SALINAN

**BUPATI GUNUNG MAS**
**PROVINSI KALIMANTAN TENGAH**

**PERATURAN BUPATI GUNUNG MAS**
**NOMOR 7 TAHUN 2019**

**TENTANG**

**STANDARISASI TEKNOLOGI INFORMASI DAN KOMUNIKASI BERBASIS ELEKTRONIK**

**DENGAN RAHMAT TUHAN YANG MAHA ESA**

**BUPATI GUNUNG MAS,**

Menimbang :

a. bahwa kemajuan teknologi informasi dan komunikasi yang sangat pesat memberi peluang pengelolaan data dan informasi yang cepat dan akurat sehingga perlu dimanfaatkan oleh Pemerintah Daerah dalam melaksanakan tugas dan fungsinya dalam memberikan pelayanan kepada masyarakat;
b. bahwa penyelenggaraan layanan elektronik pemerintahan (*e-Government*) di Kabupaten Gunung Mas perlu kesamaan pemahaman, keserampakan tindak, dan keterpaduan langkah dari seluruh Perangkat Daerah untuk mewujudkan tata kelola pemerintahan yang baik dalam meningkatkan layanan publik yang efektif dan efisien;
c. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b, perlu menetapkan Peraturan Bupati tentang Standarisasi Teknologi Informasi dan Komunikasi Berbasis Elektronik;

Mengingat :

1. Undang-Undang Nomor 5 Tahun 2002 tentang Pembentukan Kabupaten Katingan, Kabupaten Saruyan, Kabupaten Sukamara, Kabupaten Lamandau, Kabupaten Gunung Mas, Kabupaten Pulang Pisau, Kabupaten Murung Raya, dan Kabupaten Barito Timur di Provinsi Kalimantan Tengah (Lembaran Negara Republik Indonesia Tahun 2002 Nomor 18, Tambahan Lembaran Negara Republik Indonesia Nomor 4180);

| HUKUM | KASUBBAG |
| --- | --- |
| | |

2. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843);
3. Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 61, Tambahan Lembaran Negara Republik Indonesia Nomor 4846);
4. Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik (Lembaran Negara Republik Indonesia Tahun 2009 Nomor 112, Lembaran Negara Republik Indonesia Nomor 5038);
5. Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 244, Tambahan Lembaran Negara Republik Indonesia Nomor 5587) sebagaimana telah diubah beberapa kali terakhir dengan Undang-Undang Nomor 9 Tahun 2015 tentang Perubahan Kedua atas Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2015 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 5679);
6. 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);
7. Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2012 Nomor 189, Tambahan Lembaran Negara Republik Indonesia Nomor 5348);
8. Peraturan Pemerintah Nomor 12 Tahun 2017 tentang Pembinaan dan Pengawasan Penyelenggaraan Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2017 Nomor 73, Tambahan Lembaran Negara Republik Indonesia Nomor 6041);
9. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
10. Peraturan Menteri Komunikasi dan Informatika Nomor 41/PER/MEN.KOMINFO/11/2007 tentang Panduan Umum Tata Kelola Teknologi Informasi dan Komunikasi Nasional;

| KABAG HUKUM | KASUBBAG |
| --- | --- |
| | |

11. Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2015 tentang Registrar Nama Domain Instansi Penyelenggara Negara (Berita Negara Republik Indonesia Tahun 2015 Nomor 209);
12. Peraturan Daerah Kabupaten Gunung Mas Nomor 8 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah Kabupaten Gunung Mas (Lembaran Daerah Kabupaten Gunung Mas Tahun 2016 Nomor 236, Tambahan Lembaran Daerah Kabupaten Gunung Mas Nomor 236.a);

MEMUTUSKAN:

Menetapkan : **PERATURAN BUPATI TENTANG STANDARISASI TEKNOLOGI INFORMASI DAN KOMUNIKASI BERBASIS ELEKTRONIK.**

## BAB I
## KETENTUAN UMUM
### Pasal 1

Dalam Peraturan Bupati ini yang dimaksud dengan:
1. Daerah adalah Kabupaten Gunung Mas.
2. Bupati adalah Bupati Gunung Mas.
3. Pemerintah Daerah adalah Bupati sebagai unsur penyelenggara Pemerintahan Daerah yang memimpin pelaksanaan urusan pemerintahan yang menjadi kewenangan daerah otonom.
4. Perangkat Daerah yang selanjutnya disingkat PD adalah Unsur Pembantu Bupati dan Dewan Perwakilan Rakyat Daerah dalam penyelenggaraan urusan pemerintahan di Kabupaten Gunung Mas.
5. Dinas adalah Dinas Komunikasi dan Informatika, Statistik dan Persandian Kabupaten Gunung Mas.
6. Kepala Dinas adalah Kepala Dinas Komunikasi dan Informatika, Statistik dan Persandian Kabupaten Gunung Mas.
7. Standarisasi Teknologi Informasi dan Komunikasi Elektronik Pemerintahan (*E-Government*) Berbasis Elektronik di Kabupaten Gunung Mas yang selanjutnya disebut sebagai Standarisasi Elektronik Pemerintahan (*E-Government*) adalah standar yang digunakan dalam pemanfaatan teknologi informasi dan komunikasi pada proses pemerintahan secara elektronik.
8. Elektronik Pemerintahan (*E-Government*) adalah pemanfaatan Teknologi Informasi dan Komunikasi untuk meningkatkan efisiensi, efektifitas, transparasi dan akuntabilitas penyelenggaraan pemerintah.
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. Teknologi Informasi dan Komunikasi adalah suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan/atau menyebarluaskan informasi.

| KABAG HUKUM | KASUBBAG |
|---|---|
| | |

11. Data adalah kumpulan fakta berupa angka, huruf, gambar, suara, peta, atau citra tentang karakteristik atau ciri-ciri suatu objek.
12. 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.
13. Infrastruktur teknologi informasi dan komunikasi adalah perangkat keras, piranti lunak sistem operasi dan aplikasi, data center serta fasilitas pendukung lainnya, untuk mendukung penyelenggaraan Elektronik Pemerintahan (*E-Government*).
14. Pusat Data (*Data Center*) adalah suatu fasilitas yang digunakan untuk menempatkan sistem komputer dan komponen terkaitnya, seperti sistem telekomunikasi dan sistem kumpulan paket program untuk menunjang kinerja suatu perangkat lunak, program dan sebagainya untuk suatu sistem operasi (*repository*).
15. Aplikasi adalah komponen Sistem Informasi yang digunakan untuk menjalankan fungsi, proses dan mekanisme kerja yang mendukung pelaksanaan Elektronik Pemerintahan (*E-Government*).
16. Aplikasi Umum adalah aplikasi Elektronik Pemerintahan (*E-Government*) yang dapat digunakan oleh seluruh PD di Kabupaten Gunung Mas.
17. Aplikasi Khusus adalah aplikasi Elektronik Pemerintahan (*E-Government*) yang digunakan untuk memenuhi kebutuhan PD tertentu sesuai dengan tugas dan fungsinya.
18. Sumber Daya Informatika adalah sumber daya dalam bentuk perangkat keras, piranti lunak, dan sumber daya manusia yang terkait dengan teknologi informasi dan komunikasi.
19. Cetak Biru *(Blue Print)* adalah dokumen perencanaan yang menjadi acuan penyelenggaraan Elektronik Pemerintahan (*E-Government*).
20. Interoperabilitas adalah kemampuan dua sistem atau dua komponen atau lebih untuk bertukar informasi dan untuk menggunakan informasi yang telah dipertukarkan.
21. 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.
22. Akses adalah kegiatan melakukan interaksi dengan sistem elektronik yang berdiri sendiri atau dalam jaringan.
23. Badan Usaha adalah perusahaan perseorangan atau perusahaan persekutuan, baik yang berbadan hukum maupun yang tidak berbadan hukum.
24. 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.

