SALINAN

GUBERNUR GORONTALO

PERATURAN GUBERNUR GORONTALO

NOMOR 57 TAHUN 2019

TENTANG

TATA KELOLA SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK PROVINSI GORONTALO

DENGAN RAHMAT TUHAN YANG MAHA ESA

GUBERNUR GORONTALO,

Menimbang :

a. bahwa pengelolaan sistem pemerintahan berbasis elektronik menjadi urusan pemerintahan yang wajib yang tidak berkaitan dengan pelayanan dasar telah ditetapkan dalam Peraturan Daerah Provinsi Gorontalo Nomor 3 Tahun 2016 tentang Penyelenggaraan Pemerintahan Berbasis Teknologi Informasi dan Komunikasi;

b. bahwa untuk mewujudkan tata kelola pemerintahan yang bersih, efektif, transparan, dan akuntabel serta pelayanan publik yang berkualitas dan terpercaya diperlukan tata kelola dan manajemen sistem pemerintahan berbasis elektronik;

c. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b, perlu membentuk Peraturan Gubernur tentang Tata Kelola Sistem Pemerintahan Berbasis Elektronik Provinsi Gorontalo;

Mengingat :

1. Pasal 18 Ayat (6) Undang-Undang Dasar Negara Republik Indonesia Tahun 1945;
2. Undang-Undang Nomor 36 Tahun 1999 tentang Telekomunikasi (Lembaran Negara Republik Indonesia Tahun 1999 Nomor 154, Tambahan Lembaran Negara Republik Indonesia Nomor 4252);
3. Undang-Undang Nomor 38 Tahun 2000 tentang Pembentukan Provinsi Gorontalo (Lembaran Negara Republik Indonesia Tahun 2000 Nomor 258, Tambahan Lembaran Negara Republik Indonesia Nomor 4060);
4. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 4843);

5. Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (Lembaran Negara Republik Indonesia Tahun 2008 Nomor 61, Tambahan Lembaran Negara Republik Indonesia Nomor 4846);
6. Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik (Lembaran Negara Republik Indonesia Tahun 2009 Nomor 112, Tambahan Lembaran Negara Republik Indonesia Nomor 5038);
7. Undang-Undang Nomor 12 Tahun 2011 tentang Pembentukan Peraturan Perundang-undangan (Lembaran Negara Republik Indonesia Tahun 2011 Nomor 82, Tambahan Lembaran Negara Republik Indonesia Nomor 5234);
8. Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 244, Tambahan Lembaran Negara Republik Indonesia Nomor 5587) sebagaimana telah beberapa kali diubah,terakhir dengan Undang-Undang Nomor 9 Tahun 2015 tentang Perubahan Kedua Atas Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2015 Nomor 58, Tambahan Lembaran Negara Republik Indonesia Nomor 5679);
9. Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Tahun 2012 Nomor 189, Tambahan Lembaran Negara Nomor 5348);
11. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (Lembaran Negara Republik Indonesia Tahun 2018 Nomor 182);
12. Peraturan Daerah Provinsi Gorontalo Nomor 3 Tahun 2016 Tentang Penyelenggaraan Pemerintahan Berbasis Teknologi Informasi dan Komunikasi (Lembaran Daerah Provinsi Gorontalo Tahun 2016 Nomor 03, Tambahan Lembaran Daerah Provinsi Gorontalo Nomor 03);

MEMUTUSKAN:

Menetapkan : PERATURAN GUBERNUR TENTANG TATA KELOLA SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK PROVINSI GORONTALO.

BAB I
KETENTUAN UMUM
Pasal 1

Dalam Peraturan Gubernur ini yang dimaksud dengan :

1. Daerah adalah Provinsi Gorontalo.
2. Pemerintahan Daerah adalah penyelenggaraan urusan pemerintahan oleh penerintah daerah dan dewan perwakilan rakyat daerah menurut asas otonomi dan tugas pembantuan dengan prinsip otonomi seluas-luasnya dalam system dan prinsip Negara Kesatuan Republik Indonesia sebagaimana dimaksud dalam Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.
3. Gubernur adalah Gubernur Gorontalo
4. Pemerintah Daerah Kabupaten/Kota adalah Pemerintah Daerah Kabupaten/Kota di Daerah Provinsi
5. Perangkat Daerah adalah Perangkat Daerah Provinsi sebagai unsur pembantu Gubernur dan Dewan Perwakilan Rakyat Daerah dalam penyelenggaraan Urusan Pemerintahan yang menjadi kewenganan Daerah Provinsi
6. Dinas adalah Perangkat Daerah yang menyelenggarakan urusan pemerintahan dibidang Komunikasi Informatika dan Statistik.
7. Kepala Dinas adalah Kepala Dinas Kominukasi, Informatika dan Statistik Provinsi Gorontalo.
8. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada Pengguna SPBE.
9. Tata Kelola SPBE adalah kerangka kerja yang memastikan terlaksananya pengaturan, pengarahan, dan pengendalian dalam penerapan SPBE secara terpadu.
10. Manajemen SPBE adalah serangkaian proses untuk mencapai penerapan SPBE yang efektif, efisien, dan berkesinambungan, serta layanan SPBE yang berkualitas.
11. Layanan SPBE adalah keluaran yang dihasilkan oleh 1 (satu) atau beberapa fungsi aplikasi SPBE dan yang memiliki nilai manfaat.
12. Rencana Induk SPBE Nasional adalah dokumen perencanaan pembangunan SPBE secara nasional untuk jangka waktu 20 (dua puluh) Tahun.
13. Arsitektur SPBE adalah kerangka dasar yang mendeskripsikan integrasi proses bisnis, data dan informasi, infrastruktur SPBE, aplikasi SPBE, dan keamanan SPBE untuk menghasilkan layanan SPBE yang terintegrasi.

14. Arsitektur SPBE Nasional adalah Arsitektur SPBE yang diterapkan secara nasional.
15. Arsitektur SPBE Instansi Pusat adalah Arsitektur SPBE yang diterapkan di instansi pusat.
16. Arsitektur SPBE Pemerintah Daerah adalah Arsitektur SPBE yang diterapkan di pemerintah daerah.
17. Peta Rencana SPBE adalah dokumen yang mendeskripsikan arah dan langkah penyiapan dan pelaksanaan SPBE yang terintegrasi.
18. Peta Rencana SPBE Nasional adalah Peta Rencana SPBE yang diterapkan secara nasional.
19. Peta Rencana SPBE Instansi Pusat adalah Peta Rencana SPBE yang diterapkan di instansi Pusat.
20. Peta Rencana SPBE Pemerintah Daerah adalah Peta Rencana SPBE yang diterapkan di pemerintah daerah.
21. Proses Bisnis adalah sekumpulan kegiatan yang terstruktur dan saling terkait dalam pelaksanaan tugas dan fungsi instansi pusat dan pemerintah daerah masing-masing.
22. Infrastruktur SPBE adalah semua perangkat keras, perangkat lunak, dan fasilitas yang menjadi penunjang utama untuk menjalankan sistem, aplikasi, komunikasi data, pengolahan dan penyimpanan data, perangkat integrasi/penghubung, dan perangkat elektronik lainnya.
23. Infrastruktur SPBE Nasional adalah Infrastruktur SPBE yang terhubung dengan Infrastruktur SPBE instansi pusat dan pemerintah daerah dan digunakan secara bagi pakai oleh instansi pusat dan pemerintah daerah.
24. Infrastruktur SPBE Instansi Pusat dan Pemerintah Daerah adalah Infrastruktur SPBE yang diselenggarakan oleh instansi pusat dan pemerintah daerah masing-masing.
25. Pusat Data atau *Data Center* adalah fasilitas yang digunakan untuk penempatan sistem elektronik dan komponen terkait lainnya untuk keperluan penempatan, penyimpanan dan pengolahan data, dan pemulihan data.
26. Jaringan Intranet adalah jaringan tertutup yang menghubungkan antar simpul jaringan dalam suatu sistem layanan.
27. Sistem Penghubung Layanan adalah perangkat integrasi/penghubung untuk melakukan pertukaran Layanan SPBE.

28. Aplikasi SPBE adalah satu atau sekumpulan program komputer dan prosedur yang dirancang untuk melakukan tugas atau fungsi Layanan SPBE.
29. Aplikasi Umum adalah Aplikasi SPBE yang sama, standar, dan digunakan secara bagi pakai oleh instansi pusat dan/atau pemerintah daerah.
30. Aplikasi Khusus adalah Aplikasi SPBE yang dibangun, dikembangkan, digunakan, dan dikelola oleh instansi pusat atau pemerintah daerah tertentu untuk memenuhi kebutuhan khusus yang bukan kebutuhan instansi pusat dan pemerintah daerah lain.
31. Keamanan SPBE adalah pengendalian keamanan yang terpadu dalam SPBE.
32. Audit Teknologi Informasi dan Komunikasi adalah proses yang sistematis untuk memperoleh dan mengevaluasi bukti secara objektif terhadap aset teknologi informasi dan komunikasi dengan tujuan untuk menetapkan tingkat kesesuaian antara teknologi informasi dan komunikasi dengan kriteria dan/atau standar yang telah ditetapkan.
33. Pengguna SPBE adalah instansi pusat, pemerintah daerah, pegawai Aparatur Sipil Negara, perorangan, masyarakat, pelaku usaha, dan pihak lain yang memanfaatkan Layanan SPBE.
34. Instansi Pusat adalah kementerian, lembaga pemerintah non kementerian, kesekretariatan lembaga negara, kesekretariatan lembaga non struktural, dan lembaga pemerintah lainnya.
35. Tim koordinasi SPBE pemerintah daerah adalah tim yang dibentuk untuk melakukan koordinasi penerapan dan kebijakan SPBE serta memberikan arahan, evaluasi dan monitoring SPBE
36. *Government Chief Information Officer* Pemerintah Provinsi Gorontalo yang selanjutnya disingkat GCIO adalah Kepala Dinas Komunikasi, Informatika dan Statistik Daerah Provinsi Gorontalo
37. Server atau Peladen adalah piranti khusus dalam jaringan komputer yang menjadi tempat bagi semua simpul di dalam jaringan untuk bisa melakukan *resource sharing*
38. Penyediaan Infrastruktur adalah kegiatan yang meliputi pekerjaan konstruksi untuk membangun atau meningkatkan kemampuan infrastruktur dan/atau kegiatan pengelolaan infrastruktur dan/atau pemeliharaan infrastruktur dalam rangka meningkatkan kemanfaatan infrastruktur informatika

39. Integrasi Sistem adalah proses rekayasa teknologi informasi yang berkaitan dengan penggabungan berbagai sub sistem menjadi satu sistem besar.
40. Application Programming Interface untuk selanjutnya disingkat API adalah teknologi yang digunakan untuk memfasilitasi pertukaran informasi atau data antara dua atau lebih aplikasi perangkat lunak.
41. *Network Operation Center* untuk selanjutnya disingkat NOC adalah sebuah lokasi terpusat yang digunakan untuk melakukan pengelolaan dan pengawasan jaringan internet dan intranet Pemerintah Provinsi Gorontalo.
42. Keamanan Informasi adalah suatu kondisi dimana terjaganya aspek kerahasiaan, integritas dan ketersediaan dari informasi.
43. *Bandwidth* adalah besaran yang menunjukkan seberapa banyak data yang dapat dilewatkan dalam koneksi melalui sebuah jaringan.
44. Hosting adalah tempat penitipan/penyewaan untuk menampung data-data yang diperlukan oleh sebuah website sehingga dapat diakses lewat Internet.
45. *Colocation Server* adalah tempat yang menyediakan layanan untuk menyimpan atau menitipkan server di Data Center yang memiliki standar keamanan fisik dan infrastuktur;
46. Data Center adalah suatu fasilitas yang digunakan untuk menempatkan sistem komputer dan komponen-komponen terkaitnya, seperti sistem telekomunikasi dan penyimpanan data.
47. *Disaster Recovery Center* yang selanjutnya disingkat DRC adalah fasilitas pengganti pada saat Pusat Data (Data Center) mengalami gangguan atau tidak dapat, yang digunakan sementara waktu selama dilakukannya pemulihan pada Pusat Data.
48. *Service Level Agreement* yang selanjutnya disingkat SLA adalah kesepakatan perjanjian layanan antara dua kelompok.
49. *System Development Life Cycle* yang selanjutnya disingkat SDLC adalah model dan metodologi yang digunakan untuk mengembangkan sistem peragkat lunak.
50. Infrastruktur TIK adalah infrastruktur mencakup perangkat keras pemrosesan informasi (*server, workstation, dan peripheral*), jaringan komunikasi dan software infrastruktur (sistem operasi, tool sistem).

51. *Government Service Bus* adalah layanan infrastruktur integrasi data antar aplikasi Pemerintah Daerah Provinsi Gorontalo yang selanjutnya disebut GSB;
52. *User Interface* adalah tampilan muka pada aplikasi yang memudahkan penggunaanya untuk berinteraksi
53. E-mail resmi adalah email yang digunakan dalam aktivitas kegiatan kedinasan di lingkup Pemerintah Daerah Provinsi Gorontalo yaitu mail.gorontaloprov.go.id
54. *Source Code* yang selanjutnya disebut Kode Sumber/Kode Program adalah komponen dasar dari suatu program komputer atau aplikasi
55. *White List* atau daftar putih adalah sebuah daftar yang berisi situs, aplikasi dan port yang boleh diakses dalam jaringan. Daftar putih dapat bersifat statik atau dinamik (menyesuaikan dengan jam kerja)
56. Domain adalah nama unik yang diberikan untuk mengidentifikasikan alamat IP address server komputer seperti situs, aplikasi maupun host jaringan
57. IP Address adalah alamat atau identitas numerik yang diberikan kepada sebuah perangkat komputer agar komputer tersebut teridentifikasi dan dapat berkomunikasi dengan komputer lain
58. Media sosial adalah media berbasis internet yang bersifat dua arah (Web 2.0) dan terbuka bagi siapa saja, yang memungkinkan para penggunaanya dengan mudah berinteraksi, berpartisipasi, berdiskusi, berkolaborasi, berbagi, serta menciptakan dan berbagi isi.
59. *Aplication Programing Interface* yang selanjutnya disingkat API adalah sekumpulan perintah, fungsi, serta protokol yang dapat digunakan oleh pembuat/pengembang saat membangun perangkat lunak untuk sistem operasi tertentu dan memungkinkan pembuat/pengembang menggunakan fungsi standar untuk berinteraksi dengan system operasi.

Pasal 2

(1) Maksud tata kelola sistem pemerintahan berbasis elektronik adalah untuk menjamin integrasi dan sinkronisasi TIK di lingkungan Pemerintah Daerah.

(2) Tujuan pengaturan tata kelola SPBE adalah :

a. mewujudkan pengelolaan SPBE berbasis Rencana Induk SPBE;

b. mewujudkan keselaran antara pengelolaan SPBE di dinas dan perangkat daerah;dan
c. mewujudkan sinkronisasi dan integrasi pengelolaan SPBE.

Pasal 3

Peraturan Gubernur ini menjadi pedoman perangkat daerah dalam pelaksanaan pengelolaan SPBE.

Pasal 4

Ruang Lingkup Peraturan Gubernur ini meliputi :
a. entitas tata kelola SPBE;
b. perencanaan SPBE;
c. manajemen belanja SPBE;
d. pembangunan sistem teknologi informasi dan komunikasi;
e. pembangunan dan pengembangan aplikasi serta standar interoperabilitas;
f. manajemen pusat data;
g. keamanan informasi;
h. pengelolaan email dan domain;
i. operasionalisasi sistem elektronik;
j. mekanisme dan tatacara penetapan standarisasi penyelenggaraan komunikasi dan diseminasi informasi;dan
k. pembinaan dan pengawasan.

BAB I

ENTITAS TATA KELOLA SPBE

Pasal 5

(1) Gubernur menetapkan entitas struktur tata kelola SPBE terdiri atas :
a. Tim koordinasi SPBE;dan
b. GCIO
(2) Tim Kooordinasi SPBE sebagaimana dimaksud pada ayat 1 huruf a melakukan koordinasi dan kebijakan SPBE di pemerintah daerah dengan tugas-tugas sebagai berikut:
a. memfasilitasi proses koordinasi, kerjasama, atau integrasi penerapan SPBE dengan Instansi Pusat/Pemerintah Daerah lain;
b. melakukan evaluasi secara berkala terkait penerapan kebijakan internal Tim Pengarah SPBE;dan

c. memfasilitasi penyempurnaan kebijakan internal Tim Pengarah SPBE sebagai akibat terjadinya perubahan peraturan, perkembangan teknologi, dan/atau kebutuhan Instansi Pusat/Pemerintah Daerah.

(3) Tim Koordinasi SPBE terdiri dari:

a. Sekretaris Daerah dengan tugas yaitu
   1) mengkoordinasikan penerapan kebijakan SPBE di Pemerintah Daerah Provinsi;
   2) mengkoordinasikan layanan SPBE;dan
   3) mengkoordinasikan SPBE dengan instansi pusat dan pemerintah daerah lain

b. Organisasi dan Tata Laksana dengan tugas yaitu
   1) mengkoordinasikan integrasi proses bisnis di K/L/D;
   2) mengelola arsitektur bisnis;dan
   3) mengelola layanan SPBE

c. Badan Keuangan dengan tugas yaitu Mengkoordinasikan penganggaran SPBE

d. Tim Pengarah yaitu memberikan rekomendasi arah pembangunan TIK dengan tugas sebagai berikut:
   1) menyusun rencana kerja tahunan beserta target capaiannya sesuai visi misi organisasi;
   2) melakukan pemantauan dan pengawasan inisiatif SPBE;
   3) melakukan evaluasi inisiatif SPBE;
   4) melakukan koordinasi implementasi SPBE dengan tim koordinasi SPBE Nasional/Instansi Pemerintah lainnya, maupun dengan pihak eksternal dalam dan/atau luar negeri;dan
   5) pemetaan RACI Chart telah dilakukan terhadap tugas dan fungsi sesuai struktur Tim Pengarah yang telah ditetapkan.

e. Dinas dengan tugas yaitu TIK
   1) mengelola Arsitektur SPBE;
   2) mengkoordinasikan pembangunan aplikasi dan infrastruktur TIK;
   3) menerapkan keamanan SPBE;
   4) melaksanakan manajemen aset TIK dan Layanan;dan
   5) mengkoordinasikan tata kelola data dan manajemen data;

e. Badan Perencanaan dengan tugas yaitu menkgoodinasikan perencanaan SPBE.

f. Perangkat Daerah
   1) menyampaikan kebutuhan layanan SPBE di K/L/D;dan
   2) mengelola kebutuhan layanan SPBE

(4) GCIO sebagaimana dimaksud pada ayat 1 huruf b adalah pimpinan dinas yang bertanggung jawab atas perencanaan, penyelarasan, penyiapan, implementasi dan evaluasi SPBE di Daerah Pemerintah Provinsi dan memiliki tugas dan wewenang sebagai berikut:

a. mengkoordinasikan perencanaan, pelaksanaan, dan pemantauan investasi TIK yang strategis di pemerintah daerah provinsi;
b. mengkoordinasikan penyusunan dan pemutakhiran rencana Arsitektur SPBE agar selaras dengan rencana strategis Pemerintah Daerah;
c. mengkoordinasikan perencanaan dan pelaksanaan perumusan kebijakan, standar, dan prosedur TIK di Pemerintah Daerah Provinsi Gorontalo ;
d. mengkoordinasikan perencanaan dan pelaksanaan pengembangan arsitektur SPBE;
e. mengajukan rancangan kebijakan dan standar TIK Perintah Daerah Provinsi Gorontalo kepada Kepala Daerah melalui Sekretaris Daerah untuk ditetapkan;
f. menetapkan keputusan terkait dengan penyelenggaraan tata kelola TIK;
g. melakukan pemantauan dan evaluasi operasional layanan TIK Pemerintah Provinsi Gorontalo;
h. melakukan pemantauan dan evaluasi penerapan kebijakan, standar, dan prosedur TIK di lingkungan Pemerintah Provinsi Gorontalo; dan
i. menyatakan kondisi bencana terkait dengan kelangsungan layanan TIK di lingkungan Pemerintah Daerah Provinsi Gorontalo.

(5) Tim Koordinasi SPBE sebagaimana dimaksud pada Ayat (1) huruf a ditetapkan dengan Keputusan Gubernur.

BAB II
PERENCANAAN SPBE
Bagian Kesatu
Rencana Induk SPBE
Pasal 6

(1) Gubernur menetapkan Rencana Induk SPBE Pemerintah Daerah Provinsi untuk jangka waktu 5 Tahun.

(2) Rencana Induk SPBE sebagaimana dimaksud pada Ayat (1) paling sedikit memuat
   a. visi, misi dan tujuan sasaran TIK SPBE;
   b. arsitektur SPBE;
   c. peta jalan SPBE;dan
   d. rencana anggaran SPBE.
(3) Penyusunan Rencana Induk SPBE sebagaimana dimaksud pada ayat 2 mengacu pada RJPMD Provinsi dan Rencana Pembangunan Jangka Menengah Provinsi dan grand desain reformasi birokrasi Daerah Provinsi
(4) Rencana Induk sebagaimana dimaksud pada ayat 2 menjadi acuan dalam penyusunan program kerja implementasi SPBE diseluruh perangkat daerah.
(5) Rencana Induk SPBE dilakukan peninjauan kembali setiap lima tahun atau sewaktu waktu berdasarkan :
   a. hasil pemantauan dan evaluasi pelaksanaan Rencana Induk;
   b. perubahan kebijakan strategis daerah;
   c. perkembangan teknologi;
   d. perubahan peta Rencana Induk SPBE nasional;dan/atau
   e. perubahan ketentuan perundang-undangan.
(6) Ketentuan lebih lanjut mengenai Rencana Induk sebagaimana dimaksud pada Ayat (2) diatur dengan Peraturan Gubernur.

Pasal 7

Dinas melaksanakan penyusunan Rencana Induk sebagaimana dimaksud dalam pada Pasal 6

Pasal 8

(1) Perubahan Rencana Induk SPBE dapat dilakukan atas usulan perangkat daerah berdasarkan pertimbangan sebagaimana dimaksud pada pasal 6 ayat 6
(2) Ketentuan lebih lanjut mengenai tata cara perubahan Rencana Induk SPBE sebagaimana dimaksud pada Ayat (1) diatur dengan Peraturan Gubernur.

Bagian Kedua

Arsitektur SPBE

Pasal 9

(1) Arsitektur SPBE bertujuan memberikan panduan dalam pelaksanaan integrasi proses bisnis, data dan informasi,

infrastruktur SPBE dan keamanan SPBE untuk menghasilkan layanan SPBE yang terpadu, yang memuat :

a. referensi arsitektur;dan
b. domain arsitektur.

(2) Domain arsitektur sebagaimana dimaksud pada Ayat (1) huruf b mendeskripsikan substansi arsitektur yang memuat :

a. domain arsitektur proses bisnis;
b. domain arsitektur data dan informasi;
c. domain arsitektur infrastruktur SPBE;
d. domain arsitektur aplikasi SPBE;
e. domain arsitektur keamanan SPBE;dan
f. domain arsitektur layanan SPBE.

(3) Arsitektur SPBE Pemerintah Provinsi Gorontalo disusun dengan berpedoman pada arsitektur SPBE Nasional dan RPJMD.

(4) Arsitektur SPBE Pemerintah Provinsi Gorontalo disusun untuk jangka waktu 5 (lima) tahun.

(5) Arsitektur SPBE Pemerintah Provinsi Gorontalo dapat dilakukan peninjauan kembali pada paruh waktu dan tahun berakhir pelaksanaan atau sewaktu-waktu sesuai dengan kebutuhan.

(6) Peninjauan kembali Arsitektur SPBE Pemerintah Daerah sebagaimana dimaksud pada ayat (4) dilakukan berdasarkan:

a. perubahan Arsitektur SPBE Nasional;
b. hasil pemantauan dan evaluasi SPBE di Pemerintah Daerah;
c. perubahan pada unsur SPBE Pemerintah Daerah;dan
d. perubahan Rencana Pembangunan Jangka Menengah Daerah.

(7) Reviu Arsitektur SPBE Pemerintah Daerah sebagaimana dimaksud pada ayat (4) dilakukan oleh kepala daerah.

(8) Ketentuan lebih lanjut mengenai Arsitektur SPBE Pemerintah Provinsi Gorontalo sebagaimana dimaksud pada Ayat (1) diatur dengan Peraturan Gubernur

Bagian Ketiga

Peta Rencana SPBE

Pasal 10

(1) Peta rencana SPBE disusun dalam bentuk program dan kegiatan dan memuat :

a. tata kelola SPBE
b. manajemen SPBE
c. layanan SPBE

d. infrastruktur SPBE
e. aplikasi SPBE
f. keamanan SPBE
g. audit teknologi informasi dan komunikasi

(2) Peta rencana SPBE sebagaimana dimaksud pada Ayat (1) disusun untuk jangka waktu 5 Tahun dan berpedoman pada peta rencana SPBE nasional, arsitektur SPBE, RJPMD serta rencana strategis pemerintah daerah.
(3) Peta rencana SPBE ditetapkan oleh Gubernur
(4) Peta rencana SPBE dapat dilakukan peninjauan kembali pada paruh waktu dan tahun terakhir pelaksanaan atau sewaktu-waktu sesuai dengan kebutuhan.
(5) Peninjauan kembali peta rencana SPBE sebagaimana dimaksud pada Ayat (4) dilakukan oleh Dinas berdasarkan:
a. perubahan peta rencana SPBE nasional;
b. perubahan rencana strategis Pemerintah Daerah;
c. perubahan arsitektur SPBE; dan/atau
d. hasil pemantauan dan evaluasi SPBE
(6) Ketentuan lebih lanjut mengenai Peta Rencana SPBE sebagaimana dimaksud Pada Ayat (1) diatur dengan Peraturan Gubernur.

