Sistem Elektronik yang mengajukan permintaan hak akses terhadap *Application Programming Interface (API)* milik Pemerintah Daerah harus mengajukan permohonan secara online menggunakan SOP yang ditentukan oleh Dinas;

b. Permohonan hak akses tersebut harus dilengkapi dengan Surat Permohonan Resmi yang ditandatangani oleh Pimpinan Lembaga Pengelola Sistem Elektronik yang mengajukan hak akses tetsebut.

c. Surat Permohonan tersebut dilengkapi dengan dokumen pendukung yang diperlukan yang menjelaskan lembaga pemohon hak akses dan tujuan mengajukan hak akses;

d. Kepala Dinas atau pejabat yang ditugaskan untuk hal tersebut, dapat menyetujui atau menolak permintaan hak akses terhadap *Application Programming Interface (API)* atas nama Gubernur.

GUBERNUR BANTEN,

ttd

WAHIDIN HALIM

Salinan sesuai dengan aslinya
KEPALA BIRO HUKUM

ttd

AGUS MINTONO, SH.M.Si
Pembina Tk. I
NIP. 19680805 199803 1 010