Pasal 2

(1) Peraturan Bupati ini dimaksudkan sebagai pedoman Standarisasi Elektronik Pemerintahan (*E-Government*) Kabupaten Gunung Mas.
(2) Peraturan Bupati ini bertujuan untuk mencapai tata kelola pemerintahan yang baik melalui penerapan standarisasi Elektronik Pemerintahan (*E-Government*) di Kabupaten Gunung Mas.

| KABAG HUKUM | KASUBBAG |
| --- | --- |
| | |

Pasal 3

Ruang Lingkup pengaturan dalam Peraturan Bupati ini meliputi:
a. infrastruktur teknologi informasi dan komunikasi Elektronik Pemerintahan (*E-Government*);
b. aplikasi;
c. data dan informasi;
d. surat elektronik (*e-mail*) Kabupaten Gunung Mas;
e. tata kelola; dan
f. evaluasi.

## BAB II
## INFRASTRUKTUR TEKNOLOGI INFORMASI DAN KOMUNIKASI ELEKTRONIK PEMERINTAHAN (*E-GOVERNMENT*)

Pasal 4

(1) Infrastruktur teknologi informasi dan komunikasi yang digunakan dalam Standarisasi Elektronik Pemerintahan (*E-Government*) harus sesuai dengan standar teknologi, Interoperabilitas dan keamanan informasi.
(2) Ketentuan 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) Ketentuan 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) Ketentuan standar keamanan informasi sebagaimana dimaksud pada ayat (1) tercantum dalam Lampiran I yang merupakan bagian tidak terpisahkan dari Peraturan Bupati ini.

Pasal 5

(1) Dinas menyediakan fasilitas berupa Ruang Server sebagai tempat server data/Pusat Data (*Data Center*) dalam penyelenggaraan Standarisasi Elektronik Pemerintahan (*E-Government*).
(2) Ruang server dan server data sebagaimana dimaksud pada ayat (1) dikelola oleh Dinas.
(3) Ketentuan ruang server sebagai tempat server data/Pusat Data (*Data Center*) sebagaimana dimaksud pada ayat (1) tercantum dalam Lampiran II yang merupakan bagian tidak terpisahkan dari Peraturan Bupati ini.

| KABAG HUKUM | KASUBBAG |
| --- | --- |
| | |

## BAB III
## APLIKASI
### Pasal 6

(1) Aplikasi Elektronik Pemerintahan (*E-Government*) terdiri atas Aplikasi Umum dan Aplikasi Khusus.
(2) Aplikasi Elektronik Pemerintahan (*E-Government*) sebagaimana dimaksud pada ayat (1) harus dilengkapi dengan:
    a. kode program;
    b. basis data; dan
    c. dokumentasi.
(3) Dokumentasi sebagaimana dimaksud pada ayat (2) huruf c sekurang-kurangnya terdiri atas:
    a. identifikasi kebutuhan;
    b. desain aplikasi;
    c. penjelasan kode program;
    d. prosedur standar manual;
    e. penjelasan basis data;
    f. hak Akses; dan
    g. kebutuhan sumber daya informatika.

### Pasal 7

(1) Aplikasi Elektronik Pemerintahan (*E-Government*) harus memenuhi standar pengembangan, interoperabilitas, dan standar keamanan informasi.
(2) Penyelenggara aplikasi pada PD wajib berkoordinasi dengan Dinas dalam perencanaan dan pengembangan aplikasi.
(3) Hak cipta atas aplikasi dan kelengkapannya sebagaimana dimaksud dalam ayat (1) yang dibangun oleh mitra kerja menjadi milik Pemerintah Kabupaten Gunung Mas.
(4) Aplikasi sebagaimana dimaksud pada ayat (1) yang berbasis *web* harus dipasang pada ruang server/Pusat Data (*Data Center*) di Dinas.
(5) Ketentuan standar pengembangan aplikasi sebagaimana dimaksud pada ayat (1) tercantum dalam Lampiran III yang merupakan bagian tidak terpisahkan dari Peraturan Bupati ini.

## BAB IV
## DATA DAN INFORMASI
### Pasal 8

(1) Data dan informasi dalam penyelenggaraan Elektronik Pemerintahan (*E-Government*) wajib disediakan oleh masing-masing PD.
(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 PD dan Dinas.
(4) Data dan informasi sebagaimana dimaksud pada ayat (1) dapat dimanfaatkan oleh seluruh PD.

| KABAG HUKUM | KASUBBAG |
| --- | --- |
| | |

Pasal 9

(1) Data dan informasi sebagaimana dimaksud dalam Pasal 8 ayat (1) merupakan Hak Cipta Kabupaten Gunung Mas.
(2) Data dan informasi sebagaimana dimaksud dalam Pasal 8 ayat (1) harus disimpan pada server data Dinas.
(3) Pemanfaatan data dan informasi sebagaimana dimaksud dalam Pasal 8 ayat (1) harus berkoordinasi dengan Dinas.
(4) Pemanfaatan data dan informasi selain oleh PD sebagaimana dimaksud dalam Pasal 8 ayat (4) harus berkoordinasi dengan Pejabat Pengelola Informasi dan Dokumentasi Kabupaten Gunung Mas.

## BAB V
## SURAT ELEKTRONIK (*E-MAIL*)

Pasal 10

(1) Alamat surat elektronik (*e-mail*) resmi Kabupaten Gunung Mas menggunakan nama domain mail.gunungmaskab.go.id.
(2) Akun surat elektronik (*e-mail*) resmi Kabupaten Gunung Mas menggunakan alamat @gunungmaskab.go.id.
(3) Surat elektronik (*e-mail*) Kabupaten Gunung Mas diperuntukkan bagi Aparatur Sipil Negara Kabupaten Gunung Mas dengan mengajukan permohonan secara resmi kepada Dinas.
(4) Surat elektronik Kabupaten dikelola oleh Dinas.

## BAB VI
## TATA KELOLA

Pasal 11

Tata kelola Elektronik Pemerintahan (*E-Government*) di Kabupaten Gunung Mas dilaksanakan pada tingkat Kabupaten dan PD.