BAB III
MANAJEMEN BELANJA SPBE
Bagian Kesatu
Umum
Pasal 11

(1) Manajemen belanja SPBE pemerintah daerah provinsi berpedoman pada Rencana Induk SPBE.
(2) Rencana dan anggaran belanja SPBE harus disusun berdasarkan Arsitektur SPBE dan Peta Rencana SBPE.
(3) Pengelolaan anggaran untuk keperluan belanja SPBE dilakukan melalui mekanisme penganggaran tahunan.

Pasal 12

(1) Belanja SPBE mencakup belanja infrastruktur SPBE, aplikasi serta peningkatan kuantitas dan kualitas SPBE.
(2) Dinas menyusun standar biaya umum dan standar biaya khusus untuk belanja SPBE dan ditetapkan dengan Keputusan Gubernur.

Bagian Kedua

Penganggaran dan Pembelanjaan

Pasal 13

Penganggaran belanja SPBE pada perangkat daerah dikoordinasikan oleh Perangkat Daerah yang melaksanakan fungsi penunjang perencanaan pembangunan daerah

Pasal 14

(1) Perangkat Daerah mengusulkan penganggaran belanja SPBE kepada Perangkat Daerah yang melaksanakan fungsi penunjang perencanaan pembangunan daerah
(2) Perangkat daerah yang melaksanakan fungsi penunjang perencanaan pembangunan daerah bersama-sama Dinas melakukan verifikasi dan persetujuan terhadap usulan penganggaran belanja SPBE sebagaimana dimaksud pada Ayat (1) untuk memastikan tidak adanya duplikasi anggaran dengan perangkat daerah lainnya

Pasal 15

Belanja infrastruktur intra Pemerintah Daerah, internet, intranet dan pembangunan/pengembangan aplikasi yang sifatnya umum atau lintas Perangkat Daerah (integrasi) dilakukan oleh Dinas.

BAB IV

PEMBANGUNAN SISTEM TEKNOLOGI INFORMASI DAN KOMUNIKASI

Bagian Kesatu

Umum

Pasal 16

(1) Pemerintah Daerah Provinsi melakukan pembangunan sistem TIK untuk mengimplementasikan perencanaan SPBE, mulai dari pemilihan sistem TIK sampai dengan evaluasi pasca implementasi
(2) Pembangunan sistem TIK sebagaimana dimaksud pada Ayat (1), meliputi :
    a. identifikasi dan pemilihan sistem;
    b. pembangunan sistem elektronik;
    c. pembangunan infrastruktur TIK;
    d. keamanan sistem TIK; dan
    e. perancangan data dan informasi.

Bagian Kedua

Pembangunan Infrastruktur Teknologi Informasi dan Komunikasi

Pasal 17

(1) Dinas melaksanakan pembangunan dan pengelolaan infrastruktur TIK, meliputi :
   a. data center Pemerintah Provinsi Gorontalo;
   b. jaringan internet dan intranet dari NOC pemerintah daerah provinsi kepada perangkat daerah; dan
   c. *disaster recovery plan.*

(2) Dinas melakukan standarisasi infrastruktur TIK untuk seluruh perangkat daerah, meliputi:
   a. standarisasi perangkat aktif jaringan;
   b. standarisasi manajemen jaringan;
   c. standarisasi ruang perangkat aktif jaringan lokal;dan
   d. standarisasi peladen dan perangkat pendukung

(3) Pembangunan infrastruktur TIK yang dilakukan oleh perangkat daerah hanya mencakup pengadaan ruang perangkat aktif jaringan.

(4) Setiap perangkat dan pengguna yang terhubung dan atau menggunakan jaringan lokal terintegrasi wajib didaftarkan ke Dinas dan wajib menggunakan alamat protokol internet yang dikeluarkan oleh Dinas.

(5) Pendaftaran perangkat dan pengguna sebagaimana dimaksud pada Ayat (4) yaitu dengan menggunakan sistem masuk terpusat (*single sign on*).

Bagian Ketiga

Manajemen Infrastruktur Komunikasi Data

Pasal 18

(1) Dinas menyediakan jaringan internet dan intranet bagi seluruh perangkat daerah dan unit pelaksana teknis dibawahnya.

(2) Jaringan internet dan intranet yang disediakan oleh dinas sebagaimana dimaksud pada Ayat 1 disebut dengan Jaringan *Moawota* Provinsi Gorontalo.

(3) *Bandwith* yang disediakan oleh Dinas minimal 1 setengah kali dari total kebutuhan data center dan perangkat daerah.

(4) Pengguna jaringan *moawota* dalam menggunakan akses Internet dan Intranet bertanggung jawab untuk :

a. menggunakan fasilitas akses Intranet dan Internet secara bijak sesuai dengan tugas, fungsi, dan wewenang;
b. menggunakan fasilitas akses Intranet dan Internet sesuai norma hukum dan etika yang berlaku; dan
c. melaporkan kepada Dinas jika terjadi gangguan pada fasilitas akses Intranet dan Internet.

(5) Pengguna jaringan *moawota* dalam menggunakan akses internet dan intranet dilarang untuk :
a. menyampaikan pendapat pribadi ke pihak lain dengan mengatasnamakan Pemerintah Daerah Provinsi atau Perangkat Daerah melalui fasilitas akses Intranet atau Internet;
b. menyampaikan pendapat yang bermuatan ujaran kebencian terhadap Pancasila, Undang-Undang Dasar Negara Republik Indonesia Tahun 1945, Bhinneka Tunggal Ika, Negara Kesatuan Republik Indonesia (NKRI), Pemerintah, dan Suku, Agama, Ras, dan Antar golongan (SARA) melalui fasilitas akses Intranet atau Internet;
c. mengirimkan dan/atau mempublikasikan konten yang berisi ancaman penghinaan atau pencemaran nama baik terhadap sesama pegawai, pimpinan, mitra, dan/atau pihak lain melalui fasilitas akses Intranet atau Internet;
d. menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian bagi individu maupun Pemerintah Daerah Provinsi melalui fasilitas akses Intranet atau Internet;
e. menggunakan perangkat lunak yang dapat mengelabui sistem pengendalian/pembatasan akses Internet;
f. melakukan kegiatan yang dapat menimbulkan gangguan terhadap Sistem TIK Unit di Lingkungan Pemerintah Daerah Provinsi antara lain menggunakan *tunneling tools*, mengakses laman yang berpotensi mengandung virus, mengakses video *streaming* yang membutuhkan *bandwidth* besar;
g. mengunggah, mengunduh, dan/atau menjalankan perangkat lunak berlisensi milik Pemerintah Daerah Provinsi untuk keperluan di luar kedinasan;

h. mengakses, mengunggah, mengunduh, dan/atau mempublikasikan situs-situs yang tidak menunjang kedinasan;
i. menggunakan hak atas kekayaan intelektual pihak lain secara tidak sah melalui fasilitas akses Internet atau Internet;
j. melakukan kegiatan yang dapat merusak/mencoreng nama baik individu maupun Pemerintah Daerah Provinsi melalui fasilitas akses Intranet atau Internet;
k. mengungkapkan atau menyebarkan aset informasi milik Pemerintah Daerah Provinsi yang termasuk informasi yang dikecualikan sesuai peraturan perundang-undangan yang berlaku melalui fasilitas akses Intranet atau Internet; dan
l. melakukan kegiatan yang melanggar hukum dan peraturan perundang-undangan yang berlaku melalui fasilitas akses Intranet atau Internet.

(6) Penyediaan jaringan internet dan intranet sebagaimana dimaksud pada Ayat (1), dilakukan dengan cara:
a. melakukan analisis kebutuhan bandwidth pemerintah daerah;
b. mengatur pembagian *bandwidth* ke perangkat daerah sesuai dengan analisis kebutuhan *bandwidth*;
c. mendistribusi akses internet dengan sistem whitelist, yaitu distribusi bebas namun melakukan pembatasan akses terhadap situs, port dan aplikasi;dan
d. melakukan pengawasan dan pengendalian penggunaan *bandwidth* pemerintah daerah secara rutin, berkala dan periodic.

(7) Perangkat daerah tidak dapat menyewa/membeli *bandwidth* ke pihak ketiga secara mandiri.

(8) Institusi pemerintah formal maupun non formal lainnya dapat memperoleh bantuan *bandwidth* dan *hosting* dengan persetujuan Kepala Dinas.

(9) Segala pembiayaan yang timbul dari perangkat bagi penyediaan *bandwidth* menjadi tanggungjawab institusi pemohon.

(10) Dalam rangka penyebarluasan informasi, Dinas dapat menyediakan perangkat dan *bandwidth* secara gratis kepada masyarakat pada tempat-tempat publik.

(11) Penyediaan perangkat dan *bandwidth* sebagaimana dimaksud pada Ayat (10) dilakukan dengan syarat:

a. tempat publik yang ditetapkan melalui Keputusan Gubernur;
b. *bandwidth* yang didistribusi tidak mengganggu kebutuhan *bandwidth* Perangkat Daerah dan Data Cente;
c. masyarakat pengakses wajib mendaftarkan diri dengan menggunakan NIK;
d. akses internet dengan sistem *whitelist;*dan
e. melakukan pengawasan dan pengendalian penggunaan bandwidth secara rutin, berkala dan periodik.

Pasal 19

Dinas wajib menjaga keberlangsungan jaringan internet dan intranet *moawota* pendukung administrasi perkantoran pemerintah daerah provinsi.

Bagian Keempat

Identifikasi dan Pemilihan Sistem

Pasal 20

(1) Perangkat daerah melakukan identifikasi pemilihan sistem TIK dengan mempertimbangkan :
a. capaian program;
b. kebutuhan program;
c. keluaran program; dan
d. kerangka acuan kerja.
(2) Identifikasi pemilihan sistem TIK sebagaimana dimaksud pada Ayat (1), dituangkan dalam bentuk dokumen yang memuat :
a. analisis kebutuhan; dan
b. analisis manfaat dari pemilihan sistem yang direncanakan.

Pasal 21

(1) Berdasarkan hasil identifikasi sebagaimana dimaksud dalam Pasal 20, perangkat daerah mengajukan permohonan pemilihan sistem kepada Dinas
(2) Dinas melakukan persetujuan atau penolakan terhadap pengajuan sebagaimana dimaksud pada Ayat (1) berdasarkan hasil analisis yang mengacu kepada Rencana Induk SPBE
(3) Dalam hal permohonan pemilihan sistem disetujui, dinas melampirkan dokumen sebagaimana dimaksud dalam Pasal 20 Ayat (2) dan dokumen analisis beban biaya sebagai bahan pengajuan penganggaran belanja SPBE

(4) Dalam hal pemilihan sistem ditolak, Perangkat Daerah melakukan penyesuaian atas pemilihan sistem sesuai saran Dinas dan mengajukan permohonan pemilihan sistem kembali

BAB V
PEMBANGUNAN DAN PENGEMBANGAN APLIKASI SERTA STANDAR INTEROPERABILITAS

Bagian Kesatu
Pembangunan dan Pengembangan Aplikasi

Pasal 22

(1) Pembangunan aplikasi meliputi :
   a. aplikasi umum; dan
   b. aplikasi khusus

(2) Pembangunan dan /atau pengembangan aplikasi umum ditujukan untuk memberikan Layanan SPBE yang mendukung kegiatan pemerintahan di bidang:
   a. perencanaan;
   b. penganggaran;
   c. pengadaan barang dan jasa pemerintah;
   d. akuntabilitas kinerja;
   e. pemantauan dan evaluasi;
   f. kearsipan;
   g. kepegawaian; dan
   h. pengaduan pelayanan publik.

(3) Perangkat daerah tidak diperkenankan membangun dan mengembangkan aplikasi sejenis dengan aplikasi umum sebagaimana dimaksud pada ayat 2

(4) Dalam hal perangkat daerah menggunakan aplikasi sejenis sebagaiamana dimaksud pada Ayat (2) perangkat daerah harus memenuhi persyaratan sebagai berikut :
   a. telah mengoperasikan aplikasi sejenis sebelum aplikasi umum ditetapkan;
   b. melakukan kajian biaya dan manfaat terhadap penggunaan dan manfaat aplikasi sejenis;
   c. melakukan pengembangan aplikasi sejenis yang disesuaikan dengan proses bisnis dan fungsi pada aplikasi umum; dan
   d. mendapatkan pertimbangan dari menteri yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika.

(5) Perangkat Daerah dapat melakukan pembangunan dan pengembangan aplikasi khusus yang didasarkan pada arsitektur SPBE Pemerintah Provinsi Gorontalo

(6) Sebelum melakukan pembangunan dan pengembangan aplikasi khusus sebagaimana dimaksud pada Ayat (5), Perangkat Daerah harus melakukan asistensi ke Dinas untuk mendapatkan pertimbangan dari kementerian yang menyelenggarakan urusan pemerintahan di bidang aparatur negara

(7) Pengembangan aplikasi khusus harus mengikuti standar-standar teknis dan prosedur pembangunan dan pengembangan aplikasi khusus.

(8) Standar teknis dan prosedur sebagaimana dimaksud pada Ayat (7) berlaku sampai dengan diterbitkannya standar dan prosedur yang diatur dengan Peraturan Menteri yang menyelenggarakan urusan pemerintahan di bidang Komunikasi dan Informatika,

(9) Dalam hal pembangunan dan pengembangan aplikasi, diutamakan harus menggunakan aplikasi kode sumber terbuka (*opensource*), jika tidak maka pembangunan aplikasi harus ada pertimbangan dari menteri yang menyelenggarakan urusan pemerintahan dibidang Komunikasi dan Informatika

(10) Aplikasi khusus dan kode sumbernya sebagaimana dimaksud pada Ayat (9) didaftarkan dan disimpan pada repository aplikasi SPBE Nasional dan/atau repository yang dikelola oleh Dinas.

(11) Aplikasi yang disimpan pada repository aplikasi SPBE Nasional dilakukan oleh Dinas.

(12) Pembangunan dan pengembangan aplikasi khusus dapat dilakukan oleh Perangkat Daerah melalui swakelola sesuai ketentuan peraturan perundang-undangan.

(13) Pembangunan dan pengembangan aplikasi khusus Perangkat Daerah dapat dilakukan dan dibebankan kepada Dinas

(14) Usulan Pembangunan dan pengembangan aplikasi sebagaimana dimaksud pada Ayat (13) diterima oleh Dinas paling lambat 6 bulan sebelum penetapan anggaran dan/atau peluncuran aplikasi ke publik.

(15) Pembangunan dan pengembangan aplikasi yang diusulkan telah harus memiliki payung hukum yang mengikat

(16) Usulan aplikasi ke Dinas ditujukan ke Sekretaris Daerah dilengkapi dengan dokumen proses bisnis aplikasi dan dokumen lain yang akan ditetapkan melalui Keputusan Gubernur.

(17) Pengembangan dan pembangunan aplikasi tercantum dalam Lampiran I Peraturan Gubernur ini.

Pasal 23

Kegiatan analisis kebutuhan aplikasi terdiri atas ;

a. mengidentifikasi spesifikasi kebutuhan aplikasi yang meliputi keluaran (*output*), kinerja, keamanan, dan kebutuhan spesifik lainnya;
b. mengidentifikasi dan menganalisa resiko;
c. merancang prosedur mitigasi dan rehabilitasi (pemulihan);dan
d. membuat rangkuman/ikhtisar aplikasi yang akan dikembangkan, dan membuat analisis kesenjangan (*gap analysis*) jika aplikasi yang akan dikembangkan adalah pengembangan dari aplikasi yang sudah ada.

Pasal 24

(1) Pembangunan aplikasi sebagaimana dimaksud Dalam Pasal 22 Ayat (5) dilakukan berdasarkan metodologi *System Development Life Cycle* (SDLC).
(2) Metodologi *System Development* sebagaimana dimaksud pada Ayat (1), paling sedikit mencakup kebutuhan:
    a. penerjemah kebutuhan/persyaratan bisnis ke dalam spesifikasi desain;
    b. penyusunan desain detail dan teknikal aplikasi, termasuk pengendalian aplikasi/*application control* yang memungkinkan setiap pemrosesan dalam peranti lunak akurat, lengkap, tepat waktu terotorisasi dan dapat diaudit dan pengendalian keamanan aplikasi (*application security control*) yang memungkinkan terpenuhinya aspek kerahasiaan (*confidentiality*), ketersediaan (*avaliability*), dan integritas (*integrity*);
    c. implementasi desain detail dan teknikal kedalam kode program sumber (*coding*);
    d. mempersiapkan desain integritas dan interoperabilitas sistem
    e. mempersiapkan dan menjamin keamanan sistem dan informasi dan aplikasi;
    f. manajemen perubahan persyaratan/kebutuhan;
    g. melaksanakan penjamin mutu (*quality assurance*);

h. melaksanakan uji coba (*testing*), meliputi :
   1) *Unit testing*;
   2) *Penetration testing*;
   3) *System testing*;
   4) *Integration testing*;
   5) *User Acceptance Test* (UAT);dan
   6) Instalasi dan akreditasi.

Bagian Kedua

Manajemen Aplikasi

Pasal 25

(1) Setiap pengoperasian aplikasi harus mengikuti standar teknis dan pengembangan sistem informasi yang ditetapkan oleh Kementrian Komunikasi dan Informatika.
(2) Setiap perangkat lunak harus selalu menyertakan prosedur *backup* dan *restore*, dan juga mengimplementasikan fungsionalitasnya di dalam *software* aplikasi
(3) Setiap kode sumber peranti lunak harus disimpan pada *repository* aplikasi SPBE yang dikelola oleh Dinas.
(4) Setiap aplikasi yang akan menggunakan meta data dan terhubung dengan aplikasi lain harus menyediakan dan atau membuka akses API
(5) API sebagaimana dimaksud ayat (4) diawasi penggunaannya oleh Dinas
(6) Perangkat Daerah yang memiliki aplikasi harus secara berkala melakukan backup mandiri terhadap aplikasinya
(7) Setiap pengoperasian aplikasi harus disertai oleh dokumentasi berikut ini:
   a. dokumentasi hasil aktivitas tahapan-tahapan dalam SDLC;
   b. dokumentasi penggunaan API
   c. manual pengguna, operasi, dukungan teknis dan administrasi; dan
   d. materi transfer pengetahuan dan materi training.

Pasal 26

(1) Perangkat daerah melaksanakan pengelolaan aplikasi TIK dengan mengacu pada standar pengelolaan aplikasi yang disusun dan ditetapkan oleh Dinas
(2) Pengelolaan aplikasi TIK sebagaimana dimaksud pada Ayat (1) meliputi :

a. pemeliharaan aplikasi; dan
b. pengelolaan kode sumber.

(3) Pemeliharaan aplikasi sebagaimana dimaksud pada Ayat (2) huruf a, dilakukan dengan cara:
a. menjaga, memperbaiki, dan mencegah kerusakan aplikasi;
b. melakukan pembaruan kode sumber aplikasi secara berkala;dan
c. melakukan *patching* keamanan kode sumber aplikasi.

(4) Pengelolaan kode sumber sebagaimana dimaksud pada Ayat (2) huruf b dilakukan melalui:
a. pembuatan salinan kode sumber;
b. kepastian hak cipta kode sumber berada pada Perangkat Daerah pemilik aplikasi; dan
c. penyimpanan kode sumber.

(5) Perangkat daerah wajib memelihara keberlangsungan keamanan sistem dan informasi yang berada di bawah tanggungjawabnya.

(6) Setiap aplikasi yang menggunakan kredential user, harus menggunakan email resmi pemerintah daerah Provinsi dalam mengauthentikasi.

Bagian Ketiga

Manajemen Data Sistem Elektronik

Pasal 27

(1) Data dari setiap aplikasi secara kumulatif dilakukan *backup* oleh Dinas secara terpusat dalam media penyimpanan data, terutama *software* aplikasi kritikal.

(2) Selain *backup* oleh Dinas, Perangkat Daerah wajib melakukan backup mandiri terhadap aplikasi dan data yang dimiliki.

(3) *Backup* dan data dilakukan secara reguler, dengan frekuensi dan jenis *backup* disesuaikan dengan tingkat kritikal sistem.

(4) Pengujian secara teratur mekanisme *backup* dan *restore* data untuk memastikan integritas dan validitas prosedur.

(5) Implementasi mekanisme *inventory* atas media penyimpanan data, terutama media yang *offline.*

(6) Dinas wajib menyediakan media penyimpanan data dengan kapasitas minimal 2 kali kapasitas terpakai.

(7) Media penyimpanan data disimpan pada Data Center yang dikelola oleh Dinas.

Bagian Keempat

Pengelolaan Data dan Informasi

Pasal 28

(1) Perangkat daerah dalam melakukan manajemen data harus berkoordinasi dengan perangkat daerah yang melaksanakan fungsi penunjang perencanaan pembangunan daerah.
(2) Perangkat daerah pengelola data harus memperhatikan tahapan:
    a. input;
    b. proses;dan
    c. output data.
(3) Pada tahapan input sebagaimana dimaksud pada Ayat (2) huruf a, prosedur yang dijalankan adalah prosedur akses data, prosedur transaksi data untuk memeriksa akurasi, kelengkapan dan validitasnya, serta prosedur pencegahan kesalahan input data.
(4) Pada tahapan proses sebagaimana dimaksud pada Ayat (2) huruf b, prosedur yang harus dijalankan adalah prosedur pengolahan data, prosedur validasi dan editing, serta prosedur penanganan kesalahan.
(5) Pada tahapan output sebagaimana dimaksud pada Ayat (2) huruf c, prosedur yang harus dijalankan adalah prosedur distribusi, penanganan kesalahan dan keamanan data.

Pasal 29

(1) Perangkat daerah pengelola data melakukan tata kelola data dan informasi sesuai ketentuan peraturan perundang-undangan, melalui :
    a. membuat daftar data dan informasi yang dikelola;
    b. membuat daftar penganggungjawab data dan informasi yang dikelola;
    c. menetapkan klasifikasi, distribusi, dan masa retensi data dan informasi;
    d. membuat daftar lokasi penyimpanan data dan informasi; dan
    e. menentukan periode *backup* dan media backup data dan informasi
(2) Daftar data dan informasi sebagaimana dimaksud pada Ayat (1) huruf a meliputi :
    a. basis data;
    b. file digital;
    c. kode sumber; dan

d. dokumen TIK.

(3) Klasifikasi sebagaimana dimaksud pada Ayat (1) huruf c meliputi:
a. publik; dan
b. dikecualikan.

Bagian Kelima

Standar Interoperabilitas

Pasal 30

(1) Dinas dan Perangkat Daerah membangun dan mengembangkan sistem elektronik dengan mengutamakan integrasi atau interoperabilitas antar aplikasi dengan memperhatikan metodologi SDLC sebagaimana dimaksud dalam Pasal 24 Ayat (2).
(2) Dalam membangun dan mengembangkan sistem elektronik, dinas dan perangkat daerah wajib membuat dokumentasi sistem meliputi :
a. diagram;
b. fungsi dan modul yang terdapat dalam aplikasi;
c. struktur basis data dan relasinya;
d. diagram alir data;
e. *user interface* dan alurnya;
f. spesifikasi teknis aplikasi;
g. manual instalasi dan konfigruasi, pemeliharaan melalui *backup* dan *restore* sistem, penggunaan aplikasi paling sedikit pada penggunaan admin dan *user*, dan
h. penerapan keamanan sistem.
(3) Dalam hal pembangunan sistem elektronik dilakukan oleh pihak ketiga, maka kode sumber dan sistem informasi yang dibangun/dikembangkan menjadi hak cipta Pemerintah Daerah Provinsi

Pasal 31

(1) Pemerintah daerah menerapkan sistem *Government Service Bus* (GSB) untuk mengelola integrasi informasi dan pertukaran data dengan instansi lain.
(2) Dalam melaksanakan penerapan sistem *Government Service Bus* (GSB) sebagaimana dimaksud pada Ayat (1), dinas membangun dan mengembangkan aplikasi yang berfungsi *Government Service Bus* (GSB).

(3) Dinas memfasilitasi layanan pertukaran data dengan pemerintah pusat, pemerintah daerah provinsi, dan pemerintah kabupaten/kota.
(4) Dinas menyusun dan menetapkan format meta data yang ditetapkan dengan Keputusan Gubernur.

BAB VI

MANAJEMEN PUSAT DATA

Pasal 32

Setiap pengoperasian infrastruktur data selalu memperhatikan kontrol yang terkait dengan faktor keamanan dan *auditability* atau memungkinkan audit atas kinerja dan sejarah transaksi yang dilakukan.

Pasal 33

(1) Perangkat daerah wajib menempatkan aplikasi pada *hosting* dan *server* pada *colocation server* di data *center* yang dikelola oleh Dinas.
(2) Dinas wajib menyediakan fasilitas data *center* yang layak sesuai dengan standar-standar yang berlaku dengan ketentuan :
    a. perangkat daerah tidak dapat melakukan pembangunan data *center;*
    b. data *center* harus terhubung dengan pusat data nasional;
    c. data *center* harus memenuhi SNI terkait pusat data dan manajemen pusat data atau menggunakan standar internasional yang berlaku;
    d. data *center* harus memenuhi pertimbangan kelaikan operasi dari Menteri yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika;dan
    e. data *center* harus memenuhi pertimbangan kelaikan keamanan dari Lembaga yang menyelenggarakan Urusan pemerintahan dibidang keamanan siber.
(3) Bagi perangkat daerah yang telah memiliki data *center* yang sesuai dengan standar yang berlaku wajib menempatkan *backup* sistem di data *center.*
(4) Dalam hal perangkat daerah telah memiliki data *center* tetapi tidak sesuai dengan standar yang berlaku maka wajib menempatkan seluruh perangkat di data *center.*

(5) Penempatan aplikasi pada *hosting* dan *server* pada *colocation server* di data *center* sebagaimana dimaksud pada Ayat (1), dilakukan dengan tahapan :

a. perangkat daerah mengajukan permohonan penyimpanan aplikasi dan *server* di data center kepada Dinas;
b. dinas melakukan uji keamanan dan kelayakan;
c. dinas melakukan analisis hasil dari uji keamanan dan kelaikan;
d. berdasarkan hasil analisis sebagaimana dimaksud pada huruf c, dinas menentukan:
   1) aplikasi dipublikasikan dan mendapatkan domain/subdomain;
   2) aplikasi dikembalikan;dan
   3) aplikasi tidak dapat dilanjutkan pembangunan dan pengembangannya.
e. dalam hal aplikasi dikembalikan pada Perangkat Daerah sebagaimana dimaksud pada huruf d angka 2, Perangkat Daerah melakukan perbaikan terhadap aplikasi yang akan ditempatkan di data *center*

(6) Dalam mengelola *Data Center*, Dinas dapat bekerjasama dengan Lembaga yang menyelenggarakan tugas pemerintahan di bidang keamanan siber dan atau lembaga lainnya yang telah memiliki *Data Center* terakreditasi

(7) Data *Center* sebagaimana tercantum dalam Lampiran II Peraturan Gubernur ini.

BAB VII
KEAMANAN INFORMASI
Bagian Kesatu
Standar Keamanan SPBE
Pasal 34

(1) Dalam setiap operasi sistem TIK, pemerintah daerah memperhatikan persyaratan minimal aspek keamanan sistem dan keberlangsungan sistem, terutama sistem TIK yang memfasilitasi layanan-layanan kritikal.

(2) Aspek keamanan dan keberlangsungan sistem TIK sebagaimana dimaksud pada Ayat (1), meliputi unsur:

a. *confidentiality*, yaitu penjamin kerahasiaan;
b. *integrity*, yaitu keutuhan;
c. *authentication*, yaitu keaslian;

d. *availability*, yaitu ketersediaan;dan
e. *Nonrepudiation*, yaitu kenirsangkalan.

(3) Lingkup aspek keamanan SPBE meliputi sumber daya SPBE, yaitu :
a. data dan informasi SPBE;
b. infrastruktur SPBE;dan
c. aplikasi SPBE.

(4) Penerapan keamanan SPBE harus memenuhi standar teknis dan prosedur keamanan SPBE sesuai dengan ketentuan yang ditetapkan oleh Lembaga yang menyelenggarakan urusan pemerintahan dibidang keamanan siber.

Pasal 35

(1) Dinas melaksanakan keamanan SPBE dengan memperhatikan aspek keamanan dan keberlangsungan SPBE sebagaimana dimaksud dalam Pasal 34.

(2) Dalam melakukan pengamanan SPBE, Dinas melakukan mekanisme :
a. Untuk pengamanan dari sisi aplikasi dapat diimplementasikan komponen standar sebagai berikut :
1) Metoda *scripting* aplikasi yang aman;
2) Implementasi mekanisme otentikasi dan otorisasi di dalam aplikasi yang tepat; dan
3) pengaturan keamanan *database* yang tepat
b. Untuk pengamanan dari sisi infrastruktur SPBE dapat diimplementasikan komponen standar sebagai berikut:
1) *Hardening* dari sisi sistem operasi;
2) *Firewall*, sebagai pagar untuk menghadang ancaman dari luar sistem;
3) *Intrusion Detection Sistem*/Intrution-Prevention Sistems (IDS/IPS) sebagai pendeteksi atau pencegah aktivitas ancaman terhadap sistem;
4) *Network monitoring tool*, sebagai usaha untuk melakukan monitoring atas aktivitas didalam jaringan; dan
5) *Log processor* dan analisis, untuk melakukan pendeteksian dan analisis kegiatan yang terjadi di sistem;
c. Untuk sistem kritikal dengan SLA yang ketat, dapat ditempuh melalui penyediaan sistem cadangan yang dapat secara cepat mengambil alih sistem utama jika terjadi gangguan ketersediaan *(availability)* pada sistem utama;

d. *Assessment* kerentanan keamanan sistem SPBE (*security vulnerability sistem*) secara teratur sesuai dengan kebutuhan.

Pasal 36

(1) Perangkat daerah harus melaksanakan pengelolaan keamanan informasi dengan cara:
   a. menjaga kerahasiaan informasi;
   b. menjaga keutuhan informasi; dan
   c. menjaga ketersediaan informasi.
(2) Menjaga kerahasiaan informasi sebagaimana dimkasud pada Ayat (1) huruf a dilakukan melalui:
   a. penetapan klasifikasi informasi;
   b. pembatasan akses terhadap informasi berklasifikasi;
   c. pengamanan pada jaringan intra pemerintah; dan
   d. penerapan teknik/kontrol keamanan pada saat proses pembuatan, pengiriman, penyimpanan, dan pemusnahan informasi.
(3) Menjaga keutuhan informasi sebagaimana dimaksud pada Ayat (1) huruf b dilakukan melalui :
   a. penerapan metode otentikasi pada informasi; dan
   b. penerapan teknik/kontrol untuk mendeteksi adanya modifikasi informasi
(4) Menjaga ketersediaan informasi sebagaimana dimaksud pada Ayat (1) huruf c dilakukan melalui:
   a. penyediaan backup informasi;
   b. penyediaan pemulihan sistem informasi; dan
   c. penyediaan *backup* infrastruktur.
(5) Pengelolaan keamanan SPBE sebagaimana tercantum dalam lampiran III Peraturan Gubernur ini.

Bagian Kedua

Manajemen Keamanan Informasi

Pasal 37

(1) Dinas melaksanakan manajemen keamanan informasi untuk menjamin keberlangsungan SPBE dengan meminimalkan dampak resiko keamanan informasi.
(2) Manajemen keamanan informasi dilakukan melalui serangkaian proses yang meliputi:
   a. penetapan ruang lingkup;
   b. penetapan penanggung jawab;

c. perencanaan;
d. dukungan pengoperasian;
e. evaluasi kinerja;dan
f. perbaikan keberkelanjutan terhadap keamanan informasi dalam SPBE.

(3) Manajemen keamanan informasi sebagaimana dimaksud pada Ayat (2) dilaksanakan berdasarkan pedoman manajemen keamanan informasi SPBE.

(4) Dalam pelaksanaan manajemen keamanan informasi, Dinas berkoordinasi, bekerjasama dan dapat melakukan konsultasi dengan kepala lembaga yang menyelenggarakan tugas pemerintahan di bidang keamanan siber.

(5) Manajemen keamanan informasi SPBE berpedoman pada Peraturan perundang-undangan di bidang keamanan siber.

BAB VIII
PENGELOLAAN EMAIL DAN DOMAIN
Bagian kesatu
Manajemen layanan email
Pasal 38

(1) Dinas menyediakan dan mengelola email resmi pemerintah daerah Provinsi.

(2) Perangkat daerah menunjuk pegawai yang bertanggung jawab mengelola email perangkat daerah dengan Surat Keputusan Perangkat Daerah.

(3) Setiap pegawai wajib menjaga keamanan email resmi yang dimiliki dan dikelolanya.

(4) Komunikasi pelaksanaan kegiatan kedinasan yang dilakukan oleh pegawai maupun perangkat daerah wajib menggunakan email resmi pemerintah daerah Provinsi.

(5) Pegawai pemerintah daerah provinsi dapat melakukan komunikasi pada pelaksanaan kedinasan dengan menggunakan email resmi yang disediakan dan dikelola oleh pemerintah pusat.

(6) Ketentuan mengenai pengelolaan e-mail diatur lebih lanjut dengan Keputusan Gubernur .

Bagian Kedua

Manajemen Pengelolaan Domain

Pasal 39

(1) Domain resmi Pemerintah Provinsi adalah gorontaloprov.go.id dengan sub-sub domainnya.
(2) Perangkat Daerah dapat menggunakan sub domain gorontaloprov.go.id untuk penamaan situs dan aplikasi pemerintahan atas persetujuan Dinas.
(3) Untuk aplikasi publik, Perangkat Daerah dapat menggunakan domain lain selain domain resmi sebagaimana dimaksud pada ayat (1) dengan melakukan permohonan ke Kementrian yang menangani domain internet melalui Dinas.
(4) Setiap pengajuan nama domain/subdomain yang disampaikan ke Dinas wajib disertai dengan data penanggung jawab website/aplikasi berbasis *web* yang ditetapkan melalui keputusan Kepala Perangkat Daerah.
(5) Dinas dapat menonaktifkan nama domain/subdomain terhadap *website* dan aplikasi yang tidak melakukan pembaharuan konten, kode sumber dan sistem operasi *server* selama 6 (enam) bulan berturut-turut.
(6) Sub domain *gorontaloprov.go.id*, penamaan domain, syarat-syarat permohonan dan syarat penggunaan domain tercantum dalam Lampiran IV Peraturan Gubernur ini.

BAB IX

OPERASIONALISASI SISTEM ELEKTRONIK

Bagian Kesatu

Umum

Pasal 40

(1) Pemerintah daerah Provinsi memberikan dukungan kepada proses bisnis manajemen dan kepada pihak-pihak yang membutuhkan sesuai spesifikasi minimal yang telah ditentukan dalam Rencana Induk SPBE.
(2) Dukungan sebagaimana dimaksud pada Ayat (1) dalam bentuk operasionalisasi sistem elektronik yang merupakan proses penyampaian layanan SPBE.
(3) Operasionalisasi sistem elektronik sebagaimana dimaksud pada Ayat (2) meliputi :
    a. manajemen tingkat layanan SPBE;
    b. manajemen aplikasi;

c. manajemen infrastruktur data;
d. manajemen infrastruktur komunikasi data;
e. manajemen data sistem elektornik
f. manajemen layanan email;
g. manajemen layanan oleh pihak ketiga;
h. manajemen sumber daya manusia SPBE;
i. manajemen risiko TIK dan keberlangungan bisnis TIK;
j. manajemen keamanan informasi;
k. manajemen asset TIK;
l. manajemen perubahan;
m. manajemen pengetahuan;dan
n. pengelolaan kepatuhan dan penilaian internal.

Bagian Kedua

Manajemen Tingkat Layanan

Pasal 41

(1) Perangkat daerah mengusulkan kepada Dinas layanan-layanan TIK yang kritikal untuk ditetapkan.
(2) Perangkat daerah yang memberikan layanan TIK bertanggung jawab atas penyusunan dan *update* katalog layanan TIK, yang berisi sistem yang beroperasi dan layanan-layanan TIK.
(3) Layanan-layanan TIK harus menetapkan SLA sebagai sebuah *requirement* atau persyaratan oleh pemilik proses bisnis.
(4) Aspek minimal yang harus tercakup dalam setiap SLA layanan TIK kritikal meliputi:
    a. waktu yang diperlukan untuk setiap layanan TIK yang diterima oleh konsumen;
    b. presentase tingkat ketersediaan (*availability*) sistem elektronik; dan
    c. waktu yang diperlukan untuk penyelesaian pengaduan insiden atau permasalahan dengan beberapa tingkatan kritikal sesuai dengan kebutuhan.
(5) Dalam hal aspek minimal SLA sbagaimana dimaksud pada Ayat (4) huruf c tidak terpenuhi, maka komite pengarah TIK memberikan surat peringatan dan/atau surat teguran kepada Dinas untuk menutup sementara *web service* sampai dengan perangkat daerah melakukan perbaikan.

Pasal 42

(1) Perangkat Darah melaksanakan layanan TIK.

(2) Dalam melaksanakan layanan TIK sebagaimana dimaksud pada Ayat (1) wajib membuat standar operasional prosedur.

(3) Penyusunan standar operasional prosedur sebagaimana dimaksud pada Ayat (2), disusun sesuai dengan ketentuan peraturan perundang-undangan.

(4) Layanan TIK sebagaimana dimaksud pada Ayat (1), merupakan layanan yang diberikan perangkat daerah kepada pihak lain dengan memanfaatkan TIK sebagai alat bantu utama.

(5) Layanan TIK sebagaimana dimaksud pada Ayat (1), paling sedikit memuat :

a. definisi layanan;
b. kebijakan layanan;
c. pengelolaan gangguan dan permasalahan;
d. pengelolaan permintaan layanan;
e. pengelolaan hubungan dengan pelanggan; dan
f. jaminan tingkat layanan yang dapat disediakan.

Bagian Ketiga

Manajemen Layanan Yang Dilakukan Pihak Ketiga

Pasal 43

(1) Layanan SPBE dapat diselenggarakan sebagian atau seluruhnya oleh pihak ketiga, dengan mempertimbangkan sumber daya internal yang dimiliki oleh pemerintah daerah Provinsi untuk mencapai tingkat layanan minimal yang diberikan kepada konsumen.

(2) Dalam hal penyelenggaraan layanan SPBE oleh pihak ketiga, pemilihan pihak ketiga harus menjamin kompetensi dan integritas pihak ketiga.

(3) Seluruh data yang diolah melalui layanan pihak ketiga adalah data milik pemerintah daerah Provinsi yang tidak dapat dipergunakan pihak ketiga di luar kerjasama.

(4) Pihak ketiga wajib memberikan transfer pengetahuan terhadap layanan SPBE yang diselenggarakan kepada Dinas.

Pasal 44

Dalam hal layanan SPBE diselenggarakan oleh pihak ketiga, perangkat daerah melakukan audit atas laporan yang disampaikan oleh pihak ketiga untuk memastikan validitasnya, baik dilakukan

secara internal atau menggunakan jasa pihak ketiga lain yang independen.

Bagian Keempat

Manajemen Sumber Daya Manusia SPBE

Pasal 45

(1) Perangkat daerah melaksanakan pengelolaan sumber daya manusia melalui :
   a. Pemetaan kompetensi TIK personel perangkat daerah;
   b. Pimpinan perangkat daerah menunjuk personal pengelola TIK di internal perangkat daerah berdasarkan hasil pemetaan sebagaimana dimaksud pada huruf a;
   c. Analisis kebutuhan pelatihan dengan cara membandingkan antara kebutuhan kompetensi dengan hasil pemetaan kompetensi TIK;
   d. Perencanaan program pelatihan peningkatan kompetensi personel; dan
   e. Fasilitasi kepada personel yang memiliki kompetensi TIK berupa pelatihan atau pendidikan pengelolaan TIK
(2) Dalam upaya pengembangan sumber daya TIK, Dinas membuat rencana pelatihan peningkatan kompetensi personel TIK sesuai kebutuhan.
(3) Pelaksanaan pelatihan dilakukan melalui kerjasama dengan perangkat daerah yang membidangi urusan pengembangan sumber daya manusia.

Bagian Kelima

Manajemen Risiko dan Keberlangsungan Bisnis SPBE

Pasal 46

Dinas melaksanakan pengelolaah risiko dan keberlangsungan bisnis melalui tahapan:

a. menentukan sistem pengendalian yang ada berikut efektivitasnya;
b. mengestimasikan level kemungkinan risiko;
c. mengestimasikan level dampak risiko;
d. menentukan level risiko; dan
e. menggambarkan kondisi risiko dalam peta risiko perangkat daerah.

Pasal 47

Dinas memastikan rencana keberlangsungan bisnis SPBE melalui uji coba terhadap seluruh sistem dan infrastruktur secara berkala.

Bagian Keenam

Manajemen Asset TIK

Pasal 48

(1) Dinas dan perangkat daerah melaksanakan manajemen aset teknologi informasi dan komunikasi sebagaimana dimaksud dalam Pasal 40 Ayat (3) huruf k untuk menjamin ketersediaan dan optimalisasi pemanfaatan aset teknologi informasi dan komunikasi dalam SPBE.
(2) Manajemen aset teknologi informasi dan komunikasi dilakukan melalui :
    a. perencanaan;
    b. pengadaan;
    c. pengelolaan;dan
    d. penghapusan perangkat keras dan perangkat lunak yang digunakan dalam SPBE.
(3) Manajemen aset teknologi informasi dan komunikasi sebagaimana dimaksud pada Ayat (2) dilaksanakan berdasarkan pedoman aset teknologi informasi dan komunikasi SPBE.
(4) Dalam pelaksanaan manajemen aset teknologi informasi dan komunikasi, Dinas berkoordinasi dan dapat melakukan konsultasi dengan menteri yang menyelenggarakan urusan pemerintahan di bidang komunikasi dan informatika.
(5) Manajemen aset teknologi informasi dan komunikasi berpedoman pada peraturan perundang-undangan di bidang komunikasi dan informatika.

Bagian Ketujuh

Manajemen Perubahan

Pasal 49

(1) Dinas dan perangkat daerah melaksanakan manajemen perubahan sebagaimana dimaksud dalam Pasal 40 Ayat (3) huruf l untuk menjamin keberlangsungan dan meningkatkan kualitas layanan SPBE melalui pengendalian perubahan yang terjadi dalam SPBE.
(2) Manajemen perubahan dilakukan melalui:
    a. perencanaan;

b. analisis;
c. pengembangan;
d. implementasi;dan
e. pemantauan dan evaluasi terhadap perubahan SPBE.

(3) Manajemen perubahan sebagaimana dimaksud pada Ayat (2) dilaksanakan berdasarkan pedoman manajemen perubahan SPBE.

(4) Dalam pelaksanaan manajemen perubahan, Dinas berkoordinasi dan konsultasi dengan Menteri yang menyelenggarakan urusan pemerintahan di bidang aparatur negara.

(5) Manajemen perubahan SPBE berpedoman pada peraturan perundang-undangan yang menyelenggarakan urusan pemerintahan di bidang aparatur negara.

Bagian Kedelapan

Manajemen pengetahuan

Pasal 50

(1) Dinas dan perangkat daerah melaksanakan manajemen pengetahuan sebagaimana dimaksud dalam Pasal 40 Ayat (3) huruf m untuk meningkatkan kualitas layanan SPBE dan mendukung proses pengambilan keputusan dalam SPBE.

(2) Manajemen pengetahuan dilakukan melalui :
a. Pengumpulan;
b. Pengolahan;
c. Penyimpanan;
d. Penggunaan;dan
e. alih pengetahuan dan teknologi yang dihasilkan dalam SPBE.

(3) Manajemen pengetahuan sebagaimana dimaksud pada Ayat (2) dilaksanakan berdasarkan pedoman pengetahuan SPBE.

(4) Dalam pelaksanaan manajemen pengetahuan, dinas berkoordinasi dan konsultasi dengan Lembaga/Kementerian yang menyelenggarakan tugas pemerintahan di bidang pengkajian dan penerapan teknologi.

(5) Manajemen pengetahuan SPBE berpedoman pada peraturan perundang-undangan Lembaga/Kementerian di bidang pengkajian dan penerapan teknologi.

Bagian Kesembilan

Manajemen Kepatuhan dan Penilaian Internal

Pasal 51

Dinas melaksanakan manajemen kepatuhan dan penilaian internal melalui:

a. proses identifikasi persyaratan, standar dan aturan yang berlaku;
b. pentuan tingkat kepatuhan; dan
c. tingkat lanjut dari hasil kepatuhan.

Pasal 52

(1) Dinas melakukan manajemen kepatuhan dan penilaian internal SPBE pada perangkat daerah secara sistematik, terencana dan terdokumentasi.
(2) Manajemen kepatuhan dan penilaian internal SPBE sebagaimana dimaksud pada Ayat (1), dilakukan untuk melihat tingkat kesesuaian dan keefektifan implementasi pengelolaan TIK yang diterapkan.
(3) Penilaian internal SPBE dilakukan oleh tim evaluator internal yang ditunjuk GCIO.
(4) Tim evaluator internal sebagaimana dimaksud pada Ayat (3) melaporkan secara tertulis hasil penialain kepada GCIO sebagai bahan laporan kepada tim koordinasi SPBE setiap Tahun.

BAB X

MEKANISME DAN TATACARA PENETAPAN STANDARISASI PENYENLENGGARAAN KOMUNIKASI DAN DISEMINASI INFORMASI

Pasal 53

(1) Portal *website* resmi Pemerintah Provinsi adalah *www.gorontaloprov.go.id* dan dikelola oleh Dinas.
(2) Masing-masing Perangkat Daerah dapat memiliki portal *web* sesuai kebutuhannya.
(3) Pemerintah Provinsi memiliki akun media sosial dalam menjalin komunikasi dengan masyarakat yang dikelola oleh Dinas
(4) Dalam rangka mengelola akun media sosial oleh dinas sebagaimana dimaksud pada Ayat (3), Gubernur menetapkan Tim Kerja Media Sosial dengan Keputusan Gubernur.
(5) Sebagai sarana pendukung komunikasi, Pemerintah Provinsi memiliki nomor pusat pesan yang dikelola oleh Dinas
(6) Nomor pusat pesan sebagaimana dimaksud pada ayat (5) digunakan untuk :

a. media komunikasi Pemerintah Daerah dengan masyarakat melalui sms dan telepon;dan
b. pendaftaran akun Media Sosial Pemerintah Daerah Provinsi

(7) Dinas, dalam mengelola nomor pusat pesan sebagaimana dimaksud pada Ayat (4), menunjuk penanggungjawab berdasarkan keputusan Pimpinan Dinas
(8) Gubernur melalui Dinas melakukan evaluasi terhadap pelaksanaan informasi melalui media sosial dan web sebagai bahan perbaikan kinerja layanan informasi.
(9) Panduan mengenai portal *website*, media sosial tercantum dalam Lampiran V Peraturan Gubernur ini

BAB XI

PEMBINAAN DAN PENGAWASAN

Pasal 54

(1) Gubernur sebagai wakil pemerintah pusat melakukan pembinaan dan pengawasan pelaksanaan Tata Kelola Sistem Pemerintahan Berbasis Elektronik.
(2) Gubernur menugaskan perangkat daerah yang membidangi Komunikasi, Informatika dan statistik untuk melakukan pembinaan dan pengawasan pelaksanaan Tata Kelola Sistem Pemerintahan Berbasis Elektronik sesuai ketentuan peraturan perundang-undangan.

BAB XII

KETENTUAN PERALIHAN

Pasal 55

Perangkat daerah yang telah memiliki aplikasi dan perangkat TIK dan tidak sesuai dengan Peraturan Gubernur ini, wajib menyesuaikan dengan ketentuan dalam Peraturan Gubernur ini paling lambat 1 (satu) Tahun sejak Peraturan Gubernur ini ditetapkan.

BAB XIII

KETENTUAN PENUTUP

Pasal 56

Peraturan Gubernur ini mulai berlaku pada tanggal diundangkan.

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

Ditetapkan di Gorontalo
pada tanggal 8 November 2019

DITANDA TANGANI SECARA ELEKTRONIK OLEH :

RUSLI HABIBIE
Gubernur Gorontalo

Diundangkan di Gorontalo
pada tanggal 8 November 2019
SEKRETARIS DAERAH PROVINSI GORONTALO,

ttd

DARDA DARABA

BERITA DAERAH PROVINSI GORONTALO TAHUN 2019 NOMOR 57

Salinan sesuai dengan aslinya
Kepala Biro Hukum
Setda Provinsi Gorontalo,

Mohamad Irizal Entengo, S.H., M.H.
Pembina Utama Muda (VI/c)
NIP. 19700115 199803 1 011

KARO HUKUM	KADIS	ASISTEN	SEKDA	WAGUB

LAMPIRAN I PERATURAN GUBERNUR GORONTALO
NOMOR : 57 TAHUN 2019
TANGGAL : 8 November 2019
TENTANG : TATA KELOLA SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK PROVINSI GORONTALO.

PEDOMAN PEMBANGUNAN DAN PENGEMBANGAN APLIKASI

1. TUJUAN

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

2. RUANG LINGKUP

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

3. KEBIJAKAN

   3.1 Aplikasi harus dikembangkan oleh pemilik proses bisnis sesuai dengan tugas dan fungsinya;

   3.2 Pemilik proses bisnis bertanggung jawab atas aplikasi yang dikembangkan;

   3.3 Penyelenggara pengembangan aplikasi adalah pihak yang ditunjuk oleh pemilik proses bisnis untuk mengembangkan aplikasi mulai dari perencanaan hingga implementasinya;

   3.4 Setiap Pimpinan Perangkat Daerah bertanggung jawab dalam penerapan Kebijakan dan Standar Pengembangan Aplikasi di Perangkat Daerah masing-masing;

   3.5 Perangkat Daerah harus menerapkan Kebijakan dan Standar Pengembangan Aplikasi di Perangkat Daerah masing-masing

   3.6 Setiap Pimpinan Perangkat Daerah bertanggung jawab dalam membangun kompetensi pengembangan aplikasi bagi pejabat/staf di lingkungan masing-masing untuk mendukung kelancaran pengembangan aplikasi;

   3.7 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*);

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

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

3.10 Aplikasi yang telah dikembangkan untuk kepentingan Pemerintah Daerah Provinsi dan Perangkat Daerah harus ditempatkan di pusat data (*data center*) Pemerintah Daerah Provinsi yang dikelola oleh Dinas;

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

4. TANGGUNG JAWAB

4.1 Pihak-pihak yang terkait dalam pengembangan aplikasi terdiri dari:

4.1.1 Pemilik proses bisnis adalah Pimpinan Perangkat Daerah yang memiliki kebutuhan akan adanya aplikasi untuk mendukung berjalannya tugas dan fungsi;

4.1.2 Pengembang aplikasi adalah ASN pada Perangkat Daerah dan/atau Pihak Ketiga yang melaksanakan pembungan dan pengembangan aplikasi;

4.1.3 Tim pengendalian mutu (*quality assurance*) adalah tim yang ditunjuk oleh Dinas dan Perangkat Daerah untuk melaksanakan kegiatan pengendalian mutu dalam pengembangan aplikasi di luar tim pengembang aplikasi;

4.1.4 Pengguna aplikasi;

4.1.5 Dinas

4.2 Pemilik proses bisnis mempunyai tanggung jawab terhadap:

4.2.1 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.