Pasal 12

(1) Tata kelola Elektronik Pemerintahan (*E-Government*) di Kabupaten dikoordinasikan oleh Dinas.
(2) Dalam tata kelola *E-Government* Kabupaten, Dinas mempunyai tugas:
    a. menyusun Cetak Biru (*Blue Print*);
    b. menyusun standar manual peralatan, interoperabilitas, dan keamanan Sistem Informasi;
    c. memfasilitasi PD dalam pembangunan dan pengembangan Sistem Informasi;
    d. membina sumber daya manusia di bidang teknologi informasi dan komunikasi;
    e. menyediakan data dan informasi untuk keperluan internal dan eksternal sesuai dengan tugas dan fungsinya;
    f. menyediakan infrastruktur teknologi informasi dan komunikasi Elektronik Pemerintahan (*E-Government*);
    g. membangun, mengembangkan dan memelihara Aplikasi Umum berdasarkan masukan proses kerja PD;

| KABAG HUKUM | KASUBBAG |
|---|---|
| | |

h. membangun, mengembangkan dan memelihara aplikasi yang melibatkan lebih dari satu PD;
i. memfasilitasi dan mengelola nama sub domain Kabupaten untuk situs *web* resmi PD;
j. menyediakan menu PD pada portal *web* Kabupaten sebagai sarana pendukung penyelenggaraan *E-Government*; dan
k. melakukan evaluasi Sistem Informasi secara berkala.

(3) Cetak Biru (*blue print*) sebagaimana dimaksud pada ayat (2) huruf a harus memuat:
a. arsitektur infrastruktur teknologi informasi dan komunikasi Elektronik Pemerintahan (*E-Government*);
b. arsitektur Sistem Informasi;
c. kebutuhan data dan informasi;
d. tata kelola teknologi informasi dan komunikasi; dan
e. rencana pengembangan teknologi informasi dan komunikasi.

Pasal 13

(1) Tata kelola Elektronik Pemerintahan (*E-Government*) PD dilaksanakan oleh masing-masing PD yang ada berdasarkan kewenangannya.
(2) Penyelenggara Elektronik Pemerintahan (*E-Government*) sebagaimana dimaksud pada ayat (1) sesuai kewenangannya mempunyai tugas:
a. melaporkan dan mengkoordinasikan penyelenggaraan Elektronik Pemerintahan (*E-Government*);
b. menyusun rencana dan mengembangkan Elektronik Pemerintahan (*E-Government*) PD sesuai Cetak Biru (*Blue Print*) sebagaimana yang dimaksud dalam Pasal 12 ayat (2) huruf a;
c. membina sumber daya manusia di bidang teknologi informasi dan komunikasi;
d. menyediakan dan memutakhirkan data dan informasi;
e. menyediakan Akses bagi Sistem Informasi lain;
f. menyediakan infrastruktur;
g. menyediakan Aplikasi Khusus; dan
h. mengelola situs web unit organisasi.
(3) Penyelenggara Elektronik Pemerintahan (*E-Government*) PD sebagaimana dimaksud pada ayat (1) berkoordinasi dengan Dinas.

Pasal 14

(1) Untuk memperlancar penyelenggaraan Elektronik Pemerintahan (*E-Government*) Kabupaten, dapat dibentuk Tim Pengelola Elektronik Pemerintahan (*E-Government*) Kabupaten yang ditetapkan dengan Keputusan Bupati.
(2) Penyelenggaraan Elektronik Pemerintahan (*E-Government*) sebagaimana dimaksud dalam Pasal 12 dan Pasal 13 dapat bekerja sama dengan instansi Pemerintah Pusat, Pemerintah Provinsi, Badan Usaha, dan/atau masyarakat.

| ABAG HUKUM | KASUBBAG |
| --- | --- |
| | |

**BAB VII**
**EVALUASI**
Pasal 15

(1) Evaluasi Elektronik Pemerintahan (*E-Government*) di Daerah dilakukan oleh Kepala Dinas secara periodik setiap 1 (satu) tahun sekali.
(2) Evaluasi Elektronik Pemerintahan (*E-Government*) sebagaimana dimaksud pada ayat (1), meliputi:
    a. infrastruktur teknologi informasi dan komunikasi;
    b. aplikasi;
    c. data dan informasi; dan
    d. tata kelola.
(3) Hasil evaluasi sebagaimana dimaksud pada ayat (2) dilaporkan kepada Bupati.

**BAB VIII**
**KETENTUAN PENUTUP**
Pasal 16

Peraturan Bupati ini mulai berlaku pada tanggal diundangkan.

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

Ditetapkan di Kuala Kurun
pada tanggal 20 Februari 2019

**BUPATI GUNUNG MAS,**

**ttd**

**ARTON S. DOHONG**

Diundangkan di Kuala Kurun
pada tanggal 28 Februari 2019

**SEKRETARIS DAERAH**
**KABUPATEN GUNUNG MAS,**

**ttd**

**YANSITERSON**

**BERITA DAERAH KABUPATEN GUNUNG MAS TAHUN 2019 NOMOR 444**

Salinan sesuai dengan aslinya
KEPALA BAGIAN HUKUM,

**GUANHIN, SH**
NIP. 19651110 199203 1 013

**LAMPIRAN I**
**PERATURAN BUPATI GUNUNG MAS**
**NOMOR 7 TAHUN 2019**
**TENTANG**
**STANDARISASI TEKNOLOGI INFORMASI DAN KOMUNIKASI BERBASIS ELEKTRONIK**

## STANDAR KEAMANAN INFORMASI

(1) TUJUAN

Standarisasi ini digunakan sebagai pedoman dalam rangka melindungi aset informasi Kabupaten dari berbagai bentuk ancaman baik dari dalam maupun luar 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. Standarisasi ini berlaku untuk pengelolaan pengamanan seluruh aset informasi Daerah dan dilaksanakan oleh seluruh PD, pegawai Kabupaten baik sebagai pengguna maupun pengelola Teknologi Informasi dan Komunikasi Elektronik Pemerintahan (*E-Government*), dan pihak ketiga di lingkungan Pemerintah Kabupaten Gunung Mas.
b. Aset informasi Kabupaten 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 PD bertanggung jawab mengatur penerapan Kebijakan dan Standar Keamanan Informasi yang ditetapkan dalam Peraturan Bupati ini di unit kerja masing-masing.
b. PD harus menerapkan Kebijakan dan Standar Keamanan Informasi yang ditetapkan dalam Peraturan Bupati ini di PD masing-masing.
c. setiap Kepala PD bertanggung jawab mengatur pelaksanaan pengamanan dan perlindungan aset informasi di Unit masing-masing dengan mengacu pada Kebijakan dan Standar Keamanan Informasi di Kabupaten yang ditetapkan dalam Peraturan Bupati ini.
d. Dinas dan PD bertanggung jawab meningkatkan pengetahuan, keterampilan, dan kepedulian terhadap keamanan informasi pada seluruh pengguna di lingkungan unit kerja masing-masing.

| KABAG HUKUM | KASUBBAG |
| --- | --- |
| | |

e. Dinas dan PD 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 Daerah.
g. Dinas dan PD melakukan evaluasi terhadap pelaksanaan Keamanan Informasi secara berkala untuk menjamin efektivitas dan meningkatkan keamanan informasi.
h. Inspektorat Kabupaten melakukan audit internal Keamanan Informasi di Daerah untuk memastikan pengendalian, proses, dan prosedur Keamanan Informasi dilaksanakan secara efektif sesuai dengan Kebijakan dan Standar Keamanan Informasi di Daerah.
i. Dinas dan PD menggunakan laporan audit internal Keamanan Informasi untuk meninjau efektivitas penerapan Keamanan Informasi dan melakukan tindak lanjut terhadap temuan auditor.

(4) TANGGUNGJAWAB

a. Pihak-pihak yang terkait dalam keamanan informasi terdiri dari:
   1. pemilik aset informasi adalah Kepala PD yang memiliki kebutuhan akan keamanan informasi untuk mendukung tugas dan fungsinya;
   2. petugas keamanan informasi adalah pegawai PD 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; dan
   4. pengguna, adalah pegawai dan bukan pegawai PD yang mengakses informasi PD,
b. pemilik aset informasi mempunyai tanggung jawab terhadap:
   1. menetapkan target keamanan informasi setiap tahunnya dan menyusun rencana kerja masing-masing PD, maupun yang bersifat lintas unit;
   2. memastikan efektivitas dan konsistensi penerapan Kebijakan dan Standar Keamanan Informasi di Daerah; dan
   3. melaporkan kinerja penerapan Kebijakan dan Standar Keamanan Informasi di 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 Daerah;
   2. memberi masukan peningkatan terhadap Kebijakan dan Standar Keamanan Informasi di 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

| KABAG HUKUM | KASUBBAG |
| --- | --- |
| | |

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; dan
   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 Daerah
      a) Dinas dan Unit Organisasi harus menggunakan catatan penerapan Kebijakan dan Standar Keamanan Informasi di Daerah untuk mengukur kepatuhan dan efektivitas penerapan keamanan informasi.
      b) catatan penerapan Kebijakan dan Standar Keamanan Informasi di 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

| KABAG HUKUM | KASUBBAG |
| --- | --- |
| | |

f) dokumen referensi yang digunakan dalam menyusun dokumen pendukung kebijakan keamanan informasi.

3. pengendalian dokumen
   a) Dinas dan PD 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 PD 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 yang berlaku.

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 di posisi kunci (*key person*) harus memastikan ketersediaan pengganti pegawai tersebut dengan kompetensi yang setara apabila pegawai yang bersangkutan mutasi/berhenti;
   3. 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; dan
      d) melaporkan kejadian, potensi kejadian, atau risiko keamanan informasi sesuai dengan Kebijakan dan Standar Keamanan Informasi di Daerah.
   4. pemeriksaan latar belakang calon pegawai dan pihak ketiga, Pemerintah Daerah harus memperhitungkan privasi, perlindungan data pribadi dan/atau pekerjaan berdasarkan peraturan perundang-undangan yang berlaku, meliputi:
      a) ketersediaan referensi, dari referensi hubungan kerja, dan referensi pribadi;
      b) pemeriksaan kelengkapan dan ketepatan dari riwayat hidup pemohon;
      c) konfirmasi kualifikasi akademik dan profesional yang diklaim;
      d) pemeriksaan identitas (KTP, paspor atau dokumen sejenis); dan
      e) pemeriksaan lebih rinci, seperti pemeriksaan catatan kriminal.

| KABAG HUKUM | KASUBBAG |
| --- | --- |
| | |

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) perlindungan keamanan 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 pipa pelindung (*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 pemisah peralatan jaringan dan perangkat jaringan (*panel patch*) diperlukan untuk mengurangi kesalahan; dan

| KABAG HUKUM | KASUBBAG |
| --- | --- |
| | |

6) pengendalian untuk sistem informasi yang sensitif harus mempertimbangkan:
   a. penggunaan pipa pelindung (*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 pemisah peralatan jaringan dan perangkat jaringan (*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/kesepakatan tingkat layanan (*service level agreement*) 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 Daerah.
   Penggunaan perangkat yang dibawa ke luar dari Kabupaten 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.

| KABAG HUKUM | KASUBBAG |
| --- | --- |
| | |

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 PD 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, pusat data (*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 PD 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 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 komunikasi data yang dapat bernegosiasi ulang jika terjadi kerusakan data atau gangguan jalur komunikasi (*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.

| KABAG HUKUM | KASUBBAG |
| --- | --- |
| | |

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) intruksi 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.

| KABAG HUKUM | KASUBBAG |
| --- | --- |
| | |

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 Kementerian 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 (*miss-routing*), 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.

| KABAG HUKUM | KASUBBAG |
| --- | --- |
| | |

3) pengendalian pertukaran informasi bila menggunakan perangkat komunikasi elektronik, mencakup:
   a. pencegahan terhadap penyalahgunaan wewenang pegawai dan pihak ketiga yang dapat membahayakan PD;
   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; dan
      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 perlu 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

PD 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.

| KABAG HUKUM | KASUBBAG |
| --- | --- |
| | |

2. pengelolaan Akses pengguna
   Dinas dan PD 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 Kabupaten;
   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 PD 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;

| HUKUM | KASUBBAG |
| --- | --- |
| | |

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 elektroniktanpa 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; dan
      5) mendapat persetujuan pejabat yang berwenang/ atasan langsung pegawai.
   b) 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.

| BAG HUKUM | KASUBBAG |
| --- | --- |
| | |

2. pengolahan data pada aplikasi
   a) pemeriksaan data masukan harus mempertimbangkan:
      1) penerapan masukan rangkap (*dual input*) atau mekanisme pengecekan masukan lainnya untuk mendeteksi kesalahan sebagai berikut:
         a. di luar rentang/batas nilai-nilai yang diperbolehkan;
         b. karakter tidak valid dalam bidang (*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 kunci bidang 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 seluruh 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) Alat transformasi string karakter menjadi nilai tetap yang lebih pendek (*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 pengembalian perubahan (*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;

| KABAG HUKUM | KASUBBAG |
| --- | --- |
| | |

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 teknologi informasi dan komunikasi 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 *(review)* 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.

| KABAG HUKUM | KASUBBAG |
| --- | --- |
| | |

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;
   2) perjanjian legalitas kepemilikan piranti lunak (*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, proses penambalan (*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 tambalan (*patch*) sebelum proses instalasi untuk memastikan *patch* dapat bekerja secara efektif dan tidak menimbulkan risiko yang lain. Apabila tambalan (*patch*) tidak tersedia, harus melakukan hal sebagai berikut:
   a. mematikan layanan (*services*) yang berhubungan dengan kerentanan;
   b. menambahkan pengendalian akses seperti sistem keamanan jaringan (*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 teknologi komunikasi dan informasi;
   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 teknologi komunikasi dan informasi;
   6) kelalaian manusia; dan
   7) ketidaksesuaian dengan ketentuan yang berlaku.