4.2.2 Pelaksanaan User Acceptance Test (UAT);

4.2.3 Memastikan bahwa aplikasi yang akan ditempatkan (hosting) di pusat data (data center) sudah bebas bug dan error;

4.2.4 Memastikan aplikasi telah memenuhi syarat keamanan informasi

4.2.5 Pemeriksaan laporan UAT untuk memastikan keluaran yang dihasilkan oleh pengembang aplikasi sesuai dengan dokumen sebagaimana dimaksud pada butir 4.2.1.a;

4.2.6 Pemeriksaan dan penandatanganan berita acara analisis hasil pengujian dan juga berita acara hasil tinjauan pasca implementasi aplikasi; dan

4.2.7 Memberi masukan kepada pengembang aplikasi terkait pengembangan dan penyempurnaan aplikasi.

4.2.8 Melakukan evaluasi pasca implementasi dan melaporkan hasilnya ke Dinas.

4.3 Pengembang aplikasi mempunyai tanggung jawab terhadap:

4.3.1 Pelaksanaan siklus pengembangan aplikasi sesuai kebijakan dan standar siklus pengembangan aplikasi;

4.3.2 Tindak lanjut masukan dari pemilik proses bisnis terkait pengembangan dan penyempurnaan aplikasi;

4.3.3 Pemeriksaan dan penandatanganan berita acara analisis hasil pengujian dan juga berita acara hasil tinjauan pasca implementasi aplikasi;

4.3.4 Proses perkembangan, histori bug dan eror dicatat dalam gitlab yang dikelola oleh Dinas

4.3.5 Penyusunan laporan status dan kemajuan pelaksanaan pengembangan aplikasi secara berkala serta pelaporan kepada pemilik proses bisnis;

4.3.6 Penyusunan laporan terkait perubahan pengembangan aplikasi berdasarkan hasil UAT serta pelaporan kepada pemilik proses bisnis; dan

4.3.7 Penyusunan dokumentasi yang merupakan keluaran pada semua tahapan pengembangan aplikasi.

4.4 Tim pengendalian mutu (quality assurance) mempunyai tanggung jawab terhadap:

4.4.1 Pendampingan dan pengendalian mutu dalam

pengembangan aplikasi;

4.4.2 Penyusunan laporan pengendalian mutu (quality assurance) dalam setiap tahapan pengembangan aplikasi;

4.4.3 Pelaksanaan User Acceptance Test (UAT).

4.5 Pengguna dapat memberi masukkan kepada Pemilik proses bisnis terkait pengembangan dan penyempurnaan aplikasi.

4.6 Dinas mempunyai tanggung jawab terhadap:

4.6.1 Pendampingan dalam pelaksanaan pengendalian mutu dalam pengembangan aplikasi;

4.6.2 Persetujuan dalam penyusunan laporan pengendalian mutu (quality assurance) dalam setiap tahapan pengembangan aplikasi;

4.6.3 Pengaturan, pembinaan, dan pengawasan pelaksanaan pengembangan aplikasi di Pemerintah Provinsi Gorontalo;

4.6.4 Memastikan bahwa pengembangan aplikasi baik proses maupun produk yang dihasilkan sesuai dengan standar aplikasi yang berlaku di Pemerintah Daerah Provinsi yang ditetapkan oleh Dinas;

4.6.5 Terlibat dalam proses pengujian aplikasi;

4.6.6 Memastikan tidak terjadi redundansi pengembangan aplikasi untuk produk aplikasi sejenis;

4.6.7 Melakukan monitoring dan evaluasi proses pengembangan aplikasi dan melaporkan setiap akhir tahun anggaran.

5. STANDAR

5.1 Siklus pengembangan aplikasi terdiri atas:

5.1.1 Proses analisis kebutuhan aplikasi, merupakan proses untuk mengumpulkan dan menganalisis spesifikasi kebutuhan bisnis dan aplikasi secara rinci;

5.1.2 Proses perancangan aplikasi, merupakan proses penyusunan rancangan aplikasi berdasarkan analisis kebutuhan aplikasi dan hasilnya akan digunakan sebagai acuan dalam proses pengembangan aplikasi;

5.1.3 Proses pengkodean (*coding*) aplikasi, merupakan proses yang dilaksanakan untuk membangun aplikasi sesuai dengan kebutuhan berdasarkan rancangan aplikasi;

5.1.4 Proses pengujian aplikasi, merupakan proses yang dilaksanakan

untuk menguji aplikasi yang telah dikembangkan;

5.1.5 Proses implementasi aplikasi, merupakan proses penerapan aplikasi yang telah dikembangkan pada lingkungan operasional; dan

5.1.6 Proses tinjauan pasca implementasi aplikasi, merupakan proses evaluasi yang dilaksanakan sebagai bahan pembelajaran untuk pengembangan aplikasi selanjutnya.

5.2 Proses analisis kebutuhan aplikasi

5.2.1 Proses analisis kebutuhan aplikasi meliputi kegiatan:

1) Pengumpulan, analisis, penyusunan, dan pendokumentasian spesifikasi kebutuhan bisnis dan aplikasi yang m encakup:
   a) Kebutuhan aplikasi termasuk fungsi kemampuan yang diinginkan, target kinerja, tingkat keamanan, dan kebutuhan spesifik lainnya;
   b) Identifikasi dan analisis risiko teknologi serta rencana mitigasi;
   c) Deskripsi aplikasi yang sudah ada (jika ada), dan analisis kesenjangannya (gap analysis) dari target aplikasi yang diinginkan;
   d) Target waktu pengembangan aplikasi;
   e) Konsep dasar operasional aplikasi;
   f) Rencana kapasitas (capacity planning);
   g) Infrastruktur pendukung.
2) Pendokumentasian perubahan analisis dan spesifikasi kebutuhan aplikasi yang terjadi dalam proses ini.

5.2.2 Proses analisis kebutuhan aplikasi menghasilkan keluaran:

1) Dokumen analisis dan spesifikasi kebutuhan aplikasi; dan
2) Dokumen perubahan analisis dan perubahan spesifikasi kebutuhan aplikasi.

5.3 Proses Perancangan Aplikasi

5.3.1 Sistem aplikasi dan basis data, meliputi kegiatan:

1) Penyusunan dan pendokumentasian rancangan tingkat tinggi dengan mengacu pada dokumen sebagaimana dimaksud pada butir (5.2.2) yang mencakup:
   a) Kebutuhan informasi dan struktur informasi;
   b) Pemetaan hak akses atas informasi oleh peran-peran yang

terlibat; dan

c) Infrastruktur pendukung yang mencakup jaringan komunikasi, *server, workstation,* perangkat pendukung, piranti lunak, dan media penyimpanan data.

2) Penyusunan dan pendokumentasian rancangan rinci yang mencakup:

a) Rancangan kebutuhan sistem aplikasi dan basis data serta infrastruktur pendukung dengan mengacu pada rancangan tingkat tinggi;

b) 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*);

c) Rancangan proses waktu nyata (*real-time processing*) dan/atau proses bertahap (*batch processing*);

d) Rancangan laporan dan dokumen keluaran;

e) Formulir pracetak (*pre-printed form*) (jika dibutuhkan) serta distribusinya sesuai dengan tingkatan pengguna dan pemisahan fungsi tugas;

f) Rancangan antarmuka (*interface*) untuk integrasi dengan aplikasi yang lain (jika dibutuhkan);

g) *Rancangan* konversi dan/ atau migrasi data (jika dibutuhkan);

h) *Rancangan* kendali internal (*internal control*) yang diperlukan dalam kegiatan antara lain validasi, otorisasi dan, jejak audit (*audit trail*); dan

i) Rancangan keamanan logika (*logic*).

5.3.2 Sistem jaringan pendukung aplikasi, meliputi kegiatan:

1) Penyusunan dan pendokumentasian rancangan tingkat tinggi dengan mengacu pada dokumen sebagaimana dimaksud pada butir (5.2.2.2) yang mencakup:

a) Gambaran secara garis besar mengenai penempatan aplikasi sistem jaringan yang ada dan rencana penempatan aplikasi dalam sistem jaringan; dan

b) Gambaran integrasi antara aplikasi dengan sistem jaringan.

2) Penyusunan dan pendokumentasian rancangan rinci yang

mencakup:

a) Rancangan kebutuhan sistem jaringan dengan mengacu pada rancangan tingkat tinggi pengembangan aplikasi;
b) Rancangan kapasitas mengacu pada rencana kapasitas (*capacity planning*) dan/atau kebutuhan dukungan sistem jaringan terhadap aplikasi;
c) Rancangan integrasi aplikasi dengan sistem jaringan yang sudah ada;
d) Rancangan keamanan aplikasi dalam sistem jaringan yang meliputi keamanan fisik maupun logika (*logic*); dan
e) Rancangan penempatan dan pemasangan sesuai dengan Kebijakan dan Standar Keamanan Aplikasi di Pemerintah Provinsi Gorontalo.

3) Menghasilkan keluaran:
   a) Dokumen rancangan tingkat tinggi; dan
   b) Dokumen rancangan rinci.

5.4 Proses Pengkodean (*coding*) Aplikasi

5.4.1 Sistem aplikasi dan basis data, meliputi kegiatan:

1) Pelaksanaan Pengkodean (*coding*) aplikasi dan basis data sesuai dengan rancangan rinci yang telah disetujui;
2) Pengelolaan perubahan dalam pengkodean (*coding*) aplikasi dan basis data;
3) Penyusunan dokumentasi pengkodean (*coding*) aplikasi dan basis data yang terdiri atas :
   a) Formulir perubahan dan rencana dan laporan hasil pengembangan;
   b) Kode program (*source code*) disertai dengan penjelasannya.
4) Pengendalian terhadap kode program (*source code*) yang sesuai dengan Kebijakan dan Standar Keamanan Aplikasi di Pemerintah Provinis Gorontalo.

5.4.2 Sistem jaringan pendukung aplikasi, meliputi kegiatan:

1) Pelaksanaan pengembangan sistem jaringan pendukung aplikasi sesuai dengan rancangan rinci yang telah disetujui;
2) Pengelolaan perubahan sistem jaringan akibat adanya proses pengembangan sistem aplikasi;

3) Penyusunan dokumentasi pengembangan sistem jaringan pendukung aplikasi:
   a) Formulir perubahan;
   b) Rencana dan laporan hasil pengembangan jaringan terkait pengembangan aplikasi;
   c) Dokumentasi setiap tahapan pengembangan sistem jaringan pendukung aplikasi;
   d) Petunjuk instalasi sistern jaringan pendukung aplikasi;
   e) Petunjuk teknis pengoperasian dan pemeliharaan sistem jaringan pendukung aplikasi; dan
   f) Materi pelatihan.
4) Pengendalian konfigurasi perangkat jaringan yang sesuai dengan Kebijakan dan Standar Keamanan Aplikasi di Pemerintah Provinsi Gorontalo;
5) Menghasilkan keluaran:
   a) Sistem aplikasi dan basis data, serta sistem jaringanpendukung aplikasi sesuai dengan rancangan rinci: dan
   b) Dokumentasi pengernbangan aplikasi.

5.5 Proses Pengujian Aplikasi

5.5.1 Proses pengujian aplikasi meliputi kegiatan:

1) Penyusunan rencana dan skenario untuk setiap jenis pengujian yang mencakup:
   a) Tujuan dan sasaran:
   b) Strategi dan metode, termasuk langkah-langkah alternatif apabila aplikasi gagal dalam pengujian;
   c) Ruang lingkup;
   d) Asumsi dan batasan;
   e) Jadwal:
   f) Pihak pelaksana dan kompetensi yang dibutuhkan;
   g) Alat bantu;
   h) Skenario dengan mempertimbangkan risiko teknologi yang telah diidentifikasi;
   i) Kriteria penerimaan (*acceptance criteria*); dan
   j) Sumber daya yang diperlukan, termasuk penyiapan lingkungan pengujian yang mencerminkan lingkungan operasional.

2) Pelaksanaan setiap jenis pengujian dengan mengacu pada rencana dan skenario. Jenis pengujian terdiri dari:
   a) Pengujian unit (*unit testing*);
   b) Pengujian sistem (*system testing*);
   c) Pengujian integrasi (*integration testing*); *dan*
   d) *UAT.*
3) Pelaksanaan analisis hasil pengujian.

5.5.2 Proses pengujian aplikasi menghasilkan keluaran:
1) Dokumen rencana dan skenario pengujian;
2) Dokumen hasil pengujian;
3) Dokumen analisis hasil pengujian.

5.6 Proses Implementasi Aplikasi

5.6.1 Proses implementasi aplikasi meliputi kegiatan:
1) Penyusunan rencana implementasi aplikasi di lingkungan operasional yang mencakup sekurang-kurangnya:
   a) Kebutuhan sumber daya;
   b) Urutan langkah implementasi dari komponen aplikasi;
   c) Pemindahan perangkat lunak dari/atau perangkat keras dari lingkungan pengujian ke lingkungan operasional;
   d) *Fall-backplan* dan/atau *backup plan* untuk mengantisipasi kegagalan dalam implementasi aplikasi; dan
   e) Jadwal pelatihan dan pengajar.
2) Implementasi aplikasi dilakukan sesuai rencana implementasi dengan memperhatikan kebijakan dan standar manajemen rilis yang akan ditetapkan dalam ketentuan tersendiri;
3) Pelaksanaan pelatihan dan transfer pengetahuan;
4) Pendampingan dalam pengoperasian aplikasi dalam kurun waktu tertentu; dan
5) Serah terima aplikasi berikut dokumentasinya kepada pemilik proses bisnis.

5.6.2 Proses implementasi aplikasi menghasilkan keluaran:
1) Dokumen rencana implementasi aplikasi;
2) Dokumen implementasi/rilis aplikasi;
3) Laporan pelaksanaan pelatihan;
4) Berita acara serah terima aplikasi;

5) Petunjuk instalasi sistem aplikasi dan basis data;
6) Petunjuk instalasi dan pengoperasian perangkat pendukung (jika dibutuhkan);
7) Payung hukum beserta petunjuk teknis yang selaras dengan proses bisnis; dan
8) Materi pelatihan.

5.6.3 Proses tinjauan pasca implementasi aplikasi meliputi kegiatan:
1) Pelaksanaan evaluasi yang dijadikan bahan pembelajaran untuk pengembangan aplikasi selanjutnya yang mencakup:
a) Pencapaian tujuan pengembangan aplikasi; dan
b) Pelaksanaan pengembangan aplikasi.
2) Penyusunan hasil tinjauan pasca implementasi aplikasi ke dalam dokumen tinjauan pasca implementasi aplikasi.

5.6.4 Proses tinjauan pasca implementasi aplikasi menghasilkan keluaran:
1) Laporan evaluasi pasca implementasi aplikasi;
2) Dokumen tinjauan pasca implementasi aplikasi.

5.7 Pengendalian Mutu

5.7.1 Pengendalian mutu meliputi kegiatan:
1) Menyusun rencana pengendalian mutu pengembangan aplikasi;
2) Melaksanakan pengendalian mutu pengembangan aplikasi melalui evaluasi/audit; dan
3) Melaporkan hasil kegiatan pengendalian mutu.

5.7.2 Setiap kegiatan pada pengendalian mutu merupakan tanggung jawab dari tim pengendalian mutu (*quality assurance*) pengembangan aplikasi.

5.7.3 Menghasilkan keluaran berupa laporan pengendalian mutu.

5.8 Standar keamanan aplikasi yang dikembangkan harus mengacu pada Kebijakan dan Standar Keamanan Informasi di Pemerintah Provinsi Gorontalo.

6. ISTILAH YANG DIGUNAKAN

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

6.2 *Fall-backplan* adalah merupakan rencana alternatif (yang menghilangkan dampak negatif) apabila terjadi kegagalan di dalam

implementasi TIK.

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

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

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

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

6.7 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.

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

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

6.10 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.

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

6.12 *User Acceptance Test* (UAT) adalah uji penerimaan yang dilakukan dengan persetujuan pemilik proses bisnis dengan menugaskan tim

quality assurance beserta pengguna. Suatu aplikasi dikatakan dapat diterima apabila telah lulus dari UAT. UAT terdiri dari uji penerimaan sistem *(systems acceptance testing)*, uji penerimaan contoh (*pilot acceptance test*), uji setiap fase pengembangan (*roll-out*), dan pengujian akhir *(final acceptance test)*.

DITANDA TANGANI SECARA ELEKTRONIK OLEH :

Balai Sertifikasi Elektronik

RUSLI HABIBIE
Gubernur Gorontalo

LAMPIRAN II PERATURAN GUBERNUR GORONTALO
NOMOR : 57 TAHUN 2019
TANGGAL : 8 November 2019
TENTANG : TATA KELOLA SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK PROVINSI GORONTALO

PUSAT DATA (*DATA CENTER*)

1. TUJUAN

   Standar ini bertujuan untuk mengatur penyelenggaraan pusat data *(data center)* di Dinas.

2. RUANG LINGKUP

   Standar ini berlaku untuk penyelenggaraan pusat data *(data center)* di Dinas yang dilaksanakan secara internal dan/atau menggunakan pihak ketiga.

3. KEBIJAKAN

   3.1 Pemerintah Provinsi menyediakan fasilitas berupa pusat data (*data center*) untuk pengelolaan SPBE.

   3.2 Penyelenggara pusat data (*data center*) Pemeritah Provinsi dilakukan secara terpusat oleh Dinas.

   3.3 Dinas menyediakan layanan penempatan (*hosting*) portal web (*website*) dan aplikasi berbasis web kepada setiap Perangkat Daerah.

   3.4 Dinas menyediakan layanan pencadangan sistem (*system backup*) untuk aplikasi yang bersifat umum dan aplikasi khusus untuk Perangkat Daerah.

   3.5 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*) pada butir 3.3.

   3.6 Perangkat Daerah selaku pemilik aplikasi bertanggung jawab akan pengelolaan aplikasi, validitas data, dan pengelolaan hak aksesnya.

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

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

3.9 Seluruh peralatan, baik perangkat keras maupun piranti lunak termasuk di dalamnya data dan aplikasi, yang berada di dalam pusat data *(data center)* menjadi milik Pemerintah Provinsi.

4. TANGGUNG JAWAB

4.1 Pihak-pihak yang terkait dalam penyelenggaraan pusat data *(data center)* terdiri dari:

4.1.1 Pemilik aplikasi adalah Perangkat Daerah di Pemerintah Provinsi yang membutuhkan aplikasi untuk mendukung tugas dan fungsinya;

4.1.2 Penyelenggara pusat data *(data center)* adalah Dinas yang melaksanakan pengembangan, pengelolaan, dan penyelenggaraan pusat data *(data center)*;

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

4.1.4 Pengguna, adalah pegawai Pemerintah Provinsi.

4.2 Pemilik aplikasi mempunyai tanggung jawab terhadap:

4.2.1 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).*

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

4.2.3 Menjamin aplikasi yang akan ditempatkan (*hosting*) di pusat data *(data center)* telah bebas dari *bug* dan *error* serta celah keamanan.

4.2.4 Melakukan perbaikan dan update aplikasi apabila ditemukan *bug* dan *error* serta penutupan celah keamanan pada aplikasi yang ditempatkan (*hosting*) di pusat data *(data center)*

4.3 Penyelenggara pusat data *(data center)* mempunyai tanggung jawab

terhadap:

4.3.1 Penyelenggaraan pusat data *(data center)* sesuai Kebijakan dan Standar pusat data *(data center)*;

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

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

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

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

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

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

5. STANDAR

5.1 Pedoman penyelenggaraan *pusat data (data center)* terdiri atas:

5.1.1 Persyaratan Disain Teknis dan Implementasi;

5.1.2 Persyaratan Operasi;

5.1.3 Persyaratan Keberlangsungan Kegiatan.

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

5.2.1 Lokasi

1) Bangunan harus berada pada lokasi yang aman berdasarkan kajian indeks rawan bencana Indonesia.

2) Bangunan harus mempunyai akses jalan yang cukup dan fasilitas parkir.

3) Lokasi sebaiknya berada di kawasan yang memiliki temperatur rendah serta tingkat kelembaban yang rendah.

5.2.2 Persyaratan Bangunan dan Arsitektur

1) Tidak berada di bawah area perpipaan (*plumbing*) seperti kamar mandi, toilet, dapur, laboratorium dan ruang mekanik kecuali jika sistem pengendalian air disiapkan.

2) Tiap jendela yang menghadap ke sinar matahari harus ditutup untuk mencegah paparan panas.
3) Memiliki area bongkar muat yang memadai untuk menangani kegiatan bongkar/muat barang/peralatan.

5.2.3 Persyaratan Kontrol Akses dan Keamanan

1) Setiap pintu dan jendela yang memungkinkan akses langsung ke pusat data *(data center)*, diberi pengaman fisik.
2) Pusat data *(data center)* harus diamankan selama 24 jam dengan paling sedikit 1 (satu) orang petugas per siklus kerja (*shift*).
3) Perangkat sistem pemantau visual (seperti CCTV) harus dipasang untuk memantau dan merekam setiap aktivitas pada ruang *server*, ruang mekanik dan kelistrikan, ruang telekomunikasi, dan kawasan kantor.
4) 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

5.2.4 Peringatan Kebakaran, Deteksi Asap, dan Pemadamkebakaran

1) Jumlah dan lokasi pintu darurat kebakaran sesuai dengan peraturan perundang-undangan.
2) Pintu darurat kebakaran dapat dibuka ke arah luar.
3) Lampu darurat dan tanda keluar diletakkan pada lokasi sesuai dengan peraturan perundang-undangan.
4) Titik panggil manual harus dipasang sesuai dengan peraturan perundang-undangan.
5) 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.
6) Ruang komputer harus diproteksi dengan sistem pendeteksi asap. Seluruh sistem deteksi asap bangunan harus

diintegrasikan ke dalam satu alarm bersama.

7) Catatan pemeliharaan yang mencakup seluruh aspek yang berkaitan dengan deteksi api dan pemadaman harus tersedia untuk keperluan pemeriksaan.
8) Bukti pelatihan staf pada simulasi pengendalian kebakaran harus tersedia.
9) Ruang pusat data *(data center)* harus dilindungi dengan sistem pemadam kebakaran. Sistem pemadam kebakaran otomatis harus dapat diaktifkan secara manual.
10) Alat pemadam kebakaran harus ditempatkan sesuai ketentuan peraturan perundangan-undangan.
11) Semua tanda peringatan kebakaran harus ditempatkan pada posisinya sesuai ketentuan peraturan perundang-undangan.
12) Seluruh sistem pendeteksi dan pemadam kebakaran harus didesain dan dipasang oleh berkualifikasi sesuai standar internasional/nasional atau regulasi nasional.
13) Jika ruang *server*, ruang telekomunikasi, dan ruang mekanikal dan kelistrikan memiliki sistem pemadam api otomatis (*sprinkler*), maka sistem tersebut harus tipe *pre- action.*
14) Jika ruang atau bangunan yang berdekatan dengan lokasi pusat data *(data center)* tidak memiliki sistem pemadam api otomatis (*sprinkler*), maka risiko kebakaran harus dikaji.

5.2.5 Penyediaan Catu Daya

1) Kabel daya masuk ke dalam bangunan pusat data *(data center)* diterminasi di ruang kendali penyambungan listrik yang handal.
2) Daya listrik utama paling sedikit 20% lebih besar dari proyeksi beban puncak di mana pusat data *(data center)* berada.
3) Tersedianya catu daya listrik alternatif (seperti generator *standby*) dengan kapasitas yang memadai untuk operasional minimal 3 jam selama kejadian gangguan listrik utama.
4) Perangkat TIK (Teknologi Informasi dan Komunikasi) harus diproteksi dengan *Uninterruptible Power Supply* (UPS) atau catu daya cadangan lainnya.
5) UPS atau catu daya cadangan lainnya harus memiliki kapasitas memadai untuk memasok beban TIK sampai catu daya

alternatif mampu memikul beban perangkat TIK (*steady-state*).

6) Kapasitas UPS harus lebih besar dari proyeksi beban puncak perangkat TIK. Kapasitas beban rata-rata tidak lebih besar dari 80% kapasitas UPS.
7) UPS memiliki sistem pelaporan, pemantauan kinerja, dan sistem peringatan.
8) UPS yang digunakan telah memiliki jaminan dari pabrikan untuk dapat berfungsi sesuai spesifikasinya.
9) Bangunan harus dilengkapi dengan sistem proteksi petir.
10) Kabel komunikasi tembaga dari luar gedung diproteksi dengan peredam tegangan lebih (*surge suppressor*) sebelum ke ruang pusat data *(data center)*.
11) Ruang pusat data (data center) memiliki terminal pembumian (grounding) tembaga yang menjadi titik acuan pembumian ruangan tersebut.