b) pegawai dan pihak ketiga harus melaporkan kepada Dinas dan PD sesegera mungkin pada saat menemui kelemahan atau terjadi gangguan keamanan informasi dalam sistem atau layanan teknologi informasi dan komunikasi 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.

| BAG HUKUM | KASUBBAG |
| --- | --- |
| | |

2. pengelolaan gangguan keamanan informasi dan perbaikannya
   a) Dinas dan masing-masing PD 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 dan PD harus mengumpulkan, menyimpan, dan menyajikan bukti pelanggaran terhadap Kebijakan dan Standar Keamanan Informasi di Kabupaten.

j. standar pengendalian keamanan informasi dalam pengelolaan kelangsungan kegiatan

1. PD harus mengelola proses kelangsungan kegiatan pada saat keadaan darurat di masing-masing PD.
2. PD harus mengidentifikasi risiko, dan menganalisis dampak yang diakibatkan pada saat terjadi keadaan darurat untuk menjamin kelangsungan kegiatan.
3. PD harus menyusun dan menerapkan rencana kelangsungan kegiatan untuk menjaga dan mengembalikan kegiatan operasional dalam jangka waktu yang disepakati dan level yang dibutuhkan.
4. PD harus memelihara dan memastikan rencana-rencana yang termuat dalam rencana kelangsungan kegiatan masih sesuai, dan mengidentifikasi prioritas untuk kegiatan uji coba.
5. PD harus melakukan uji coba rencana kelangsungan kegiatan secara berkala untuk memastikan rencana kelangsungan kegiatan dapat dilaksanakan secara efektif.
6. pengelolaan kelangsungan kegiatan pada saat keadaan darurat.
7. 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) PD; dan
   f) pelaksanaan uji coba dan pemeliharaan rencana kelangsungan kegiatan secara berkala.
8. proses identifikasi risiko mengikuti ketentuan mengenai penerapan manajemen risiko di Kabupaten.
9. proses analisis dampak kegiatan harus melibatkan pemilik proses bisnis dan dievaluasi secara berkala.
10. penyusunan rencana kelangsungan kegiatan mencakup:
    a) prosedur saat keadaan darurat, mencakup tindakan yang harus dilakukan serta pengaturan hubungan dengan pihak berwenang;
    b) prosedur komunikasi data yang dapat bernegosiasi ulang jika terjadi kerusakan data atau gangguan jalur komunikasi (*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;

| KABAG HUKUM | KASUBBAG |
| --- | --- |
| | |

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, komunikasi data yang dapat bernegosiasi ulang jika terjadi kerusakan data atau gangguan jalur komunikasi (*fallback*), dan saat kondisi telah normal (*resumption*).

11. uji coba rencana kelangsungan kegiatan harus dilaksanakan untuk memastikan setiap rencana yang disusun dapat dilakukan/dipenuhi pada saat penerapannya.
12. 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 perundangan yang terkait keamanan informasi
    a) Seluruh pegawai dan pihak ketiga harus menaati peraturan perundangan yang terkait dengan keamanan informasi.
    b) Dinas dan PD 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 PD harus mematuhi ketentuan penggunaan lisensi. Penggandaan piranti lunak secara tidak sah tidak diizinkan dan merupakan bentuk pelanggaran.
    d) Perlindungan terhadap rekaman
    Rekaman milik Dinas harus dilindungi dari kehilangan, kerusakan atau penyalahgunaan.
    e) Pengamanan data
    Dinas dan PD melindungi kepemilikan dan kerahasiaan data. Data hanya digunakan untuk kepentingan yang dibenarkan oleh peraturan perundangan dan kesepakatan.

| KABAG HUKUM | KASUBAG |
|---|---|
| | |

2. kepatuhan teknis
   Dinas dan PD 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 PD bersama dengan Inspektorat Kabupaten 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 inforrnasi tidak diizinkan kecuali atas persetujuan Kepala PD.
   c) Proses audit sistem informasi harus memperhatikan hal berikut:
      1) persyaratan audit harus disetujui oleh Kepala PD;
      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 perlu 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;

| KABAG HUKUM | KASUBBAG |
| --- | --- |
| | |

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 harusdiperiksa 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

a. Akun adalah identifikasi pengguna yang diberikan oleh unit pengelola teknologi informasi dan komunikasi, bersifat unik dan digunakan bersamaan dengan kata sandi ketika akan memasuki sistem teknologi informasi dan komunikasi.
b. Akun khusus adalah akun yang diberikan oleh unit pengelola teknologi informasi dan komunikasi sesuai kebutuhan tetapi tidak terbatas pada pengelolaan teknologi informasi dan komunikasi (baik berupa aplikasi atau sistem), dan kelompok kerja (baik berupa acara kedinasan, tim, atau unit kerja).
c. 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.
d. Aset Tidak 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.
e. Pelindung kabel (*Conduit*) adalah sebuah tabung atau saluran untuk melindungi kabel yang biasanya terbuat dari baja.
f. Data adalah catatan atas kumpulan fakta yang mempunyai arti baik secara kualitatif maupun kuantitatif.

| KABAG HUKUM | KASUBBAG |
|---|---|
| | |

g. Serangan terhadap server internet (*Denial of service*) adalah suatu kondisi di mana sistem tidak dapat memberikan layanan secara normal, yang disebabkan oleh suatu proses yang tidak terkendali baik dari dalam maupun dari luar sistem.
h. Direktori adalah hirarki atau hubungan antar direktori dan sub direktori (*tree structure*).
i. 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.
j. Komunikasi data yang dapat bernegosiasi ulang jika terjadi kerusakan data atau gangguan jalur komunikasi (*Fallback*) adalah suatu tindakan pembalikan/menarik diri dari posisi awal.
k. Fasilitas adalah sarana untuk melancarkan pelaksanaan fungsi atau mempermudah sesuatu.
l. Fasilitas Utama adalah sarana utama gedung atau bangunan, seperti pusat kontrol listrik dan televisi sirkuit tertutup (*closes circuit televison*).
m. 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.
n. Jumlah numerik dari satu atau beberapa bidan dalam file (*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.
o. Jejak Audit (*Audit Trails*) adalah urutan kronologis catatan audit yang berkaitan dengan pelaksanaan suatu kegiatan.
p. Kata Sandi adalah serangkaian kode yang dibuat pengguna, bersifat rahasia dan pribadi yang digunakan bersamaan dengan Akun Pengguna.
q. Keamanan Informasi adalah perlindungan aset informasi dari berbagai bentuk ancaman untuk memastikan kelangsungan kegiatan, menjamin kerahasiaan, keutuhan, dan ketersediaan aset informasi.
r. Koneksi Eksternal (*Remote Access*) adalah suatu akses jaringan komunikasi dari luar organisasi ke dalam organisasi.
s. 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.
t. Kode Berbahaya (*Malicious Code*) adalah semua macam program yang membahayakan termasuk makro atau naskah (*script*) yang dapat diesekusi dan dibuat dengan tujuan untuk merusak sistem komputer.
u. Cakram Utama (*Master Disk*) adalah media yang digunakan sebagai sumber dalam melakukan instalasi piranti lunak.

| KABAG HUKUM | KASUBBAG |
| --- | --- |
| | |

v. 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.

w. Pemilik aset informasi adalah unit kerja yang memiliki kewenangan terhadap aset informasi.

x. Perangkat jaringan adalah peralatan jaringan komunikasi data seperti perangkat yang mehubungkan komputer dengan dunia internet (*modem*), piranti jaringan komputer dengan kabel ethernet atau serat optik (*hub*), perangkat jaringan sebagai konektor/penghubung *(switch)*, sebuah alat yang mengirimkan paket data melalui jaringan atau internet menuju tujuannya (*router*), dan lain-lain.

y. Piranti lunak adalah kumpulan beberapa perintah yang dieksekusi oleh mesin komputer dalam menjalankan pekerjaannya.

z. Perangkat pendukung adalah peralatan pendukung untuk menjamin beroperasinya perangkat keras dan perangkat jaringan serta untuk melindunginya dari kerusakan. Contoh perangkat pendukung adalah Suplai daya bebas gangguan (*Uninterruptible Power Supply)* pembangkit tenaga listrik/generator, antena komunikasi.

aa. Perangkat Pengolah Informasi adalah setiap sistem pengolah informasi, layanan atau infrastruktur. Contoh perangkat pengolah informasi adalah komputer, faksimili, telepon, mesin foto copy.

bb. Perjanjian *escrow* adalah perjanjian dengan pihak ketiga atau pembuat aplikasi untuk memastikan apabila pihak ketiga tersebut tidak beroperasi/bangkrut/mengalami kegagalan (*failure)* maka Pemerintah Daerah berhak untuk mendapatkan kode program *(source code).*

cc. 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.

dd. Pihak Berwenang adalah pihak yang mempunyai kewenangan terkait suatu hal, seperti kepolisian, instansi pemadam kebakaran, dan penyedia jasa telekomunikasi/internet.

ee. Pihak Ketiga adalah semua unsur di luar pengguna unit teknologi informasi dan komunikasi 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 kementerian/lembaga lain.

ff. 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.

gg. 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.

| KABAG HUKUM | KASUBBAG |
| --- | --- |
| | |

hh. *Rollback* adalah sebuah mekanisme yang digunakan untuk mengembalikan sistem ke kondisi semula sebelum perubahan diimplementasikan. Mekanisme ini biasanya terdapat pada sistem basis data.

ii. *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.

jj. Sanitasi (*sanitized*) adalah proses pembersihan data dan informasi sehingga tidak ada data dan informasi yang dapat diambil kembali dari perangkat keras tersebut.

kk. 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.

ll. Sistem informasi adalah serangkaian perangkat keras, piranti lunak, sumber daya manusia, serta prosedur dan/atau aturan yang diorganisasikan secara terpadu untuk mengolah data menjadi informasi yang berguna untuk mencapai suatu tujuan.

mm. Sistem Teknologi Informasi dan Komunikasi adalah sistem operasi, sistem surat elektronik, sistem aplikasi, sistem basis data, sistem jaringan intranet/internet, dan sebagainya.

nn. Administrator Sistem (*system administrator*) adalah akun khusus untuk mengelola sistem informasi.

oo. Perangkat Jarak Jauh (*teleworking*) adalah penggunaan teknologi telekomunikasi untuk memungkinkan pegawai bekerja di suatu lokasi yang berada di luar kantor untuk mengakses jaringan internal kantor.

BUPATI GUNUNG MAS,

ttd

ARTON S. DOHONG

**LAMPIRAN II**
**PERATURAN BUPATI GUNUNG MAS**
**NOMOR 7 TAHUN 2019**
**TENTANG**
**STANDARISASI TEKNOLOGI INFORMASI DAN KOMUNIKASI BERBASIS ELEKTRONIK**

## PUSAT DATA (*DATA CENTER*)

(1) TUJUAN

standar ini bertujuan untuk mengatur penyelenggaraan Pusat Data *(Data Center)* di Kabupaten.

(2) RUANG LINGKUP

standar ini berlaku untuk penyelenggaraan Pusat Data *(Data Center)* di Kabupaten yang dilaksanakan secara internal dan/atau menggunakan pihak ketiga.

(3) KEBIJAKAN

a. Kabupaten menyediakan fasilitas berupa Pusat Data (*Data Center*) untuk pengelolaan Elektronik Pemerintahan (*e-Government*).
b. penyelenggara Pusat Data (*Data Center*) Kabupaten dilakukan secara terpusat oleh Dinas.
c. Dinas menyediakan layanan penempatan (*hosting*) portal websitedan aplikasi berbasis *web* kepada setiap PD.
d. Dinas menyediakan layanan pencadangan sistem (*system backup*) untuk aplikasi yang bersifat umum dan aplikasi khusus untuk PD.
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*) sebagaimana dimaksud pada huruf c.
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 Kabupaten dan tidak boleh digunakan di luar Kabupaten tanpa izin dari Kepala Dinas.

(4) TANGGUNG JAWAB

a. pihak-pihak yang terkait dalam penyelenggaraan pusat Data *(Data Center)* terdiri dari:
   1. Pemilik aplikasi adalah Kepala PD atau Pejabat di Kabupaten 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)*;

| KABAG HUKUM | KASUBBAG |
|---|---|
| | |

3. tim penjaminan mutu (*quality assurance*) 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 Kabupaten.

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 cacat desain (*bug*) dan kesalahan penulisan kode program (*error*).
4. melakukan perbaikan aplikasi apabila ditemukan cacat desain (*bug*) dan kesalahan penulisan kode program (*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 Kabupaten;
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 desain teknis dan implementasi;
2. persyaratan operasi;
3. persyaratan keberlangsungan kegiatan.

b. persyaratan desain 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 berdasarkan 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 rendah serta tingkat kelembaban yang rendah.