5.2.6 Penyediaan Sistem Pendingin dan Kelembaban

1) Temperatur dan kelembaban ruangan dijaga dan dikendalikan sesuai dengan kebutuhan operasional normal perangkat TIK yang paling peka.
2) Peralatan pengatur temperatur dan kelembaban harus dihubungkan ke catu daya utama (didukung oleh catu daya alternatif).

5.2.7 Penyediaan Sistem Pengkabelan dan Manajemen Kabel

1) Sistem pengkabelan yang digunakan untuk konektivitas ke setiap rak sesuai dengan standar nasional/internasional.
2) Seluruh pengkabelan interior adalah kabel dalam ruangan dengan tipe tidak mudah terbakar (*low flammability*).
3) Setiap rak memiliki akses ke sistem saluran kabel, di atas atau di bawahnya, yang memungkinkan kabel-kabel dapat ditata secara baik antar rak.
4) Kabel daya satu fase dan kabel data tembaga harus dipisahkan paling sedikit 20 cm.
5) Kabel daya tiga fase dan kabel data tembaga harus dipisahkan paling sedikit 60 cm.
6) Kabel yang melewati dinding dilindungi terhadap bahaya api sesuai ketentuan peraturan perundang-undangan.

7) Kabel tidak boleh diletakkan di pintu, lantai, atau digantung antar rak.
8) Setiap kabel memiliki label identifikasi yang unik pada kedua ujung awal dan akhir, dengan data pemilik (jika diperlukan).
9) Setiap rak peralatan memiliki label identifikasi data pemilik (jika diperlukan).
10) Kabel input telekomunikasi eksternal dihubungkan di area atau ruang telekomunikasi tersendiri.
11) 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)*.

5.2.8 Seluruh item perangkat logam berisi kabel harus dibumikan (*grounded*). Sistem Manajemen Bangunan dan Pemantauan
1) Ruang pusat data *(data center)* memiliki paling sedikit satu sensor temperatur ruang dan satu sensor kelembaban ruang.
2) Ruang telekomunikasi dan ruang mekanikal dan kelistrikan memiliki sebuah sensor temperatur dan sensor kelembaban ruang.

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

5.3.1 Tata Kerja dalam Bangunan
1) Pusat data *(data center)* memiliki satu area bongkar muat barang.
2) Seluruh peralatan dibongkar atau dikemas dan dirakit di area tertentu dan tidak dilakukan di dalam ruang komputer.
3) Ruang kendali disediakan untuk melakukan fungsi pemantauan dan pengendalian.

5.3.2 Dokumentasi Manajemen Operasi
1) Manual operasi umum diperlukan dan harus mencakup seluruh persyaratan operasi pusat data *(data center)*.
2) Seluruh perangkat utama seperti pengkondisi udara, UPS, generator, dan lain sebagainya harus terdapat dalam pencatatan aset:
   a. Lokasi
   b. Nomor seri

c. Data pengadaan
d. Kontak rinci pabrikan
e. Tanggal kalibrasi jika diperlukan

3) Konfigurasi dan prosedur operasi harus didokumentasikan termasuk di dalamnya:
   a. Perubahan konfigurasi
   b. *Set-point default*

4) Informasi dokumentasi lokasi meliputi:
   a. Bangunan dan lantai
   b. Lokasi rak dan item utama dari perangkat
   c. Denah rak
   d. Koneksi fisik dan logik antar
   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.

5) Pusat data *(data center)* memiliki panduan keamanan operasi yang merinci hal-hal seperti:
   a. Prosedur pencegahan kebakaran,
   b. Penggunaan listrik secara aman,
   c. Penggunaan perangkat transmisi data optik,
   d. Pengangkatan beban berat.

6) Prosedur tertulis harus tersedia dan mudah diakses untuk menjelaskan secara rinci status peringatan dan bagaimana gangguan sistem ditangani oleh staf pusat data *(data center)*.

5.3.3 Prosedur Pemeliharaan

1) Setiap staf pusat data *(data center)* dan/atau kontraktor yang bertugas dalam pemeliharaan harus memiliki kompetensi dalam pemeliharaan pusat data *(data center)*.

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

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

5.4.1 Manajemen Risiko

1) Pusat data *(data center)* harus memiliki kajian analisa risiko yang meliputi risiko yang mungkin terjadi, dampak, dan strategi mengurangi risiko, antara lain:
   a. Lokasi: kebakaran, banjir
   b. Komunikasi: kerusakan kabel utama.
2) Seluruh perangkat kritis seperti status UPS, kondisi gangguan, dan lain-lain harus dipantau.

5.4.2 Penanganan Insiden

1) Setiap gangguan kritis dan berhentinya layanan harus diinformasikan kepada pengguna pusat data *(data center) secepatnya.*
2) Setiap gangguan dan berhentinya layanan dapat disampaikan kepada Dinas oleh pengguna pusat data *(data center)*
3) *P*ihak administrator network harus menelaah setiap insiden sebagai berikut:
   a. Insiden yang terjadi
   b. Dimana terjadi
   c. Kapan terjadi
   d. Dampak terhadap penyediaan layanan
   e. Bagaimana mengatasinya
   f. Perubahan apa yang perlu dilakukan untuk menghindari terjadinya insiden serupa
4) Memiliki peringatan tertulis yang merinci apa saja dampak kehilangan daya mendadak dan menyeluruh pada perangkat TIK serta petunjuk tertulis bagaimana proses *restart* ditangani.
5) Efek dari terputusnya aliran daya harus disimulasi secara regular untuk membuktikan UPS dan menghidupkan (*start-up*) generator dapat beroperasi dengan baik.
6) Pada setiap siklus kerja (*shift*) harus diidentifikasi oleh petugas yang bertanggung jawab untuk memberikan tanggapan terhadap setiap insiden/bencana.

5.4.3 Pusat Pemulihan Bencana (*Disaster Recovery Center*)

1) Penyelenggara pusat data *(data center)* harus memiliki fasilitas sistem cadangan (*backup system*).
2) Penempatan fasilitas Pusat Pemulihan Bencana harus

mempertimbangkan:

a. jarak terhadap lokasi pusat data *(data center)* yang meminimalkan risiko;
b. biaya yang layak; dan
c. memenuhi Perjanjian Tingkat Layanan (*Service Level Agreement* (SLA)) yang disyaratkan.

6. ISTILAH YANG DIGUNAKAN

6.1 Pusat data *(data center)* adalah suatu fasilitas yang digunakan untuk menempatkan sistem elektronik dan komponen terkaitnya untuk keperluan penempatan, penyimpanan, dan pengolahan data.

6.2 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 Dinas secara berkesinambungan ketika pusat data (data center) mati/rusak karena bencana .

DITANDA TANGANI SECARA
ELEKTRONIK OLEH :

Balai Sertifikasi Elektronik

RUSLI HABIBIE
Gubernur Gorontalo

LAMPIRAN III PERATURAN GUBERNUR GORONTALO
NOMOR : 57 TAHUN 2019
TANGGAL : 8 November 2019
TENTANG : TATA KELOLA SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK PROVINSI GORONTALO

SISTEM MANAJEMEN KEAMANAN INFORMASI

BAB I
PENDAHULUAN

A. Tujuan

Sistem Manajemen Keamanan Informasi (SMKI) ini disusun sebagai arahan dan pedoman dalam pengelolaan sistem manajemen keamanan informasi secara terpadu serta untuk pengamanan aset informasi guna memastikan terjaganya aspek kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*).

B. Ruang Lingkup

1. Ruang lingkup kebijakan ini adalah seluruh Aset informasi dan Aset pemrosesan informasi yang berada di bawah pengelolaan Data Center Pemerintah Provinsi Gorontalo, beserta Perangkat Daerah Pemilik Aset terkait.
2. Aset informasi adalah aset dalam bentuk:
   a. fisik, meliputi informasi yang tercetak, tertulis dan tersimpan dalam bentuk fisik seperti di atas kertas, papan tulis, spanduk, atau di dalam buku dan dokumen;
   b. elektronik, meliputi informasi tercetak, tertulis dan tersimpan dalam bentuk elektronik seperti database, pada *file* di dalam komputer, ditampilkan pada *website*, layar komputer dan dikirimkan melalui jaringan telekomunikasi.

C. Kebijakan

1. Perangkat Daerah berkomitmen untuk mengembangkan, mengimplementasikan, memelihara dan meningkatkan sistem Manajemen Keamanan Informasi (SMKI) secara berkesinambungan untuk menjamin keamanan informasi organisasi dari risiko keamanan informasi, baik dari pihak internal maupun eksternal.

2. Seluruh informasi dalam bentuk fisik maupun elektronik, yang dikomunikasikan langsung atau melalui teknologi komunikasi harus dilindungi dari kemungkinan kerusakan, kesalahan penggunaan baik secara sengaja atau tidak, dicegah dari akses oleh pengguna yang tidak berwenang dan dari ancaman terhadap kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*).
3. Perangkat Daerah berkomitmen untuk mendukung pemenuhan prasyarat internal maupun eksternal keamanan informasi yang relevan.
4. Perangkat Daerah berkomitmen untuk mematuhi seluruh peraturan perundang-undangan, regulasi dan kewajiban kontrak yang relevan.
5. Perangkat Daerah berkomitmen untuk memastikan ketersediaan dari sumber daya yang dibutuhkan oleh SMKI untuk menjamin terciptanya SMKI yang efektif dan efisien.
6. Kontrol keamanan informasi beserta sasaran masing-masing kontrol ditetapkan secara tahunan, didasarkan atas hasil identifikasi dan analisis resiko yang sesuai dengan ruang lingkup kebijakan SMKI, serta prioritisasi dengan mempertimbangkan ketersediaan dan kemampuan sumber daya.
7. Kebijakan keamanan informasi harus dikomunikasikan ke seluruh pegawai dan pihak ketiga terkait melalui media komunikasi yang ada agar dipahami dengan mudah dan dipatuhi.
8. Perangkat Daerah berkomitmen meningkatkan kepedulian (*awareness*), pengetahuan dan keterampilan tentang keamanan informasi bagi pegawai, serta mitra pihak ketiga lain sejauh diperlukan.
9. Seluruh kelemahan keamanan informasi yang berpotensi atau telah mengakibatkan gangguan penggunaan TIK atau gangguan keamanan informasi harus segera dilaporkan kepada penanggung jawab TIK terkait.
10. Seluruh pimpinan di semua tingkatan bertanggung jawab menjamin kebijakan ini diterapkan di seluruh unit kerja di bawah pengawasannya.
11. Seluruh pegawai bertanggung jawab untuk menjaga dan melindungi keamanan aset informasi serta mematuhi kebijakan dan prosedur keamanan informasi yang telah ditetapkan.
12. Setiap pelanggaran terhadap kebijakan ini dapat dikenai sanksi administratif sesuai ketentuan peraturan perundang-undangan.
13. Setiap pengecualian terhadap kebijakan ini dan kebijakan turunannya

harus mendapat persetujuan dari Kepala Dinas.

14. Dokumen ini harus ditinjau paling sedikit 1 (satu) kali dalam 1 (satu) tahun atau apabila terdapat perubahan signifikan dalam proses bisnis organisasi untuk menjamin kesesuaian dan kecukupan dengan kondisi terkini.
15. Setiap perubahan terhadap dokumen ini harus didokumentasikan dan disetujui melalui proses manajemen perubahan.

BAB II

PEDOMAN PELAKSANAAN SISTEM MANAJEMEN KEAMANAN INFORMASI

A. Tujuan

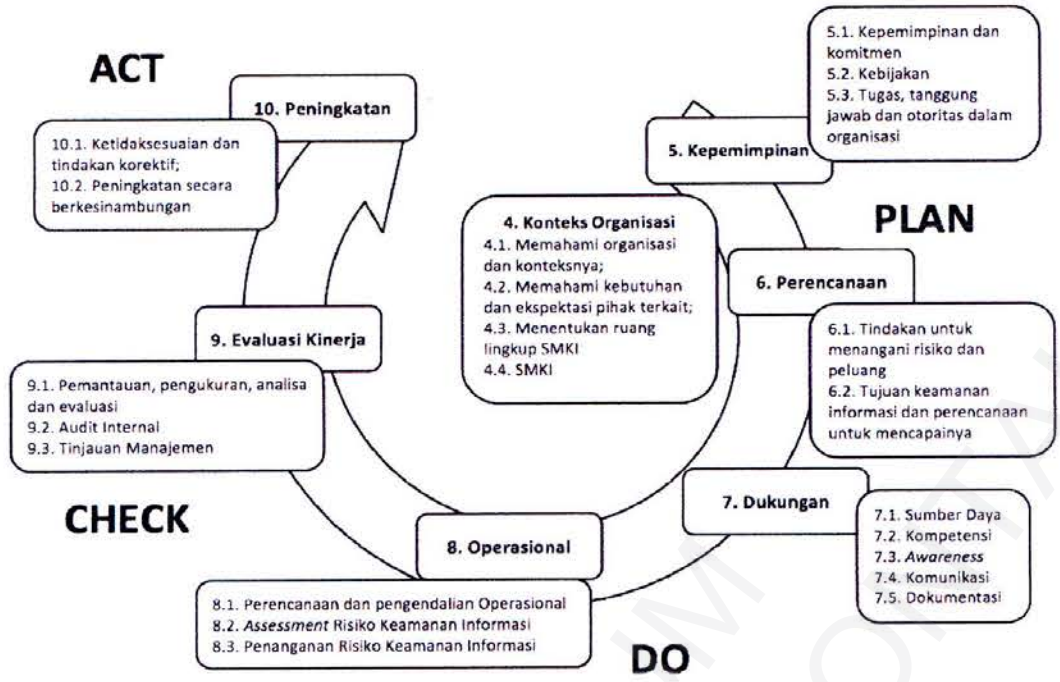
Tata kelola Sistem Manajemen Keamanan Informasi (SMKI) disusun dalam rangka untuk memastikan efektivitas dan efisiensi dari sistem manajemen keamanan informasi. Kerangka kerja ini akan menjabarkan proses-proses dan aktivitas-aktivitas yang harus dijalankan oleh Perangkat Daerah dalam rangka menetapkan, mengimplementasikan, memelihara SMKI dan meningkatkan secara berkesinambungan.

B. Ruang Lingkup

Pedoman pelaksanaan Sistem Manajemen Keamanan Informasi yang diatur dalam Peraturan Gubernur ini merupakan acuan bagi seluruh Perangkat Daerah di lingkungan Pemerintah Provinsi Gorontalo.

C. Kebijakan

1. Perangkat Daerah harus merencanakan suatu sistem manajemen keamanan informasi dengan mengadopsi siklus proses pada standard ISO 27001:2013. Deskripsi umum tentang siklus proses berdasarkan arahan standar ISO/IEC 27001:2013 dapat dilihat dari Gambar 1 sebagai berikut :



Gambar 1 Penggunaan siklus proses PDCA dalam proses SMKI

2. Proses perencanaan dalam pengembangan sistem manajemen keamanan informasi meliputi:
   2.1. Perangkat Daerah harus menentukan konteks dan ruang lingkup SMKI organisasi dengan cara:
      a. menentukan dan secara berkala meninjau faktor serta permasalahan internal dan eksternal yang dihadapi oleh organisasi yang:
         1) Relevan dengan tujuan dari Perangkat Daerah dan SMKI;
         2) Mempengaruhi kemampuan Perangkat Daerah untuk mencapai tujuan SMKI yang diharapkan oleh Dinas
      b. menentukan dan secara berkala meninjau pihak-pihak yang terkait dengan Perangkat Daerah dan dapat mempengaruhi SMKI di Perangkat Daerah;
      c. menentukan dan secara berkala meninjau kebutuhan dan ekspektasi terkait keamanan informasi dari pihak- pihak yang terkait tersebut;
      d. menentukan dan secara berkala meninjau hubungan dan ketergantungan antar proses dan aktivitas Perangkat Daerah yang dilaksanakan oleh pihak internal maupun pihak eksternal Perangkat Daerah;
      e. menentukan dan secara berkala meninjau ruang lingkup dari

SMKI di organisasi.

2.2. Risiko dan peluang yang relevan dengan SMKI harus secara jelas ditentukan dan ditangani untuk:
   a. memastikan bahwa SMKI mencapai tujuan yang diharapkan;
   b. mencegah atau mengurangi dampak yang tidak diinginkan; dan
   c. mencapai peningkatan yang berkesinambungan.

2.3. Penentuan risiko dan peluang dilakukan dengan mempertimbangkan aspek-aspek yang telah didefinisikan dalam fase penentuan konteks dan ruang lingkup Perangkat Daerah, yaitu:
   a. Faktor dan permasalahan internal maupun eksternal yang dihadapi Perangkat Daerah; dan
   b. Ekspektasi keamanan informasi dari pihak terkait Perangkat Daerah.

3. Perencanaan harus dibuat bagi risiko dan peluang yang telah ditentukan untuk:
   a. menangani risiko dan peluang;
   b. mengintegrasikan dan mengimplementasikan tindakan untuk menangani risiko dan peluang dengan proses SMKI; dan
   c. mengevaluasi efektivitas dari tindakan yang diambil dalam rangka menangani risiko dan peluang.
4. Proses manajemen risiko dilakukan melalui proses literatif yang mencakup aktivitas assessment risiko, penanganan risiko, penerimaan risiko dan pengkomunikasian risiko.
5. Seluruh manajemen risiko di organisasi harus dilakukan paling tidak 1 (satu) kali dalam satu tahun atau apabila terdapat usulan atau telah terjadi perubahan yang relevan dan signifikan pada organisasi. Seluruh catatan (*record*) terkait dengan seluruh proses manajemen risiko harus dibuat dan dipelihara.
6. Dalam proses pemilihan dari kontrol terhadap pengendalian risiko tersebut dilakukan pada saat aktifitas penanganan risiko yang merupakan bagian dari proses manajemen risiko.
7. Pemilihan dari kontrol tersebut dapat memperhatikan kontrol keamanan informasi berdasarkan standar ISO 27001:2013 atau kontrol lainnya sesuai ketentuan peraturan perundang-undangan.
8. Dalam hal proses pendokumentasian SMKI perlu memperhatikan aspek

sebagai berikut:

8.1. Dokumentasi SMKI di Perangkat Daerah perlu mencakup informasi terdokumentasi yang disyaratkan oleh ISO 27001:2013 yang mencakup namun tidak terbatas pada:

a. ruang lingkup SMKI;
b. kebijakan dan tujuan keamanan informasi;
c. metodologi assessment dan penanganan risiko;
d. *statement of applicability*;
e. rencana penanganan risiko;
f. laporan *assessment* risiko;
g. pendefinisian tugas dan tanggung jawab keamanan informasi;
h. inventarisasi aset;
i. aturan terkait penggunaan aset;
j. kebijakan pengendalian akses;
k. prosedur operasional untuk manajemen TI;
l. prinsip rekayasa sistem secara aman;
m. kebijakan keamanan terkait penyedia jasa;
n. prosedur pengelolaan insiden;
o. prosedur keberlanjutan bisnis;
p. prasyarat hukum, regulasi dan kontraktual;
q. catatan terkait pelatihan, kemampuan, pengalaman dan kualifikasi;
r. hasil pemantauan dan pengukuran SMKI;
s. program audit internal;
t. hasil audit internal;
u. hasil dari tinjauan manajemen;
v. hasil dari tindakan korektif;
w. *log* dari aktifitas pengguna, pengecualiaan dan kejadian keamanan; dan
x. informasi terdokumentasi yang dibutuhkan untuk menjamin efektifitas dari SMKI.

8.2. Dokumen yang relevan dengan SMKI dan berasal dari pihak eksternal seperti dokumen peraturan perundang-undangan harus diidentifikasi dan dikendalikan juga;

8.3. Terkait proses peninjauan dan pembaruan dokumentasi, hal-hal

berikut berlaku:

a. semua dokumentasi SMKI harus ditinjau paling sedikit satu kali dalam 1 (satu) tahun atau apabila terdapat perubahan dalam SMKI dan/atau organisasi untuk menjamin kesesuaian dan kecukupannya dengan kondisi terkini SMKI dan keamanan informasi di organisasi;
b. peninjauan harus dilakukan oleh pemilik dari dokumentasi dan dapat melibatkan pihak-pihak yang terkait dengan dokumentasi dan/atau proses yang relevan dengan dokumentasi tersebut;
c. setiap pengkinian terhadap dokumentasi SMKI sebagai hasil dari peninjauan dokumentasi harus disetujui oleh manajemen yang relevan di Perangkat Daerah;

8.4. Terkait proses salinan, distribusi dan retensi dokumentasi, hal-hal berikut berlaku:

a. salinan dari dokumentasi SMKI harus didistribusikan kepada pihak internal yang terkait untuk memastikan operasional SMKI secara efektif;
b. akses ke dokumentasi SMKI untuk pihak internal akan diberikan berdasarkan kebutuhan pengguna untuk mengakses dokumentasi tersebut (*need to know basis*);
c. pihak eksternal yang memerlukan akses kepada dokumentasi SMKI akan diberikan akses hanya setelah kontrol keamanan informasi yang memadai telah diimplementasikan. Hal ini mencakup namun tidak terbatas pada akses *read only* atau perjanjian kerahasiaan;
d. daftar distribusi harus ditetapkan dan dipelihara untuk mengendalikan distribusi dari dokumentasi SMKI; dan
e. kecuali diputuskan berbeda, seluruh dokumen SMKI memiliki masa retensi selama 10 tahun.

9. Dinas harus mempertimbangkan penyediaan sumber daya dalam melaksanakan sistem manajemen keamanan informasi yang mencakup:

9.1. ketersediaan sumber daya yang dibutuhkan bagi pelaksanaan SMKI perusahan secara efektif dan efisien sangatlah penting. Oleh karena itu perencanaan yang baik sangatlah penting untuk memastikan ketersediaan sumber daya yang tepat pada waktu yang tepat pula;

9.2. sumber daya yang dibutuhkan oleh SMKI mencakup sumber daya dengan kompetensi dan pemahaman yang memadai, dokumentasi, proses dan solusi teknis, baik berupa perangkat keras maupun perangkat lunak;

9.3. perencanaan sumber daya SMKI dapat dilakukan bersamaan dengan proses perencanaan dan penyusunan anggaran tahunan organisasi; dan

9.4. pelatihan dan program peningkatan kesadaran terkait dengan SMKI dan keamanan informasi organisasi akan dilakukan secara berkala bagi seluruh pengguna sistem informasi organisasi. Program pelatihan dan peningkatan kesadaran tersebut akan dirancang sesuai dengan fungsi dan tanggung jawab pengguna.

10. Komunikasi yang relevan dengan SMKI, baik internal maupun eksternal, harus dikendalikan dan dikoordinasikan untuk memastikan:
    a. efektivitas alur pertukaran informasi dalam organisasi SMKI dan/atau dari dan ke pihak eksternal;
    b. tidak ada kebocoran informasi sensitif milik Dinas;
    c. jalur komunikasi SMKI mencakup:
        1) komunikasi tatap muka;
        2) surat dan memo internal;
        3) *email*;
        4) *website* Perangkat Daerah;
        5) pengumuman Dinas; dan
        6) material cetak.
    d. personil Dinas yang tidak ditunjuk untuk memberikan materi informasi tidak diperbolehkan untuk memberikan informasi apapun;
    e. informasi terkait dengan SMKI dan/atau keamanan informasi yang berasal dari sumber eksternal harus dikirimkan kepada koordinator SMKI untuk peninjauan dan pendistribusian kepada pihak yang relevan dalam SMKI organisasi. Hal ini mencakup:
        1) penerbitan peraturan hukum dan perundangan yang baru maupun perubahan terhadap peraturan lama;
        2) usulan perubahan terhadap prasyarat keamanan informasi;
        3) teknologi, ancaman dan kelemahan baru terkait keamanan informasi.

11. Proses perencanaan dan pengendalian operasional SMKI harus dikoordinasikan dan dikomunikasikan. Proses perencanaan operasional SMKI harus dilakukan secara tahunan serta dokumentasikan dan dikomunikasikan kepada pihak yang terkait dengan SMKI. Proses pengendalian operasional SMKI adalah proses yang dilakukan untuk memastikan pelaksanaan operasional SMKI Perangkat Daerah telah sesuai dengan perencanaan yang telah dibuat. Proses pengendalian ini dapat mencakup aktifitas rapat peninjauan dan harus dilakukan paling sedikit 1 (satu) kali dalam tiga bulan serta melibatkan personil yang terlibat di SMKI Perangkat Daerah.
12. Metode untuk mencegah, mendeteksi dan menindaklanjuti pelanggaran terhadap hukum terkait HAKI perlu disusun dan diimplementasikan. Hal ini dapat mencakup aktivitas pemantauan, pengukuran, peninjauan dan/atau audit.
13. Pemantauan, pengukuran, analisis dan evaluasi dari implementasi dan operasional SMKI organisasi adalah aktivitas periodik yang dilakukan untuk mengevaluasi kinerja keamanan informasi dan efektivitas SMKI organisasi. Proses pemantauan, pengukuran, analisis, dan evaluasi mencakup:
    13.1. metrik pemantauan dan pengukuran harus dipilih secara seksama untuk memastikan bahwa aktivitas pengukuran akan memberikan pemahaman mendalam mengenai kinerja SMKI dan kontrol pengendalian keamanan informasi Perangkat Daerah;
    13.2. proses pengukuran tersebut mencakup proses-proses berikut:
        a. penentuan dari metrik pengukuran;
        b. pengukuran dari metrik yang telah ditentukan;
        c. analisis dan evaluasi dari hasil pengukuran.
    13.3. dalam menentukan metrik pengukuran, aspek-aspek berikut harus dipertimbangkan:
        a. sasaran SMKI yang diberikan pada kebijakan SMKI Perangkat Daerah;
        b. kontrol keamanan informasi yang diimplementasikan;
        c. metode dalam mengumpulkan data dan mengkalkulasi metrik;
        d. target pencapaian dari metrik;
        e. jadwal untuk melakukan pengukuran;

f. personil yang bertanggung jawab untuk proses pengukuran.

13.4. metrik pengukuran yang telah ditentukan harus memungkinkan evaluasi dari pencapaian sasaran SMKI;

13.5. metrik yang telah ditetapkan harus dipantau dengan mengumpulkan data yang relevan dengan metrik;

13.6. proses pengukuran harus dilakukan minimal 1 (satu) kali dalam satu tahun terutama untuk mengukur pencapaian dari sasaran SMKI;

13.7. hasil dari pengukuran harus dianalisis dan dievaluasi untuk menentukan pencapaian dari target pengukuran tersebut;

13.8. hasil dari pengukuran harus dilaporkan kepada manajemen puncak SMKI dalam rapat tinjauan manajemen SMKI;

13.9. hasil dari proses pemantauan dan pengukuran efektivitas SMKI harus dianalisis dan dievaluasi untuk menentukan apakah implementasi dan operasi SMKI organisasi:

a. sesuai dengan kebijakan, tujuan, standar dan prosedur SMKI organisasi;

b. memadai untuk menghadapi kebutuhan dan tantangan bisnis serta teknologi terkini; dan

c. sesuai dengan rencana SMKI yang sudah dibuat.

14. Peninjauan keamanan informasi secara independen harus secara rutin dilakukan.

14.1. peninjauan tersebut harus mencakup:

a. kontrol dan area keamanan informasi, seperti keamanan fisik, jaringan atau akses *logical*;

b. kebijakan, proses dan prosedur yang relevan dengan SMKI;

c. kepatuhan implementasi SMKI dan keamanan informasi dengan kebijakan, proses dan prosedur keamanan informasi Perangkat Daerah serta prasyarat hukum, perundangan serta kewajiban kontraktual terkait dengan SMKI;

d. peninjauan teknis terhadap fasilitas pengolahan informasi dan sarana pendukungnya.

14.2. hasil dari peninjauan harus didokumentasikan dan dilaporkan kepada manajemen SMKI yang relevan.

14.3. setiap permasalahan dan/atau ketidaksesuaian harus segera

ditindaklanjuti dengan cara mengidentifikasi tindakan korektif dan/atau peningkatan yang sesuai.

15. Dinas harus melakukan proses audit internal dengan ketentuan sebagai berikut:
    15.1. audit internal SMKI di Perangkat Daerah harus dilaksanakan minimal satu kali dalam satu tahun dan harus mencakup seluruh ruang lingkup SMKI;
    15.2. audit internal SMKI harus dilakukan oleh auditor yang memiliki kompetensi yang memadai serta memiliki objektifitas dan imparsialitas terhadap proses audit;
    15.3. auditor yang dipilih untuk proses audit harus ditunjuk secara formal oleh manajemen puncak SMKI;
    15.4. sebuah program audit tahunan SMKI harus ditetapkan oleh koordinator audit internal SMKI dan harus dikomunikasikan kepada koordinator SMKI;
    15.5. program audit harus mencakup jadual, metode, kriteria dan ruang lingkup, tanggung jawab serta prasyarat pelaporan dari audit;
    15.6. proses audit harus dilakukan sesuai dengan program audit yang telah ditetapkan secara formal;
    15.7. temuan audit harus diklasifikasikan berdasarkan kritikalitas dan cakupan dari temuan tersebut menjadi:
        a. mayor, ketidaksesuaian ini mengindikasikan tidak berjalannya sama sekali sebuah proses SMKI atau kontrol keamanan informasi, atau apabila sebuah temuan dapat menyebabkan dampak buruk terhadap proses atau sistem kritikal Dinas
        b. minor, ketidaksesuaian ini mengindikasikan sebuah kealpaan/ problem kecil yang tidak mengindikasikan bahwa sebuah proses SMKI atau kontrol keamanan informasi tidak berjalannya sama sekali, atau apabila sebuah temuan tidak akan menyebabkan dampak buruk terhadap proses atau sistem kritikal Dinas; dan
        c. peluang untuk perbaikan, kategori temuan ini bukan merupakan sebuah ketidaksesuaian namun mengindikasikan bahwa sebuah area dapat diperbaiki untuk meningkatkan kinerja dari proses atau sistem.
    15.8. setiap ketidaksesuaian dan/atau peluang untuk perbaikan yang

ditemukan dalam proses audit harus dicatat secara formal oleh auditor dan diterima oleh auditee;

15.9. setiap ketidaksesuaian harus dikoreksi dan ditingkatkan oleh *auditee* dalam jangka waktu yang disepakati dengan cara merencanakan dan melaksanakan koreksi dan tindakan korektif;

15.10. laporan audit harus dilaporkan kepada manajemen puncak Perangkat Daerah dan dikomunikasikan kepada koordinator SMKI;

15.11. koordinator SMKI dan auditor internal SMKI bertanggung jawab untuk memantau dan memverifikasi koreksi, tindakan korektif maupun peningkatan terkait ketidaksesuaian yang ditemukan dalam audit;

15.12. verifikasi dari auditor internal SMKI dibutuhkan sebelum ketidaksesuaian yang ditemukan dapat dinyatakan ditutup secara formal.

16. Manajemen SMKI Perangkat Daerah wajib untuk melaksanakan tinjauan manajemen SMKI minimal satu kali dalam satu tahun atau apabila terjadi perubahan signifikan terhadap SMKI di Perangkat Daerah. Tinjauan ini dilakukan untuk menjamin terjaganya kesesuaian, kecukupan dan efektivitas dari SMKI di Perangkat Daerah, dengan memperhatikan hal-hal sebagai berikut:

16.1. Tinjauan manajemen SMKI harus dihadiri oleh:

a. manajemen puncak dari SMKI di Perangkat Daerah;
b. koordinator SMKI Perangkat Daerah;
c. koordinator atau petugas fungsional SMKI.

16.2. Apabila dibutuhkan, tinjauan manajemen SMKI dapat dihadiri oleh:

a. pemangku kepentingan yang relevan dari SMKI di unit kerja yang membidangi teknologi informatika;
b. *subject matter expert* yang memadai.

16.3. Tinjauan manajemen SMKI harus mencakup masukan sebagai berikut:

a. status dari tindakan yang diputuskan pada tinjauan manajemen terdahulu;
b. perubahan baik internal maupun eksternal yang terkait dengan SMKI;

c. masukan terkait kinerja keamanan informasi yang mencakup *trend* pada:
   1) ketidaksesuaian dan tindakan korektif;
   2) hasil pemantauan dan pengukuran;
   3) hasil audit, baik internal maupun eksternal; dan
   4) pemenuhan dari sasaran keamanan informasi.
d. masukan dari pihak terkait;
e. hasil dari assessment risiko dan status rencana penanganan risiko;
f. peluang untuk peningkatan secara berkesinambungan.

16.4. Berdasarkan dari masukan tersebut, tinjauan manajemen SMKI harus menghasilkan keluaran sebagai berikut:
a. Keputusan terkait peningkatan SMKI secara berkesinambungan; dan
b. peluang dan kebutuhan untuk perubahan SMKI.

16.5. setiap keluaran dari tinjauan manajemen SMKI harus digunakan sebagai dasar bagi peningkatan dan perencanaan tahunan SMKI.

17. Ketidaksesuaian SMKI didefinisikan sebagai kondisi dimana adanya prasyarat SMKI yang tidak terpenuhi. Setiap ketidaksesuaian atau tidak terpenuhinya prasyarat SMKI harus di identifikasi dan di laporkan:

17.1. identifikasi dan laporan dari setiap ketidaksesuaian dapat didapatkan melalui:
a. proses pengelolaan insiden keamanan informasi;
b. peninjauan internal SMKI;
c. proses audit internal SMKI;
d. proses pemantauan dan pengukuran SMKI;
e. peninjauan dan/atau proses audit eksternal terhadap SMKI atau keamanan informasi; dan
f. laporan dan masukan dari *stakeholder* yang terkait.

17.2. setiap ketidaksesuaian yang terjadi, harus ditangani secara tepat dengan cara:
a. melakukan koreksi yang sesuai untuk mengendalikan dan memperbaiki ketidaksesuaian yang telah diidentifikasi; dan
b. menangani setiap akibat dari ketidaksesuaian yang mungkin terjadi.

17.3. untuk setiap ketidaksesuaian, evaluasi harus dilakukan untuk mengevaluasi kebutuhan untuk mengambil tindakan korektif untuk menghilangkan penyebab dari ketidaksesuaian supaya ketidaksesuaian tersebut tidak terjadi lagi atau terjadi ditempat lain.

17.4. tindakan korektif yang diambil harus sesuai dengan dampak dari ketidaksesuaian tersebut untuk memastikan bahwa ketidaksesuaian tersebut tidak berulang atau terjadi ditempat lain dalam ruang lingkup SMKI.

17.5. evaluasi untuk menentukan apakah perlu untuk mengambil setiap tindakan korektif harus dilakukan dengan melakukan:

a. peninjauan terhadap ketidaksesuaian yang terjadi;
b. menentukan penyebab dari ketidaksesuaian;
c. menentukan jika ada kejadian dimana ketidaksesuaian yang sama telah terjadi, atau dapat berpotensi untuk terjadi.

17.6. apabila ditentukan bahwa tindakan korektif memang perlu untuk diambil maka harus dilakukan perencanaan dan implementasi dari tindakan korektif.

17.7. setelah koreksi dan tindakan korektif telah diambil, sebuah peninjauan harus dilakukan untuk menjamin efektifitasnya dalam mencegah terjadinya kembali atau terjadinya ketidaksesuaian tersebut ditempat lain.

18. Kesesuaian, kecukupan dan efektifitas dari SMKI Perangkat Daerah harus secara berkesinambungan ditingkatkan.
19. Inisiatif peningkatan harus secara formal diidentifikasi, direncanakan, diimplementasikan dan ditinjau.
20. Identifikasi dari peningkatan harus dilakukan berdasarkan *log*, laporan dan hasil dari:

a. proses pengelolaan insiden keamanan informasi;
b. peninjauan internal SMKI;
c. proses audit internal SMKI;
d. proses pemantauan dan pengukuran SMKI;
e. peninjauan dan/atau proses audit eksternal terhadap SMKI atau keamanan informasi; dan
f. laporan dan masukan dari *stakeholder* yang terkait.

21. Perencanaan dan implementasi dari inisiatif peningkatan harus ditinjau untuk memastikan bahwa inisiatif tersebut dapat mencapai tujuannya.
22. Dokumentasi yang relevan dengan proses peningkatan secara berkesinambungan harus dibuat dan dipelihara.

BAB III

MANAJEMEN RISIKO

A. Tujuan

Tujuan dari manajemen resiko adalah untuk mengelola risiko keamanan informasi yang dihadapi oleh dinas dalam rangka untuk mempersiapkan diri terhadap terjadinya risiko beserta dampaknya.

B. Ruang Lingkup

Ruang lingkup dari manajemen risiko memastikan Perangkat Daerah dapat menerapkan proses Pengelolaan Risiko yang mencakup kegiatan:

1. Penetapan konteks;
2. *Assessment* risiko;
3. Penanganan risiko;
4. Pemantauan dan peninjauan risiko;
5. Komunikasi dan koordinasi risiko.

C. Kebijakan

1. Kriteria penerimaan risiko dan penilaian keamanan informasi harus ditetapkan untuk memberikan arahan bagi Perangkat Daerah terhadap penanganan risiko yang harus dilakukan.
2. Perangkat Daerah harus menerapkan konteks terkait rencana perencanaan identifikasi risiko yang meliputi isu-isu, pihak terkait dan prasyarat keamanan informasi internal dan eksternal yang terkait dengan keamanan informasi harus diidentifikasi dan ditetapkan sebagai pertimbangan dalam mengidentifikasi risiko keamanan informasi. Hal ini setidaknya mencakup:
   a. kegiatan utama yang dilakukan oleh organisasi;
   b. kebijakan internal organisasi;
   c. proses bisnis organisasi;
   d. kewajiban hukum, perundangan dan kewajiban kontrak yang dimiliki oleh organisasi;

e. kondisi teknologi informasi dan keamanan informasi, baik internal maupun eksternal yang relevan dengan organisasi.

3. Perangkat Daerah harus melaksanakan penilaian risiko yang berpengaruh terhadap kegagalan sistem dan operasional TI terkait dengan aspek keamanan informasi yang mencakup aktivitas:

   3.1 identifikasi risiko :

   a. mengidentifikasi ancaman, merupakan aktifitas untuk mengidentifikasi ancaman terhadap risiko keamanan informasi;
   b. ancaman didefinisikan sebagai potensi penyebab insiden yang tidak diinginkan yang dapat menyebabkan kerusakan/kerugian bagi organisasi dan sistemnya;
   c. sebuah ancaman tidak dapat dikatakan sebuah risiko apabila tanpa kombinasi dengan kelemahan yang dapat dieskplotasi;
   d. mengidentifikasi kelemahan dilakukan setelah pengidentifikasian ancaman dilakukan;
   e. kelemahan didefinisikan sebagai potensi kekurangan pada proses dan kontrol keamanan yang dapat dieksplotasi oleh satu ancaman atau lebih;
   f. mengidentifikasi dampak merupakan aktifitas yang dilakukan untuk mengidentifikasi potensi dampak jika ancaman yang teridentifikasi, mengeksploitasi kelemahan yang ada;
   g. risiko harus dialokasikan ke pemilik risiko; dan
   h. pemilik risiko bertanggung jawab untuk mengelola risiko yang telah teridentifikasi.

   3.2 analisis risiko :

   a. menilai dampak potensial yang akan terjadi apabila risiko yang teridentifikasi terwujud;
   b. kriteria dampak merupakan parameter untuk menentukan

tingkat kerugian terhadap risiko yang terjadi. Contoh kriteria dampak adalah sebagai berikut:

Tabel 1 Tabel Dampak Resiko SMKI

Tingkat Dampak	Operasional	Peraturan / Hukum	Aset Informasi	Reputasi
1 (Ringan)	Penundaan proses bisnis setengah hari	Tidak ada pelanggaran hukum	Tidak ada kebocoran atau kehilangan aset informasi.	Tidak ada dampak terhadap reputasi Perangkat Daerah/Unit Kerja
2 (Sedang)	Penundaan proses bisnis 1 hari	Pelanggaran ringan dengan surat peringatan	Berdampak pada kebocoran atau kehilangan aset informasi yang bersifat PUBLIK.	Mengganggu kepercayaan sebagian kecil pihak eksternal. Berdampak pada reputasi Perangkat Daerah namun reputasi dapat dipulihkan dalam waktu tidak terlalu lama.
3 (Berat)	Penundaan proses bisnis 3 hari	Pelanggaran sedang yang dikenakan sanksi administratif	Berdampak pada kebocoran atau kehilangan aset informasi yang bersifat TERBATAS.	Mengganggu kepercayaan sebagian besar pihak eksternal. Berdampak pada reputasi Perangkat Daerah dan pemulihan reputasi membutuhkan waktu yang lama.
4 (Sangat Berat)	Penundaan lebih dari 3 hari	Pelanggaran berat dengan sanksi hukum	Berdampak pada kebocoran atau kehilangan aset informasi yang bersifat RAHASIA.	Mengganggu kepercayaan sebagian besar pihak eksternal, Berdampak pada reputasi Perangkat Daerah dan sangat sulit dilakukan pemulihan reputasi.

c. Menilai kemungkinan realistis terjadinya risiko yang teridentifikasi; dan

d. Kriteria kecenderungan merupakan parameter untuk menentukan tingkat kejadian terhadap Risiko.

Contoh kriteria kecenderungan adalah sebagai berikut:

Nilai	Tingkat	Kriteria Kecenderungan
		Frekuensi terjadinya
1	Rendah	Kejadian tidak lebih dari 2 kali / tahun
2	Sedang	Kejadian lebih dari 2 kali / tahun, namun tidak lebih dari 5 kali / tahun
3	Tinggi	Kejadian lebih dari 5 kali / tahun, namun tidak lebih dari 10 kali / tahun
4	Ekstrim	Kejadian lebih dari 10 kali / tahun

Tabel 1 Tabel Kecenderungan Risiko SMKI

e. Evaluasi risiko :

1) Membandingkan hasil analisis risiko dengan kriteria risiko yang sudah ditetapkan;
2) risiko yang masuk dalam kriteria penerimaan risiko akan diterima;
3) risiko yang tidak masuk dalam kriteria penerimaan risiko perlu mendapatkan penanganan; dan
4) setiap penanganan risiko harus diberikan prioritas.

4. Hasil evaluasi risiko harus dianalisis terkait risiko tersebut dapat diterima dalam level tertentu berdasarkan kriteria penerimaan risiko yang telah ditetapkan atau memerlukan penanganan risiko lebih lanjut.

Tabel risiko adalah matriks antara nilai dari dampak dan kecenderungan yang menghasilkan tingkat risiko.

Contoh tabel risiko adalah sebagai berikut:

Tabel SEQ Nilai Risiko SMKI

5. Dalam hal risiko tersebut tidak dapat diterima, Perangkat Daerah harus menerapkan penanganan risiko yang diperlukan yang mencakup:
   a. mengendalikan/*control* adalah merupakan tindakan pengendalian risiko dengan mengurangi dampak maupun kemungkinan terjadinya risiko melalui menerapkan suatu sistem atau aturan;
   b. menghindari/*avoid* adalah tindakan pengendalian risiko dengan tidak melakukan suatu aktivitas atau memilih aktivitas lain dengan output yang sama untuk menghindari terjadinya risiko;
   c. mengalihkan/transfer adalah tindakan pengendalian risiko dengan mengalihkan seluruh atau sebagian tanggung jawab pelaksanaan suatu proses kepada pihak ketiga.
6. Penanganan risiko harus memadai untuk mengurangi risiko ke tingkat yang dapat diterima berdasarkan kriteria penerimaan risiko.
7. Pemilik risiko harus memastikan setiap rencana penanganan risiko telah memadai dan relevan bagi risiko yang ada.
8. Setiap rencana penanganan risiko harus diberikan prioritas oleh pemilik risiko.
9. Setiap keputusan terkait dengan penanganan risiko dan kontrol keamanan risiko yang relevan harus disetujui oleh Pimpinan Perangkat Daerah terkait.

10. Perangkat Daerah harus melakukan proses pemantauan dan peninjauan risiko untuk memastikan efektifitas kontrol yang dilakukan yang mencakup:
    a. proses pemantauan dan peninjauan risiko adalah proses berkesinambungan untuk memastikan bahwa :
        1) risiko baru telah terindentifikasi, di-*assess* dan ditangani;
        2) setiap perubahan terhadap risiko yang sudah ada telah teridentifikasi, di-*assess* dan ditangani;
        3) kontrol keamanan yang sudah ada telah memadai dan efektif dalam menangani risiko.
    b. proses pemantauan dan peninjauan risiko harus dilakukan secara formal dan rutin;
    c. Perangkat Daerah harus menentukan frekuensi pemantauan dan peninjauan risiko.
11. Perangkat Daerah harus melakukan proses komunikasi dan koordinasi risiko untuk memastikan pengelolaan penanganan kontrol terkendali dan efektif dalam mengurangi tingkat Risiko yang diharapkan.
12. Metode komunikasi dan koordinasi risiko harus ditetapkan yang meliputi:
    a. proses komunikasi dan koordinasi risiko merupakan proses berkesinambungan untuk mengkomunikasi dan mengkoordinasikan setiap informasi, aktifitas dan keputusan terkait dengan risiko keamanan informasi dan proses manajemen risiko;
    b. setiap informasi, aktifitas dan keputusan harus dikomunikasikan dan dikoordinasikan dengan pemilik risiko, personil terkait dan Kepala Perangkat Daerah; dan
    c. setiap komunikasi dan koordinasi eksternal terkait risiko keamanan informasi dan manajemen risiko harus disetujui oleh Kepala Perangkat Daerah.

BAB IV

ORGANISASI SISTEM MANAJEMEN KEAMANAN INFORMASI

A. Tujuan

Organisasi Tim Keamanan Informasi Pemerintah Provinsi Gorontalo dibentuk dengan tujuan sebagai berikut:

1. Sebagai pedoman dalam pembentukan organisasi fungsional keamanan informasi yang bertanggung jawab dalam pengelolaan keamanan informasi serta hubungan kerja dengan pihak eksternal.
2. Menumbuhkan kesadaran pada SDM Pemerintah Provinsi Gorontalo tentang arti penting keamanan informasi.
3. Memastikan keamanan informasi terkait penggunaan perangkat *mobile* dan pelaksanaan aktivitas *teleworking.*

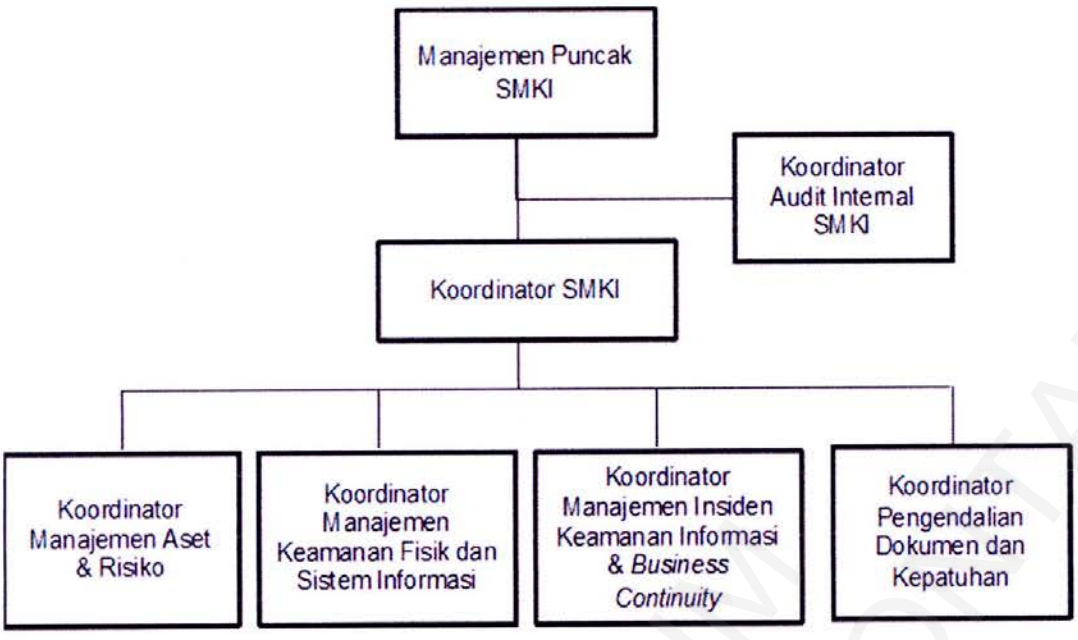
B. Ruang Lingkup

Ruang lingkup terkait dengan organisasi SMKI ini mengatur mengenai:

1. struktur organisasi Tim Keamanan Informasi Pemerintah Provinsi Gorontalo;
2. hubungan kerja dengan pihak berwenang, komunitas keamanan informasi dan pihak ketiga; dan
3. penggunaan perangkat *mobile* dan teknologi *teleworking*.

C. Kebijakan

1. Perangkat Daerah wajib membentuk struktur organisasi berbasiskan sistem manajemen keamanan informasi untuk memastikan pelaksanaan keamanan informasi sesuai dengan standar ISO 27001:2013.
2. Organisasi Sistem Manajemen Keamanan Informasi merupakan organisasi fungsional yang memiliki struktur seperti yang diberikan pada Gambar 2 berikut:



Gambar 2 Struktur Organisasi SMKI di Perangkat Daerah

3. Manajemen puncak SMKI memiliki tugas dan tanggung jawab sebagai berikut:
   a. memberikan arahan dan tujuan umum dari SMKI organisasi, dalam bentuk kebijakan Sistem Manajemen Keamanan Informasi (SMKI);
   b. memastikan bahwa tujuan dan rencana dari SMKI organisasi telah ditetapkan;
   c. menetapkan struktur organisasi beserta alokasi tugas dan tanggung jawab dalam SMKI organisasi;
   d. mengkomunikasikan kepada personil dalam organisasi terkait pentingnya pemenuhan aturan terkait keamanan informasi organisasi sesuai ketentuan peraturan perundang-undangan serta perlunya peningkatan SMKI organisasi secara berkesinambungan;
   e. menyediakan sumber daya yang memadai untuk menetapkan, mengimplementasi, mengoperasikan, memantau, meninjau, memelihara dan meningkatkan SMKI organisasi;
   f. menetapkan kriteria penerimaan risiko dan tingkat risiko yang dapat diterima;

g. menyetujui tingkat risiko residual keamanan informasi;
h. memastikan pelaksanaan audit internal SMKI;
i. menghadiri dan memimpin rapat tinjauan manajemen SMKI.