| KABAG HUKUM | KASUBBAG |
|---|---|
| | |

2. persyaratan bangunan dan arsitektur
   a) 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 yang menghadap ke sinar matahari harus ditutup untuk mencegah paparan panas.
   c) memiliki area bongkar muat yang memadai untuk menangani kegiatan bongkar/muat barang/peralatan.
3. persyaratan kontrol akses dan keamanan
   a) setiap pintu dan jendela yang memungkinkan akses langsung ke Pusat Data *(Data Center)*, diberi pengaman fisik.
   b) Pusat Data *(Data Center)* harus diamankan selama 24 (Dua Puluh Empat) jam dengan paling sedikit 1 (satu) orang petugas per siklus kerja (*shift*).
   c) perangkat sistem pemantau visual (seperti televisi sirkuit tertutup (*closes circuit televison*) 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.
4. peringatan kebakaran, deteksi asap, dan pemadam kebakaran
   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 server, ruang mekanikal dan kelistrikan, ruang telekomunikasi dan ruangan penting lainnya memiliki tingkat terbakar (*fire-rating*) sesuai dengan peraturan perundang-undangan.
   f) ruang komputer harus diproteksi dengan sistem pendeteksi asap. Seluruh sistem deteksi asap bangunan harus diintegrasikan ke dalam 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 perundangan-undangan.
   k) semua tanda peringatan kebakaran harus ditempatkan pada posisinya sesuai ketentuan peraturan perundang-undangan.

| KABAG HUKUM | KASUBBAG |
| --- | --- |
| | |

l) seluruh sistem pendeteksi dan pemadam kebakaran harus didesain dan dipasang oleh berkualifikasi 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 sistem yang menggunakan sprikler otomatis yang disambungkan pada suatu sistem perpipaan yang mengandung udara, baik yang bertekanan atau tidak, melalui suatu sistem deteksi tambahan yang dipasang pada area yang sama dengan sprinkler. (*pre-action*).

n) Jika ruang atau bangunan yang berdekatan dengan lokasi Pusat Data *(Data Center)* tidak memiliki sistem pemadam api otomatis (*sprinkler*), maka resiko kebakaran harus dikaji.

5. Penyediaan Catu Daya

a) kabel daya masuk ke dalam bangunan Pusat Data *(Data Center)* diterminasi di ruang kendali penyambungan listrik yang handal.

b) daya listrik utama paling sedikit 20% (dua puluh persen) lebih besar dari proyeksi beban puncak di mana Pusat Data *(Data Center)* berada.

c) tersedianya catu daya listrik alternatif (seperti generator *standby*) dengan kapasitas yang memadai untuk operasional minimal 3 (tiga) jam selama kejadian gangguan listrik utama.

d) perangkat teknologi informasi dan komunikasi harus diproteksi dengan Suplai daya bebas gangguan (*uninterruptible power supply*) atau catu daya cadangan lainnya.

e) Suplai daya bebas gangguan (*uninterruptible power supply*) atau catu daya cadangan lainnya harus memiliki kapasitas memadai untuk memasok beban teknologi informasi dan komunikasi sampai catu daya alternatif mampu memikul beban perangkat teknologi informasi dan komunikasi menjadi stabil (*steady-state*).

f) Kapasitas Suplai daya bebas gangguan (*uninterruptible power supply*) harus lebih besar dari proyeksi beban puncak perangkat teknologi informasi dan komunikasi. Kapasitas beban rata-rata tidak lebih besar dari 80% (delapan puluh persen) kapasitas Suplai daya bebas gangguan (*uninterruptible power supply*).

g) Suplai daya bebas gangguan (*uninterruptible power supply*) memiliki sistem pelaporan, pemantauan kinerja, dan sistem peringatan.

h) Suplai daya bebas gangguan (*uninterruptible power supply*) 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.

| KABAG HUKUM | KASUBBAG |
| --- | --- |
| | |

6. penyediaan sistem pendingin dan kelembaban
   a) temperatur dan kelembaban ruangan dijaga dan dikendalikan sesuai dengan kebutuhan operasional normal perangkat teknologi informasi dan komunikasi yang paling peka.
   b) Peralatan pengatur temperatur dan kelembaban harus dihubungkan ke catu daya utama (didukung oleh catu daya alternatif).
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 adalah kabel dalam ruangan 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 (dua puluh) cm.
   e) kabel daya tiga fase dan kabel data tembaga harus dipisahkan paling sedikit 60 (enam puluh) 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, dengan data pemilik (jika diperlukan).
   i) setiap rak peralatan memiliki label identifikasi data pemilik (jika diperlukan).
   j) Kabel input telekomunikasi eksternal dihubungkan di area atau ruang telekomunikasi tersendiri.
   k) jika area telekomunikasi terpisah dari ruang Pusat Data *(Data Center)* maka harus memiliki sistem pengatur temperatur, 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.

| KABAG HUKUM | KASUBBAG |
| --- | --- |
| | |

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, Suplai daya bebas gangguan (*uninterruptible power supply*), generator dan lain- lain harus terdapat dalam pencatatan aset:
      1) lokasi;
      2) nomor seri;
      3) data pengadaan;
      4) kontak rinci pabrikan; dan
      5) tanggal kalibrasi jika diperlukan.
   c) konfigurasi dan prosedur operasi harus didokumentasikan termasuk di dalamnya:
      1) perubahan konfigurasi; dan
      2) aturan standar (*set-point default*)
   d) informasi dokumentasi lokasi meliputi:
      1) bangunan dan lantai
      2) lokasi rak dan item utama dari perangkat
      3) denah rak; dan
      4) koneksi fisik dan logik antar peralatan
   e) daftar kontak harus tersedia berisi data dari 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; dan
      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 memiliki kompetensi dalam pemeliharaan Pusat Data *(Data Center)*.
   b) setiap peralatan yang membutuhkan pemeliharaan harus memiliki catatan pemeliharaan yang berisi peralatan, tanggal pemeliharaan, hasil, dan kontak rinci.

d. persyaratan keberlangsungan kegiatan Pusat Data *(Data Center)* paling sedikit harus memenuhi aspek sebagai berikut:
1. manajemen resiko
   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) komunikasi: kerusakan kabel utama.
   b) seluruh perangkat kritis seperti status Suplai daya bebas gangguan (*uninterruptible power supply*), kondisi gangguan, dan lain-lain harus dipantau.

| KABAG HUKUM | KASUBBAG |
| --- | --- |
| | |

2. penanganan insiden
   a) setiap gangguan kritis dan berhentinya layanan harus diinformasikan kepada pengguna Pusat Data *(Data Center)* secepatnya.
   b) setiap gangguan dan berhentinya layanan dapat disampaikan kepada Dinas oleh pengguna Pusat Data *(Data Center)*.
   c) pihak manajemen harus menelaah setiap insiden sebagai berikut:
      a. insiden yang terjadi;
      b. dimana terjadi;
      c. kapan terjadi;
      d. dampak terhadap penyediaan layanan;
      e. bagaimana mengatasinya; dan
      f. 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 teknologi informasi dan komunikasi serta petunjuk tertulis bagaimana proses memulai ulang (*restart*) ditangani.
   e) efek dari terputusnya aliran daya harus disimulasi secara regular untuk membuktikan Suplai daya bebas gangguan (*uninterruptible power supply*) dan menghidupkan (*start-up*) 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 perjanjian/kesepakatan tingkat layanan (*service level agreement*) 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 Kabupaten secara berkesinambungan ketika Pusat Data *(Data Center)* mati/rusak karena bencana.