4. Koordinator SMKI memiliki tugas dan tanggung jawab sebagai berikut:
   a. menyusun, mengkoordinasikan serta memantau pelaksanaan program kerja SMKI;
   b. mengkoordinasikan pelaksanaan proses manajemen risiko SMKI organisasi;
   c. mengkoordinasikan pelaksanaan aktifitas SMKI serta pengamanan informasi di organisasi;
   d. mengkoordinasikan proses peninjauan secara berkala terhadap implementasi SMKI di organisasi;
   e. mengkoordinasikan proses pengukuran efektivitas SMKI dan kontrol keamanan informasi di organisasi;
   f. mengkoordinasikan aktivitas dan tindakan untuk meningkatkan efektivitas SMKI, yang mencakup antara lain koreksi dan tindakan korektif untuk ketidaksesuaian yang ditemukan serta pelaksanaan rencana penanganan risiko; dan
   g. memberikan laporan secara berkala terkait kondisi SMKI dan keamanan informasi organisasi kepada manajemen puncak SMKI.

5. Koordinator audit internal SMKI memiliki tugas dan tanggung jawab sebagai berikut :
   a. menyusun dan memantau program dan jadwal audit internal SMKI;
   b. mengkoordinasikan pelaksanaan proses audit internal SMKI;
   c. merangkum dan melaporkan hasil audit internal SMKI kepada manajemen puncak SMKI;
   d. memberikan rekomendasi terkait kontrol keamanan informasi yang diperlukan untuk meningkatkan efektivitas SMKI; dan mengkoordinasikan proses verifikasi koreksi dan tindakan

korektif yang diambil terhadap ketidaksesuaian yang ditemukan dalam proses audit internal SMKI.

6. Koordinator manajemen aset dan risiko SMKI memiliki tugas dan tanggung jawab sebagai berikut :
   a. mengkoordinasikan dan memantau pengelolaan aset informasi dan aset pengolahan dan penyimpanan informasi organisasi, hal ini mencakup proses registrasi, inventarisasi serta pemeliharaan inventarisasi aset tersebut;
   b. menyusun dan memelihara dokumen registrasi aset informasi dan aset pengolahan dan penyimpanan informasi organisasi;
   c. melakukan peninjauan terkait proses penanganan aset informasi dan aset pengolahan dan penyimpanan informasi organisasi berdasarkan kebijakan dan prosedur terkait pengelolaan aset SMKI organisasi;
   d. menyusun dan mengkoordinasikan aktivitas proses pengelolaan manajemen risiko SMKI di organisasi, bekerja sama dengan pemilik risiko, berdasarkan kebijakan dan prosedur terkait pengelolaan risiko SMKI organisasi;
   e. mengkoordinasikan proses registrasi terhadap risiko SMKI di organisasi, bekerja sama dengan pemilik risiko;
   f. mengkoordinasikan pengkinian secara rutin terhadap registrasi risiko organisasi, bekerja sama dengan pemilik risiko; dan
   g. menyusun dan memelihara dokumen *risk profile* dan *risk treatment plan* SMKI organisasi.
7. Koordinator manajemen keamanan fisik dan sistem informasi SMKI memiliki tugas dan tanggung jawab sebagai berikut :
   a. mengkoordinasikan dan memantau proses dan aktifitas pengamanan fisik dan lingkungan dalam organisasi;
   b. melaksanakan proses pengelolaan dan pemeliharaan fasilitas pengamanan fisik organisasi berdasarkan kebijakan dan prosedur terkait keamanan fisik dan lingkungan SMKI

organisasi;

c. melaksanakan proses pengelolaan dan pemeliharaan hak akses fisik ke fasilitas organisasi berdasarkan kebijakan dan prosedur terkait keamanan fisik dan lingkungan smki organisasi;
d. mengkoordinasikan dan memantau proses dan aktifitas pengelolaan akses *logical*;
e. melaksanakan proses pengelolaan dan pemeliharaan akses *logical* dari pengguna ke sistem informasi organisasi berdasarkan *kebijakan* dan prosedur terkait keamanan akses logical ke sistem informasi organisasi, hal ini mencakup proses pendaftaran, pemeliharaan dan pencabutan hak akses *logical* pengguna ke sistem informasi;
f. mengakomodasi penyusunan dan pemeliharaan *access control matrix* bersama-sama dengan Perangkat Daerah pemilik aplikasi dan/atau informasi;
g. mengkoordinasikan dan memantau pengelolaan keamanan operasional sistem informasi organisasi berdasarkan kebijakan dan prosedur terkait pengelolaan keamanan operasional sistem informasi organisasi; dan
h. merancang, memantau dan memelihara sistem keamanan dari sistem informasi organisasi yang ini mencakup perangkat keras, lunak maupun aktif jaringan dan keamanan jaringan dalam sistem informasi organisasi.

8. Koordinator manajemen insiden keamanan informasi dan *business continuity* SMKI memiliki tugas dan tanggung jawab sebagai berikut:
   a. mengkoordinasikan proses pendokumentasian laporan terkait kejadian, kelemahan dan insiden keamanan informasi berdasarkan kebijakan dan prosedur terkait pengelolaan insiden keamanan informasi organisasi;
   b. mengkoordinasikan dan memantau pengelolaan insiden

keamanan informasi berdasarkan kebijakan dan prosedur terkait pengelolaan insiden keamanan informasi organisasi;

c. mendokumentasikan proses pengelolaan insiden keamanan informasi di organisasi;

d. mengkoordinasikan dan memantau pengelolaan *business continuity management* di organisasi berdasarkan kebijakan dan prosedur terkait business continuity management organisasi;

e. mengkoordinasikan penyusunan, pengujian dan pemeliharaan *business continuity plan* dan *disaster recovery plan* organisasi;

f. memastikan terjaganya aspek keamanan informasi dalam proses *business continuity management.*

9. Koordinator pengendalian dokumen dan kepatuhan SMKI memiliki tugas dan tanggung jawab sebagai berikut :

a. mengkoordinasikan dan memantau proses pengelolaan dokumentasi terkait SMKI organisasi hal ini mencakup kebijakan dan prosedur terkait SMKI organisasi;

b. mengidentifikasi dan mendokumentasikan peraturan perundang-undangan dan kewajiban kontrak yang relevan dengan SMKI dan keamanan informasi organisasi;

c. melakukan pemantauan berkala terhadap kepatuhan SMKI organisasi dengan prasyarat dari kebijakan dan prosedur SMKI organisasi serta peraturan peraturan perundang-undangan dan kewajiban kontrak yang relevan dengan SMKI dan keamanan informasi organisasi;

d. menyusun dan mengkoordinasikan pelaksanaan program *security awareness* bagi personil organisasi;

e. menyusun metrik pengukuran efektivitas SMKI dan kontrol keamanan informasi organisasi.

10. Pengelolaan Data Center di lingkungan Pemerintah Provinsi Gorontalo harus ditetapkan dalam keputusan Gubernur yang berkekuatan hukum mengikat dalam Peraturan Gubernur ini.

11. Pengelola Data Center tersebut berkewajiban melakukan

pengamanan dan pemeliharaan berkelanjutan atas aset pengolahan serta penyimpanan informasi yang dikelola di *data center* dan aset informasi yang disimpan di *Data Center*.

12. Aset informasi yang merupakan isi (content) dari sistem informasi yang dimiliki oleh Perangkat Daerah, dikelola oleh Perangkat Daerah masing-masing sesuai kepemilikannya (*ownership*).
13. Penanggung jawab Pemilik Aset Informasi adalah Kepala Perangkat Daerah terkait. Pemilik Aset Informasi bertanggung jawab melakukan pengamanan dan pemeliharaan secara berkelanjutan atas aset informasi.
14. Perangkat Daerah harus menentukan tim keamanan informasi yang mempunyai tanggung jawab dalam berkoordinasi dengan pihak lain:
    a. Mengidentifikasi pihak-pihak berwenang terkait keamanan informasi pada tingkat pemerintahan yang lebih tinggi (GoProv-CSIRT, Gov-CSIRT, Kementerian Komunikasi dan Informatika, penegak hukum, *Indonesia security incident response team on internet infrastructure* (*idsirtii*) dan sebagainya) serta menjalin kerja sama dalam rangka pelaporan dan koordinasi penanganan bersama atas gangguan keamanan informasi;
    b. tim keamanan informasi wajib berpartisipasi dalam keanggotaan komunitas atau forum yang relevan terkait keamanan informasi sebagai sarana meningkatkan keterampilan dan pengetahuan serta best practice terkini atas keamanan informasi; dan
    c. seluruh anggota Tim Keamanan Informasi dan pihak ketiga wajib menandatangani Perjanjian Kerahasiaan (*Non-Disclosure Agreements*) yang mengikat para pihak untuk menjaga kerahasiaan aset informasi.

Kebijakan dalam penggunaan Perangkat *Mobile* dan *Teleworking*

1. Penggunaan perangkat *mobile*, baik milik pribadi atau milik Perangkat Daerah untuk mengakses dan/atau menyimpan informasi milik Perangkat Daerah harus sangat dibatasi sesuai dengan kebutuhan pekerjaan dengan mempertimbangkan prinsip
2. Perangkat *mobile* harus mengaktifkan fitur otentikasi pengguna, seperti penggunaan *user name dan password,* sesuai dengan kebijakan terkait pengendalian akses.
3. Informasi sensitif harus dienkripsi atau dilindungi dengan *password* pada saat disimpan di *mobile device*, sesuai dengan klasifikasi informasinya.
4. Informasi sensitif milik Perangkat Daerah yang disimpan pada perangkat *mobile device* harus di-*backup* secara berkala untuk menghindari hilangnya aspek ketersediaan dari informasi.
5. Aktivitas *teleworking* sebagai sarana pegawai untuk bekerja dari lokasi di luar area kerja Perangkat Daerah dengan mengakses jaringan internal secara *remote* melalui jaringan internet diperbolehkan namun sangat dibatasi hanya untuk personil yang diberi izin berdasarkan kebutuhan pekerjaannya.
6. Akses ke jaringan internal Perangkat Daerah dari jaringan internet harus menggunakan koneksi aman dengan menggunakan antara lain teknologi VPN.
7. Kebijakan terkait teknologi *teleworking* sebagai sarana pegawai bekerja pada lokasi di luar Perangkat Daerah dengan mengakses jaringan internal Perangkat Daerah. Teknologi ini diperbolehkan untuk digunakan dalam kondisi sebagai berikut:
   a. perangkat akses (misalnya computer, *notebook*) yang digunakan untuk *teleworking* harus terinstalasi *firewall* dan antivirus;
   b. mekanisme akses terhadap sistem atau aplikasi disesuaikan dengan klasifikasi aset informasi:
      1) informasi publik : dapat diakses langsung.
      2) informasi rahasia :
         - harus menggunakan protokol HTTPS atau SSH; dan

- harus menggunakan VPN, sebelum kemudian mengakses melalui protokol HTTPS atau SSH.

BAB V
KEAMANAN SUMBER DAYA MANUSIA

Kebijakan keamanan sumber daya manusia ditetapkan untuk memberikan pedoman dalam mengelola keamanan sumber daya manusia dalam ruang lingkup SMKI di Pemerintah Provinsi Gorontalo.

A. Ruang Lingkup

Ruang lingkup kebijakan keamanan sumber daya manusia terdiri dari:

1. pegawai dalam lingkungan Pemerintah Provinsi Gorontalo;
2. pegawai dari pihak eksternal yang dalam aktivitas pekerjaannya memiliki akses ke aset informasi dan aset pengolahan dan penyimpanan informasi dalam lingkungan Pemerintah Provinsi Gorontalo.

B. Kebijakan

1. Calon pegawai di lingkungan Pemerintah Provinsi Gorontalo dan pegawai dari pihak eksternal, harus melalui proses *screening* untuk memastikan bahwa mereka sesuai dengan tugas dan tanggung jawab yang akan mereka dapatkan.
2. Proses *screening* perlu mencakup verifikasi terhadap latar belakang kandidat sesuai dengan peraturan hukum perundang-undangan serta etika yang ada.
3. Pegawai dalam lingkungan Pemerintah Provinsi Gorontalo dan pegawai dari pihak eksternal yang dalam aktivitas pekerjaannya memiliki akses ke aset informasi dan aset pengolahan dan penyimpanan informasi dalam lingkungan Pemerintah Provinsi Gorontalo harus menandatangani perjanjian kerahasiaan (*non-disclosure agreement*) dengan memperhatikan tingkat sensitivitas dari aset yang diakses.
4. Setiap pegawai internal maupun eksternal harus mematuhi

seluruh kebijakan dan prosedur Perangkat Daerah terkait keamanan informasi.

5. Setiap pegawai internal maupun eksternal harus diberikan informasi yang memadai terkait tugas dan tanggung jawab terkait keamanan informasi yang mereka miliki.
6. Program peningkatan kesadaran keamanan informasi (*awareness*) secara berkelanjutan untuk menjaga dan meningkatkan kesadaran keamanan informasi dari pegawai harus dilaksanakan.
7. Setiap pelanggaran terhadap kebijakan dan prosedur terkait keamanan informasi harus ditindaklanjuti dan apabila diperlukan, tindakan pendisiplinan harus diambil sesuai dengan peraturan yang berlaku.
8. Tanggung jawab dan kewajiban terkait keamanan informasi yang tetap berlaku setelah pemberhentian atau perubahan status kepegawaian harus didefinisikan, dikomunikasikan dan ditegakkan kepada pegawai internal maupun eksternal.
9. Hal ini mencakup tanggung jawab keamanan informasi yang tercakup dalam perjanjian kerja seperti:
    a. Seluruh aset organisasi harus dikembalikan setelah pemberhentian kepegawaian;
    b. Seluruh hak akses organisasi harus dinonaktifkan ataudihapus setelah pemberhentian kepegawaian; dan
    c. Seluruh hak akses organisasi harus disesuaikan setelah perubahan status kepegawaian.

BAB VI

PENGELOLAAN ASET

A. Tujuan

Pengelolaan aset informasi bertujuan untuk memberikan pedoman dalam mengelola aset yang terkait informasi serta fasilitas fisik pengolahan informasi, sehingga aset informasi mendapatkan perlindungan yang sesuai dengan tingkat kepentingannya.

B. Ruang Lingkup

Ruang lingkup kebijakan terkait pengelolaan aset informasi terdiri dari:

1. klasifikasi, pelabelan dan penanganan informasi dalam ruang lingkup Peraturan Gubernur terkait SMKI; dan
2. penanganan aset pengolahan dan penyimpanan informasi dalam ruang lingkup Peraturan Gubernur .

C. Kebijakan

1. Kepala Dinas Komunikasi dan Informatika menetapkan pemilik aset informasi di setiap unit Perangkat Daerah, beserta perangkat fisik pengolah informasi yang terkait.
2. Pemilik aset informasi memiliki tanggung jawab untuk:
   a. mengidentifikasi seluruh aset informasi dan fasilitas pengolahan dan penyimpanan informasi;
   b. mendokumentasikannya dalam daftar inventaris aset SMKI, serta senantiasa memperbaharui daftar inventaris aset SMKI tersebut sesuai kondisi terkini; dan
   c. memastikan bahwa setiap aset telah diklasifikasikan dan dilindungi secara memadai.
3. Aset pengolahan dan penyimpanan informasi yang diinventaris adalah aset dalam bentuk:
   a. perangkat keras, meliputi perangkat keras yang digunakan untuk mengolah dan menyimpan informasi dalam bentuk fisik

maupun elektronik, yang mencakup namun tidak terbatas pada komputer, *notebook, server, harddisk drive,* USB *disk*;

b. perangkat lunak, meliputi perangkat lunak yang digunakan untuk mengolah informasi dalam bentuk elektronik, yang mencakup namun tidak terbatas pada sistem operasi, aplikasi, dan *database*;

c. perangkat jaringan, meliputi perangkat keras dan lunak yang digunakan untuk membentuk dan infrastruktur jaringan telekomunikasi, yang mencakup namun tidak terbatas pada *hub, switch, router, firewall,* IDS, IPS, dan *network monitoring tools*;

d. perangkat pendukung meliputi perangkat digunakan untuk mendukung operasional perangkat pengolahan dan penyimpanan informasi yang mencakup namun tidak terbatas pada *genset,* UPS, AC, rak *server,* lemari penyimpanan informasi dan CCTV;

e. layanan, meliputi layanan yang digunakan untuk mendukung operasional perangkat pengolahan dan penyimpanan informasi yang mencakup namun tidak terbatas pada layanan jaringan komunikasi, layanan *hosting* dan *co-location,* layanan pemeliharaan perangkat dan sistem, dan layanan pemasangan infrastruktur; dan

f. sumber daya manusia meliputi personil baik internal maupun eksternal yang terlibat dalam pengolahan dan penyimpanan informasi.

4. Pemilik aset dapat mendelegasikan tugas pengamanan dan pemeliharaan aset kepada kustodian aset, namun tanggung jawab akhir terhadap aset tetap berada pada pemilik aset.
5. Aset pengolahan dan penyimpanan informasi harus secara berkala dipelihara dengan memadai.
6. Apabila dalam pemeliharaan aset pengolahan dan penyimpanan informasi tersebut harus menggunakan jasa pihak ketiga

penyedia, maka:

a. kontrak pemeliharaan perlu dibuat dengan pihak ketiga penyedia jasa yang kompeten dan relevan; dan
b. peralatan yang dibawa keluar untuk pemeliharaan harus diperiksa untuk mencegah kebocoran informasi.

7. dalam proses penghapusan aset harus dilakukan secara aman dengan metode yang dapat mencegah kebocoran informasi seperti menghancurkan secara fisik harddisk drive.
8. Semua aset informasi dan pengolahan dan penyimpanan informasi milik Pemerintah Provinsi Gorontalo harus dikembalikan setelah personil pengguna tidak memiliki hubungan kepegawaian lagi dengan Pemerintah Provinsi Gorontalo, misalnya karena pengunduran diri, pensiun.
9. Ketentuan dalam proses pengembalian aset tersebut mencakup:
   a. pengembalian aset harus terdokumentasi secara formal;
   b. untuk pengembalian aset yang disebabkan oleh terhentinya status kepegawaian, informasi yang tersimpan dalam aset harus di-backup dan informasi yang tersimpan dalam aset harus dihapus secara aman, antara lain dengan secure format atau melakukan instalasi ulang sistem operasi secara menyeluruh; dan
   c. media penyimpanan backup informasi harus diamankan secara fisik, antara lain dengan menyimpan dalam lemari terkunci dengan akses yang terbatas.
10. Aset pengolahan informasi, seperti komputer dan laptop yang akan digunakan kembali baik oleh pihak internal maupun eksternal harus diperiksa untuk menjamin tidak ada informasi sensitif yang tersimpan dalam aset tersebut.
11. Perangkat Daerah harus mendefinisikan klasifikasi aset informasi dengan mempertimbangkan sebagai berikut:
    a. Aset informasi diklasifikasikan berdasarkan tingkat sensitivitas informasi serta tingkat kritikalitas sistem, yang meliputi:

1) klasifikasi aset informasi secara berkala; dan
2) pengguna yang diijinkan mengakses aset informasi.

b. pemberian label klasifikasi informasi harus dilakukan secara konsisten terhadap seluruh aset informasi;

c. klasifikasi aset informasi dan seberapa tingkat kerahasiaan aset informasi, didefinisikan sesuai ketentuan peraturan perundang-undangan, diuraikan sesuai tabel berikut:

Klasifikasi AsetInformasi	Deskripsi
Rahasia *(Confidential)*	Aset informasi yang sangat peka dan berisiko tinggi yang pembocoran atau penyalahgunaan akses terhadapnya bisa mengganggu kelancaran oeprasional secara temporer atau mengganggu citra dan reputasi instansi.
Internal*(Internal Use Only)*	Informasi yang telah terdistribusi secara luas di lingkungan internal instansi/lembaga yang penyebarannya secara internal tidak lagi memerlukan izin dari pemilik informasi dan risiko penyebarannya tidak menimbulkan kerugian signifikan.
Publik	Aset informasi yang secara sengaja dipublikasikan secara luas, merupakan informasi yang wajib disediakan dan diumumkan secara berkala, informasi yang wajib diumumkan secara serta-merta, dan informasi yang wajib tersedia setiap saat.

12. Untuk kepentingan penyelenggaraan pengelolaan aset informasi dalam Kebijakan Sistem Manajemen Keamanan Informasi perlu diberikan penjelasan contoh-contoh aset informasi rahasia dan internal, yaitu:

Klasifikasi Aset Informasi	Contoh
Rahasia *(Confidential)*	*User ID, password, Personal Identification Number (PIN), Log* sistem, hasil *penetration test,* data konfigurasi sistem, *Internet Protocol Address* (IP *Address*)
Internal *(Internal Use Only)*	Panduan penggunaan sistem dan aplikasi, kebijakan dan prosedur SMKI, dokumen *Business Continuity Plan.*

13. Setiap pemilik informasi harus memperhatikan keamanan informasi yang tersimpan dalam media penyimpanan informasi antara lain:
    a. dalam hal data yang tersimpan di dalam media bersifat rahasia, perlu diberikan proteksi kata sandi untuk melindungi data;
    b. dalam hal tidak lagi dibutuhkan atau digunakan, seluruh data yang tersimpan di dalam media harus sepenuhnya dihapus sehingga tidak lagi dapat dipulihkan;
    c. data yang tersimpan di dalam media yang akan dibuang harus mendapatkan perlakuan khusus guna meminimalkan terjadinya kebocoran informasi kepada pihak yang tidak sah, yaitu:
        1) data yang tersimpan di dalam media yang memuat informasi rahasia harus dibuang dengan cara dihancurkan atau dibakar; dan
        2) data yang tersimpan di dalam media yang memuat informasi lainnya harus dilakukan penghapusan total dengan cara-cara tertentu yang tidak lagi dapat dipulihkan.
14. Panduan terkait pelabelan dan penanganan aset informasi berdasarkan klasifikasi aset informasi adalah sebagai berikut:

Klasifik	Publik	Internal	Rahasia
Dokumen dan catatan (*record*) dalam bentuk	Tidak diperlukan penanganan khusus.	Diberi label ***"Internal"***.	Diberi label "***Rahasia***"
Map penyimpan dokumen.	Tidak diperlukan penanganan khusus.	Tidak diperlukan penanganan khusus.	Diberi label "***Rahasia***"
Amplop pengiriman surat internal (di dalam kantor).	Tidak diperlukan penanganan khusus.	Tidak diperlukan penanganan khusus.	Amplop diberi label "***Rahasia***"

Amplop untuk surat eksternal (ke luar kantor).	Tidak diperlukan penanganan khusus.	• Pada amplop ditandai *"Internal"*	• Menggunakan 2 amplop, dimana amplop pertama dimasukkan kedalam amplop kedua; • Pada amplop pertama ditandai "Rahasia", dan pada amplop kedua tidak diberikan tanda apapun.
Dokumen dan catatan (*record*) dalam bentuk elektronik (*softcopy*).	Tidak diperlukan penanganan khusus.	Memberikan label "Internal" pada bagian awal dari nama *file* atau pada bagian tertentu dari *file properties*.	Memberikan label "Rahasia" pada bagian awal dari nama *file* atau pada bagian tertentu dari *file properties*.
Publikasi/ Distribusi	Tidak ada pembatasan.	• Tersedia untuk personil internal Perangkat Daerah pemilik informasi. • Distribusi kepada pihak eksternal dibatasi berdasakan kebutuhan pekerjaan maupun operasional di lingkungan Pemerintah Daerah Provinsi Gorontalo. • Distribusi kepada pihak eksternal perlu seijin pemilik informasi. • Sensitifitas dan kritikalitas informasi perlu diberitahukan kepada pihak eksternal.	• Distribusi kepada pihak eksternal sangat dibatasi untuk kebutuhan pekerjaan. • Apabila memungkinkan, informasi rahasia tidak disalin oleh pihak eksternal (*eyes only*). • Distribusi kepada pihak eksternal perlu seijin pemilik Informasi. • Sensitifitas dan kritikalitas informasi perlu diberitahukan kepada pihak eksternal. • Pihak ketiga harus disertai perjanjian kerahasiaan (NDA - *non disclosure agreement*).
Pencetakan informasi	Tidak ada pembatasan.	Dibatasi hanya untuk kebutuhan internal.	• Pencetakan hanya pada *printer* organisasi dan diusahakan tidak mencetak menggunaka n jasa pencetakan eksternal.

Surat menyurat internal (di dalam kantor)	Pastikan nama dan alamat tujuan sudah benar.	• Pastikan nama dan alamat tujuan sudah benar. • Mengikuti ketentuan penggunaan amplop untuk surat internal.	• Pastikan nama dan alamat tujuan sudah benar. • Mengikuti ketentuan penggunaan amplop untuk surat internal. • Menginformasikan kepada penerima akan pengiriman informasi tersebut. • Mengkonfirm asi kepada penerima bahwa informasi yang dikirim sudah diterima.