BUPATI GUNUNG MAS,

ttd

ARTON S. DOHONG

**LAMPIRAN III**
**PERATURAN BUPATI GUNUNG MAS**
**NOMOR 7 TAHUN 2019**
**TENTANG**
**STANDARISASI TEKNOLOGI INFORMASI DAN KOMUNIKASI BERBASIS ELEKTRONIK**

## STANDAR PENGEMBANGAN APLIKASI

(1) TUJUAN

standar ini digunakan sebagai pedoman dalam pengembangan aplikasi di Kabupaten Gunung Mas agar pelaksanaan pengembangan aplikasi efektif dan efisien.

(2) RUANG LINGKUP

standar ini berlaku untuk pengembangan aplikasi di Kabupaten Gunung Mas 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 Kepala PD bertanggung jawab dalam penerapan Kebijakan dan standar pengembangan aplikasi di masing-masing PD;
e. PD harus menerapkan kebijakan dan standar pengembangan aplikasi di masing-masing PD;
f. setiap Kepala PD bertanggung jawab dalam membangun kompetensi pengembangan aplikasi bagi pejabat/staf di masing-masing PD 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. PD harus berkoordinasi dengan Dinas selama proses pengembangan aplikasi sampai dengan operasionalisasi aplikasi;
i. Dinas sebagai pengatur, pembina dan pengawas teknologi informasi dan komunikasi di Kabupaten memiliki kewenangan untuk memastikan bahwa proses pengembangan telah sesuai dengan kebijakan dan standar pengembangan aplikasi;
j. aplikasi yang telah dikembangkan untuk kepentingan Kabupaten dan PD harus ditempatkan di Pusat Data (*Data Center*) Kabupaten yang dikelola oleh Dinas;
k. Aplikasi yang sudah dikembangkan menjadi milik Kabupaten dan tidak boleh digunakan di luar Kabupaten tanpa izin dari pejabat yang berwenang.

| KABAG HUKUM | KASUBBAG |
| --- | --- |
| | |

(4) TANGGUNG JAWAB

a. pihak-pihak yang terkait dalam pengembangan aplikasi terdiri dari:
   1. pemilik proses bisnis adalah Kepala PD atau Pejabat di Kabupaten yang memiliki kebutuhan akan adanya aplikasi untuk mendukung berjalannya tugas dan fungsi;
   2. pengembang aplikasi adalah pegawai pada PD di Kabupaten 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; dan
   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 Uji Penerimaan Pengguna (*User Acceptance Test*);
   3. memastikan bahwa aplikasi yang akan ditempatkan (*hosting*) di Pusat Data (*Data Center*) sudah bebas dari cacat desain (*bug*) dan kesalahan penulisan kode program (*error*);
   4. pemeriksaan laporan Uji Penerimaan Pengguna (*User Acceptance Test*) untuk memastikan keluaran yang dihasilkan oleh pengembang aplikasi sesuai dengan dokumen sebagaimana dimaksud pada angka 1 huruf a;
   5. pemeriksaan dan penandatanganan berita acara analisis hasil pengujian dan juga berita acara hasil tinjauan pasca implementasi aplikasi; dan
   6. memberi masukan kepada pengembang aplikasi terkait pengembangan dan penyempurnaan aplikasi.
   7. 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 Kabupaten;
   2. tindak lanjut masukan dari pemilik proses bisnis terkait pengembangan dan penyempurnaan 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 Uji Penerimaan Pengguna (*User Acceptance Test*) serta pelaporan kepada pemilik proses bisnis; dan
   6. penyusunan dokumentasi yang merupakan keluaran pada semua tahapan pengembangan aplikasi.

| KABAG HUKUM | KASUBBAG |
| --- | --- |
| | |

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 Uji Penerimaan Pengguna (*User Acceptance Test*).
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 Kabupaten;
   4. memastikan bahwa pengembangan aplikasi baik proses maupun produk yang dihasilkan sesuai dengan standar aplikasi yang berlaku di Kabupaten 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 Bupati 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.

| KABAG HUKUM | KASUBBAG |
| --- | --- |
| | |

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);* dan
         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 sebagaimana dimaksud pada huruf b angka 2 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, statsiun kerja (*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);

| KABAG HUKUM | KASUBBAG |
| --- | --- |
| | |

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 sebagaimana dimaksud pada huruf b angka 2 (b) 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 Kabupaten.
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 Kabupaten.
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;

| KABAG HUKUM | KASUBBAG |
| --- | --- |
| | |

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 Kabupaten;

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-langkah 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) uji Penerimaan Pengguna (*User Acceptance Test*).

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) Rencana tindakan (*fall-backplan*) dan/atau Rencana cadangan (*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;

| KABAG HUKUM | KASUBBAG |
|---|---|
| | |

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; dan
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. setiap kegiatan pada pengendalian mutu merupakan tanggung jawab dari tim pengendalian mutu (*quality assurance*) pengembangan aplikasi.
3. menghasilkan keluaran berupa laporan pengendalian mutu.

h. standar keamanan aplikasi yang dikembangkan harus mengacu pada kebijakan dan standar keamanan informasi di Kabupaten.

(6) ISTILAH YANG DIGUNAKAN
a. Rencana Cadangan (*Backup Plan*) adalah rencana pemulihan sistem ke kondisi semula sebelum terjadi permasalahan terkait proses implementasi.
b. Rencana Tindakan (*Fall-backplan*) adalah merupakan rencana alternatif (yang menghilangkan dampak negatif) apabila terjadi kegagalan di dalam implementasi teknologi informasi dan komunikasi.
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.

| KABAG HUKUM | KASUBBAG |
| --- | --- |
| | |

e. Pengembangan Aplikasi Bersama (*Joint Application Development*) adalah pengembangan aplikasi yang dilaksanakan secara bersama-sama oleh pengembang aplikasi di Kabupaten 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. Kriteria Penerimaan *(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 Tinjauan (*overview*) terhadap aplikasi yang memperlihatkan gambaran menyeluruh dari suatu aplikasi.
i. Siklus Pengembangan Aplikasi (*System Development Life Cycle*) 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 Pengembangan Aplikasi Bersama (*Joint Application Development*).
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/lunak 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. uji Penerimaan Pengguna (*User Acceptance Test*) adalah uji penerimaan yang dilakukan dengan persetujuan pemilik proses bisnis dengan menugaskan tim Penguji (*quality assurance*) beserta pengguna. Suatu aplikasi dikatakan dapat diterima apabila telah lulus dari uji Penerimaan Pengguna (*User Acceptance Test*). uji Penerimaan Pengguna (*User Acceptance Test*) terdiri dari uji penerimaan sistem *(systems acceptance testing)*, uji penerimaan contoh (*pilot acceptance test*), uji setiap fase pengembangan (*roll-out*) dan pengujian akhir *(final acceptance test)*.

**BUPATI GUNUNG MAS,**

**ttd**

**ARTON S. DOHONG**