Surat menyurat eksternal (ke luar kantor)	Pastikan nama dan alamat tujuan sudah benar.	• Pastikan nama dan alamat tujuan sudah benar. • Mengikuti ketentuan penggunaan amplop untuk surat eksternal. • Menggunakan jasa kurir pengiriman tercatat dengan tanda pengiriman	• Pastikan nama dan alamat tujuan sudah benar. • Mengikuti ketentuan penggunaan amplop untuk surat eksternal. • Menggunakan jasa kurir pengiriman tercatat dengan tanda pengiriman. • Menginformasikan kepada penerima akan pengiriman informasi tersebut. • Mengkonfirmasi kepada penerima bahwa informasi yang dikirim sudah diterima.
Pengiriman ke pihak internal melalui *email*	• Pengiriman e-mail harus meng-gunakan *account* e-mail Perangkat Daerah • Tidak diperlukan penanganan khusus.	• Pengiriman e-mail harus mengguna-kan account e-mail Perangkat Daerah • Pastikan alamat email tujuan sudah benar. • Pengiriman informasi, termasuk forwarding/ meneruskan email hanya boleh dilakukan oleh pemilik informasi	• Pengiriman e-mail harus menggunakan account e-mail Perangkat Daerah • Memberi *password* pada informasi yang dikirim melalui email dan password diinformasikan kepada penerima secara terpisah • Tidak mencantumkan informasi rahasia di *body text* e- mail • Pengiriman informasi, termasuk *forwarding/* meneruskan *email* hanya boleh dilakukan oleh pemilik informasi

Pengiriman ke pihak eksternal melalui *email*	• Pengiriman e-mail harus menggunakan *account* e- mail Perangkat Daerah • Tidak diperlukan penanganan khusus.	• Pengiriman e-mail harus menggunakan account e-mail Perangkat Daerah • Pastikan alamat email tujuan sudah benar.	• Tidak disarankan menggunakan e-mail untuk mengirim informasi dengan klasifikasi ini. • Pengiriman e-mail harus menggunakan *account* e-mail Perangkat Daerah • Pastikan alamat email tujuan sudah benar. • Memberi *password* pada informasi yang dikirim melalui email dan password diinformasika n kepada penerima secara terpisah
Penyimpanan informasi *hardcopy*	Tidak diperlukan penanganan khusus	Tidak diperlukan penanganan khusus	Disimpan secara aman dalam tempat penyimpanan yang terkunci.
Penyimpa nan informasi *softcopy*	Tidak diperlukan penanganan khusus	Tidak diperlukan penanganan khusus	• Penyimpanan pada komputer atau media penyimpanan harus yang menggunakan *password*. • *File* yang disimpan harus diberi *password*. • Media penyimpanan eksternal (*externalhard disk,* atau *flashdisk*) harus disimpan pada tempat penyimpanan yang terkunci.

Penyimpanan pada pihak ketiga	Tidak diperlukan penanganan khusus	Harus disertai dengan perjanjian kerahasiaan (*non disclosure agreement* - NDA).	Harus disertai dengan perjanjian kerahasiaan (*non disclosure agreement* - NDA).
Penghancuran (*disposal*)	• Tidak diperlukan penanganan khusus. • Masih dapat digunakan kembali sebagai kertas untuk pekerjaan (*scrap paper*).	• Memperhatikan masa retensi informasi yang disetujui oleh pemilik informasi. • Masih dapat digunakan kembali untuk kebutuhan mencetak informasi dengan klasifikasi yang sama.	• Memperhatikan masa retensi informasi yang disetujui oleh pemilik informasi • Dihancurkan dengan metode pemusnahan dan informasi tidak dapat diakses kembali (dihancurkan secara fisik atau *secure format*).
Pengamanan pada komputer penyimpan informasi	Tidak diperlukan penanganan khusus.	• *Screen saverlock* harus aktif jika meninggalkan komputer / terminal. • *Sign-off* komputer/ terminal jika tidak digunakan atau pulang kerja	• *Screen saverlock* harus aktif jika meninggalkan komputer/ terminal. • *Sign-off* komputer/ terminal jika tidak digunakan atau pulang kerja. • *File perlu* dienkripsi/ *password*.

Kehilangan atau kebocoran informasi	Tidak diperlukan penanganan khusus.	Harus dilaporkan kepada pemilik informasi	Harus dilaporkan kepada pemilik informasi dan unit kerja pengelola insiden keamanan informasi di lingkungan Pemerintah Provinsi Gorontalo

15. informasi yang dianggap kritikal oleh Perangkat Daerah harus di-*backup* secara memadai untuk menjamin ketersediaannya.
16. hal yang perlu dipertimbangkan dalam proses backup informasi meliputi:
    a. pemilik informasi bertanggung jawab untuk menentukan informasi yang membutuhkan *backup*, frekuensi dan metode *backup* serta waktu retensi untuk setiap *backup* informasi yang ada;
    b. pernyataan formal terkait informasi yang dibutuhkan untuk di-*backup* beserta metode dan frekuensi dari *backup* harus ditentukan bersama dengan personil yang bertugas melaksanakan proses *backup* serta harus dinyatakan secara jelas dalam sebuah rencana *backup* resmi;
    c. *backup* informasi harus disimpan sesuai dengan masa retensi dari informasi utama;
    d. masa retensi harus dinyatakan secara jelas dalam rencana *backup*; dan
    e. perlindungan terhadap *backup* informasi harus dilakukan berdasarkan klasifikasi dari informasi utama.
17. Perangkat Daerah menyediakan akses *internet* dan *email* kepada pegawainya hanya untuk kebutuhan pekerjaan dan operasional Pemerintah Provinsi Gorontalo.
18. Ketentuan dalam pengguaan internet dan email adalah sebagai berikut:

a. pengguna dilarang menggunakan akses internet dan *email* Perangkat Daerah untuk kegiatan melanggar hukum dan aktifitas yang dapat membahayakan keamanan jaringan Pemerintah Provinsi Gorontalo;
b. pengguna dilarang untuk menggunakan akses internet dan *email* Perangkat Daerah untuk mengakses, mendistribusikan, mengunggah dan/atau mengunduh:
    1) materi pornografi;
    2) materi bajakan seperti, perangkat lunak, *file* musik dan *video/film*;
    3) materi yang melecehkan, mendiskriminasikan, yang membakar emosi atau menimbulkan kebencian atau membuat pernyataan palsu atau yang bersifat merusak mengenai orang lain;
    4) situs yang dapat menimbulkan risiko serangan malware, penyusupan atau *hacking* ke jaringan Pemerintah Provinsi Gorontalo.

19. pengguna disarankan untuk tidak membagi informasi pribadi melalui situs internet atau media sosial.
20. pengguna dilarang untuk mendistribusikan informasi Pemerintah Provinsi Gorontalo yang bersifat rahasia tanpa izin dari pemilik informasi.
21. pesan penyangkalan ini harus dituliskan pada akhir setiap e-mail. "*Pesan ini mungkin berisi informasi rahasia dan hanya ditujukan kepada pihak yang dituju. Apabila anda bukanlah pihak yang dituju, anda dilarang untuk mengungkapkan, menyebarkan atau menyalin isi email ini. Apabila anda mendapatkan email ini tanpa sengaja mohon segera hubungi pengirim email dan hapus email ini segera. Pemerintah Provinsi Gorontalo tidak bertanggung jawab untuk pengiriman informasi ini secara lengkap dan tepat dan juga tidak bertanggung jawab untuk keterlambatan dalam pengiriman email ini.*"
22. unit kerja yang mengelola akun *email* Perangkat Daerah berhak

untuk mem- *block* akun *email* Pemerintah Provinsi Gorontalo pada saat terdapat bukti memadai terkait penyalahgunaan dan/atau pelanggaran keamanan.

BAB VII

PENGENDALIAN AKSES

A. Tujuan

Tujuan dari pengendalian akses adalah untuk:

1. membatasi akses terhadap informasi serta fasilitas fisik (data center);
2. memastikan sistem dan aplikasi diakses oleh pengguna yang telah diotorisasi, serta mencegah akses oleh yang tidak berhak; dan
3. memastikan pengguna bertanggung jawab untuk melindungi informasi otentikasi sensitif masing-masing.

B. Ruang Lingkup

Ruang Lingkup dari pengendalian akses adalah akses ke aset informasi dan aset pengolahan dan penyimpanan informasi dalam lingkungan Pemerintah Provinsi Gorontalo yang mencakup :

1. persyaratan pengendalian akses;
2. pengendalian akses jaringan;
3. pengelolaan akses pengguna;
4. tanggung jawab pengguna; dan
5. pengendalian akses atas sistem dan aplikasi.

C. Kebijakan

1. Persyaratan pengendalian akses pada suatu sistem meliputi:
   a. akses ke aset informasi serta aset pengolahan dan penyimpanan informasi dalam lingkungan Pemerintah Provinsi Gorontalo harus dikendalikan menggunakan metode pengendalian akses yang memadai;
   b. pemberian hak akses dikelola secara formal pada seluruh siklusnya, mulai dari proses pengajuan, persetujuan serta pencabutan, serta dilaksanakan oleh para pihak terkait sesuai

jenjang kewenangannya;

c. pengguna yang mengakses sistem informasi dalam lingkungan Pemerintah Provinsi Gorontalo diharuskan untuk mengotentikasi dirinya dengan menggunakan kombinasi *user* ID dan informasi otentikasi pribadi seperti *password* atau PIN;

d. pengembangan aturan pemberian akses perlu mempertimbangkan:
   1) klasifikasi dari informasi;
   2) kritikalitas dari aset yang digunakan untuk mendukung operasional bisnis;
   3) prasyarat hukum perundang-undangan, kontraktual serta keamanan yang relevan;
   4) didasarkan atas prinsip *need to know* dan *need to use*, yaitu disesuaikan dengan kebutuhan pekerjaan dan operasional dalam lingkungan Pemerintah Provinsi Gorontalo;

e. aturan pemberian akses harus dikembangkan dan didokumentasikan oleh setiap pemilik sistem dalam bentuk daftar atau matriks akses;

f. peninjauan terhadap aturan pemberian akses harus dilakukan oleh pemilik aset/sistem secara berkala tergantung tingkat kritikalitas sistem tersebut;

g. peninjauan terhadap hak akses pengguna harus didokumentasikan secara formal; dan

h. setiap penyimpangan yang ditemukan dalam proses peninjauan harus segera diperbaiki dengan cara menyesuaikan atau mencabut hak akses yang menyimpang.

2. pengendalian akses jaringan di lingkungan Perangkat Daerah meliputi:
   a. penggunaan layanan jaringan (*network services*) hanya diperbolehkan secara terbatas, sesuai kebutuhan ketugasan dan kepentingan Perangkat Daerah, layanan lainnya yang tidak diperlukan harus dinonaktifkan;
   b. jaringan komunikasi dalam lingkungan Perangkat Daerah harus

dipisahkan kedalam *domain* jaringan yang terpisah sesuai dengan kebutuhan bisnis dan operasional, dalam rangka untuk mengamankan jaringan internal Perangkat Daerah dan aset di jaringan tersebut;

c. akses secara *remote* ke jaringan internal Perangkat Daerah dari jaringan publik harus sangat dibatasi baik dari perangkat yang digunakan maupun waktu untuk kebutuhan *troubleshooting* dan harus dilakukan melalui *secure channel*, antara lain dengan menggunakan teknologi VPN; dan

d. pemberian akses pengguna terhadap jaringan, baik LAN maupun WAN, dilakukan melalui mekanisme formal.

3. pengelolaan akses terhadap pengguna di Perangkat Daerah harus memenuhi ketentuan sebagai berikut:

   a. pemilik Aset Informasi harus memiliki manajemen identitas pengguna yang mencakup proses pendaftaran dan terminasi pengguna, yang didalamnya termasuk:

      1) identitas pengguna (*user account*) harus unik, melekat ke setiap individu tunggal, sehingga setiap tindakan pengguna dapat dipertanggung jawabkan;

      2) tidak diijinkan menggunakan satu identitas pengguna yang digunakan secara bersama-sama oleh lebih dari satu individu, kecuali untuk tujuan tertentu yang sebelumnya harus mendapatkan persetujuan dari pihak berwenang; dan

      3) memastikan secara berkala bahwa tidak ada identitas pengguna yang terduplikasi atau redundan sehingga seluruh identitas pengguna aktif adalah sesuai dengan pegawai Perangkat Daerah aktif.

   b. pendaftaran, modifikasi dan pencabutan hak akses pengguna mencakup proses pembuatan *user* ID, memberikan hak akses kepada *user* ID serta mencabut hak akses dan *user* ID.

   c. pendaftaran, modifikasi dan pencabutan hak akses pengguna harus disetujui oleh atasan dari pengguna yang memohon hak

akses tersebut dan pemilik informasi dan/atau sistem. Persetujuan tersebut harus diberikan sesuai dengan aturan pemberian akses.

d. identitas pengguna harus diotorisasi secara formal oleh pejabat berwenang pada pemilik aset informasi. Akses atas sistem dan aplikasi hanya dapat diaktifkan jika proses otorisasi telah selesai.

e. identitas pengguna pada sistem, seperti *user* ID, harus bersifat unik untuk memungkinkan mengidentifikasi dan meminta pertanggungjawaban pengguna.

f. pemberian informasi otentikasi suatu pengguna yang bersifat rahasia harus dilakukan melalui proses formal yang mencakup:
   1) informasi otentikasi perdana yang diberikan untuk pertama kalinya adalah bersifat sementara, dimana pengguna wajib menggantinya pada kesempatan pertama mengakses sistem atau aplikasi;
   2) informasi otentikasi bawaan (*default*) dari penyedia barang/jasa harus segera diganti pada saat instalasi sistem atau aplikasi;

g. pemilik Aset harus melakukan tinjauan secara berkala atas seluruh hak akses pengguna secara berkala, dengan tambahan tinjauan insidental yang dilakukan pada saat:
   1) terjadinya proses kepegawaian, seperti promosi, mutasi, terminasi; dan
   2) terjadinya perubahan struktur organisasi.

h. hak akses khusus (*privileged access rights*) dari sistem informasi dalam lingkungan Perangkat Daerah, seperti *administrator, root,* hak akses untuk memodifikasi *database* atau hak akses untuk membuat, memodifikasi atau mencabut pengguna dalam sistem aplikasi, harus sangat dibatasi kepada personil yang terotorisasi.

i. hak akses khusus harus disetujui dan didokumentasikan

secara formal.

j. alokasi dari hak akses khusus harus ditinjau secara berkala dan setiap terdapat perubahan dalam status penggunaan akses tersebut.

k. setiap penyimpangan yang ditemukan dalam proses peninjauan harus segera diperbaiki dengan menyesuaikan atau menghapus hak akses khusus yang menyimpang.

l. apabila memungkinkan, hak akses khusus harus dialokasikan secara individual dan tidak di-*share*. Hal ini dilakukan untuk menjamin akuntabilitas dari pengguna khusus.

m. apabila hak akses khusus tidak bisa dialokasikan secara individual, kontrol tambahan seperti *dual custody,* harus diimplementasikan untuk menghindari penyalahgunaan.

n. jejak audit (*log*) untuk hak akses khusus pada sistem informasi dalam lingkungan Pemerintah Provinsi Gorontalo harus diaktifkan.

4. Setiap pengguna harus mempunyai tanggung jawab dalam penggunaan *User ID* dan *password* yaitu:

   a. pengguna harus menjaga kerahasiaan dan keamanan *password* pribadi atau kelompok serta informasi otentikasi rahasia lainnya;

   b. pengguna harus segera mengganti informasi otentikasi rahasia jika terindikasi bahwa informasi tersebut telah diketahui oleh orang lain;

   c. *password* yang diberikan untuk pertama kalinya adalah bersifat sementara, dimana pengguna wajib menggantinya pada kesempatan pertama pada saat mengakses sistem atau aplikasi;

   d. *password* untuk mengakses sistem informasi dalam lingkungan Perangkat Daerah harus memiliki karakteristik sebagai berikut:

      1) memiliki panjang minimum 8 karakter;

      2) mengandung kombinasi huruf kecil, minimal 1 huruf besar,

minimal 1 angka dan minimal 1 karakter simbol; tidak terdiri dari kata atau nomor yang mudah ditebak seperti password, admin, 12345678 atau abc123; dan

3) tidak terdiri dari informasi pribadi seperti ulang tahun pengguna, nama Dinas atau nama pengguna;

e. *password* untuk mengakses sistem informasi dalam lingkungan Pemerintah Provinsi Gorontalo harus diganti paling sedikit setiap 3 (tiga) bulan sekali;

f. pada saat penggantian, *password* sebelumnya tidak boleh digunakan kembali sampai setelah 3 siklus pergantian *password*;

g. prosedur *login* dari sistem harus menjamin keamanan dari *password* dengan

cara:

1) tidak menampilkan password yang dimasukkan;

2) tidak menyediakan pesan bantuan pada saat proses *login* yang dapat membantu pengguna yang tidak berwenang;

h. pengguna wajib menggunakan kata sandi yang berbeda untuk keperluan ketugasan dan pribadi

5. Pengendalian akses sistem dan aplikasi yang dikelola oleh Perangkat Daerah meliputi:

a. pemilik aset informasi harus memastikan bahwa sistem dan aplikasi dibawah pengelolaannya memiliki fasilitas manajemen hak akses pengguna, manajemen kata sandi yang baik, serta mekanisme otentikasi pengguna yang aman;

b. fasilitas manajemen hak akses pengguna harus mampu membatasi akses informasi sesuai ketugasannya (*role based access control*);

c. fasilitas manajemen kata sandi harus memastikan dihasilkannya kata sandi yang berkualitas, yaitu:

1) menegakkan akuntabilitas pengguna melalui penggunaan identitas pengguna tunggal untuk setiap individu;

2) memberikan fasilitas penggantian kata sandi mandiri;
3) membantu memberikan rekomendasi kata sandi yang berkualitas;
4) mewajibkan pengguna untuk mengganti kata sandi pada saat pertama kali login;
5) mewajibkan pengguna untuk mengganti kata sandi secara berkala;
6) menyimpan riwayat kata sandi pengguna dan mencegah agar pengguna tidak menggunakan kata sandi yang sebelumnya telah digunakan;
7) tidak menampilkan kata sandi saat sedang dientrikan; dan
8) kata sandi disimpan dalam bentuk terlindungi (dienkripsi), demikian juga pada saat kata sandi ditransmisikan.

d. Mekanisme otentikasi pengguna perlu dirancang agar meminimalkan peluang terjadinya akses yang tidak sah, yaitu:
1) kata sandi tidak ditransmisikan melalui jaringan secara *plaintext*;
2) memiliki mekanisme penguncian sistem sementara sebagai perlindungan terhadap *brute force attacks*;
3) adanya pencatatan terhadap seluruh upaya otentikasi yang sukses dan gagal;
4) adanya pembatasan jumlah akses pengguna yang sama secara simultan;

e. Parameter otentikasi pengguna disesuaikan dengan klasifikasi aset informasi sebagai berikut:

Parameter Otentikasi	Rahasia & Internal	Publik
Jumlah gagal *login* sebelum penguncian	3	10
Durasi *timeout* sebelum terminasi sesi otomatis	5 menit	16 menit

6. penggunaan program *utility khusus* dalam operasional sistem di lingkungan Perangkat Daerah harus mempertimbangkan

keamanan sebagai berikut yaitu penggunaan program *utility* khusus seperti *registry cleaner* atau *system monitoring* yang dapat mengambil alih kendali sistem/aplikasi atau mendapatkan hak akses khusus pada sistem/aplikasi harus sangat dibatasi berdasarkan kebutuhan operasional pengguna.

7. Perangkat Daerah yang mengelola aplikasi harus memastikan bahwa *source code* dikelola dan disimpan secara memadai baik yang dikembangkan oleh internal Perangkat Daerah maupun yang dikembangkan oleh penyedia jasa aplikasi.
8. Apabila *source code* dari penyedia jasa aplikasi tidak dapat diserahkan kepada pengelola aplikasi, Perangkat Daerah bersama penyedia jasa aplikasi tersebut harus mempertimbangkan *escrow aggreeement* untuk memastikan kelangsungan operasional sistem aplikasi jika ada pengembangan selanjutnya.
9. Pengendalian terhadap akses ke *source code* aplikasi sebagai berikut:
    a. Untuk sistem aplikasi yang dikembangkan secara internal dan/atau dibeli dengan *source code*, pengendalian akses harus diimplementasikan untuk mencegah akses tanpa izin ke *source code* tersebut.
    b. Pengendalian tersebut mencakup:
        1) Tidak menyimpan *source code* pada sistem operasional;
        2) Menyimpan *source code* pada lokasi fisik yang aman dari ancaman akses tanpa izin maupun ancaman kerusakan karena kondisi lingkungan;
        3) Membatasi akses secara fisik maupun logical ke *source code* program hanya kepada pengembang dan personil yang berwenang;
        4) Mengimplementasikan metode *versioning* dan proses manajemen perubahan untuk menjamin integritas dari *source code* aplikasi.
10. Pengendalian terhadap publikasi data pribadi sebagai berikut :

Data pribadi seperti Nomor Induk Kependudukan (NIK), nomor Kartu Keluarga (KK), tanggal lahir, tempat lahir, nama ibu kandung, nama istri dan nama anak tidak dipublikasikan ke publik tanpa authentikasi ke dalam aplikasi (login)

BAB VIII
KRIPTOGRAFI

A. Tujuan

Tujuan dari kebijakan terkait teknologi kriptografi adalah untuk memastikan penggunaan teknologi kriptograpi yang sesuai dan efektif untuk melindungi kerahasiaan, keaslian dan/atau integritas dari informasi dalam lingkungan Pemerintah Provinsi Gorontalo.

B. Ruang Lingkup

Ruang Lingkup kebijakan terkait teknologi kriptografi adalah penggunaan teknologi kriptografi dalam pengolahan dan penyimpanan informasi di lingkungan Pemerintah Provinsi Gorontalo.

C. Kebijakan

1. kontrol kriptografi dapat digunakan untuk menjamin kerahasiaan dan integritas dari informasi sensitif di lingkungan Perangkat Daerah.
2. kontrol kriptografi dapat mencakup namun tidak terbatas pada:
   a. enkripsi informasi dan jaringan komunikasi;
   b. pemeriksaan integritas informasi, seperti hashing;
   c. otentikasi identitas;
   d. digital *signatures;*
3. implementasi dari kontrol kriptografi harus mempertimbangkan klasifikasi dari informasi yang akan diamankan.
4. pemilihan kontrol kriptografi harus mempertimbangkan:
   a. jenis dari kontrol kriptografi;
   b. kekuatan dari algoritma kriptografi; dan
   c. panjang dari kunci kriptografi.
5. implementasi dari kontrol kriptografi harus secara berkala ditinjau untuk memastikan kecukupan dan kesesuaian dari kontrol tersebut dalam mengamankan kerahasiaan dan integritas dari

informasi.

6. pengelolaan dari kunci kriptografi harus dikendalikan secara ketat dan dibatasi hanya pada personil yang terotorisasi.
7. pengelolaan dari kunci kriptografi didasarkan pada prinsip *dual custody* untuk mengurangi risiko penyalahgunaan.

BAB IX
KEAMANAN FISIK DAN LINGKUNGAN

A. Tujuan

Tujuan dari kebijakan keamanan fisik dan lingkungan adalah untuk:

1. Mencegah akses atas aset informasi dan aset pengolahan dan penyimpanan informasi secara fisik oleh pihak yang tidak berwenang pada lingkungan Pemerintah Provinsi Gorontalo; dan
2. Mencegah terjadinya kerusakan atau gangguan pada aset informasi dan aset pengolahan dan penyimpanan informasi pada lingkungan Pemerintah Provinsi Gorontalo karena ancaman dari kondisi lingkungan.

B. Ruang Lingkup

Ruang lingkup kebijakan keamanan fisik dan lingkungan adalah pengamanan fisik dan lingkungan bagi area kerja dan penyimpanan perangkat pengolahan dan penyimpanan informasi, seperti *data center, disaster recovery center* atau ruang arsip.

C. Kebijakan

1. Setiap area yang didalamnya terdapat informasi dan fasilitas pengolahan informasi Perangkat Daerah harus dilindungi dengan menerapkan pengamanan fisik pada perimeter area tersebut.
2. Setiap area harus merupakan akses terbatas, dimana akses masuk hanya diberikan bagi personil yang telah mendapatkan otorisasi. Mekanisme pembatasan ini dapat dilakukan aturan penerimaan tamu yang diterapkan berdasarkan kritikalitas area tersebut.
3. Untuk area *Data center, disaster recovery center* dan ruang arsip Perangkat Daerah harus dilindungi dengan menerapkan pengamanan fisik pada perimeter area tersebut dengan kriteria:
   a. konstruksi dinding, atap dan lantai yang kuat;

b. pintu akses menuju area harus dilengkapi dengan mekanisme kontrol akses, seperti: *access door lock*;
c. pintu dan jendela harus senantiasa dalam kondisi terkunci, khususnya pada saat tanpa penjagaan;
d. perangkat CCTV perlu terpasang pada sisi eksterior dan interior area;
e. tidak diperbolehkan menyimpan bahan-bahan berbahaya yang mudah terbakar;
f. area bongkar muat atau penerimaan barang harus diamankan dan dipantau untuk mencegah akses tanpa izin ke *data center, disaster recovery center* dan ruang arsip Pemerintah Provinsi Gorontalo; dan
g. *delivery* dari barang harus dilaporkan dan diperiksa sebelum barang tersebut dapat dipindahkan dari area bongkar muat atau penerimaan barang ke *data center, disaster recovery center* dan ruang arsip Pemerintah Provinsi Gorontalo.

4. Pengendalian akses pengunjung ke dalam area di lingkungan Perangkat Daerah harus memperhatikan keamanan fisik yang meliputi:
   a. kunjungan ke dalam area tersebut harus disetujui secara formal oleh pengelolaan area tersebut;
   b. selama kunjungan di dalam area tersebut, pengunjung harus senantiasa didampingi oleh petugas yang telah mendapatkan otorisasi;
   c. kartu identitas pengunjung perlu diverifikasi, disimpan oleh petugas selama kunjungan, dan dikembalikan sesudah selesai kunjungan; dan
   d. setiap pengunjung ke dalam area harus tercatat, mencakup jam masuk dan keluar, serta selalu dimonitor kesesuaiannya dengan rekaman CCTV.
5. Perangkat Daerah harus memperhatikan aspek pengamanan terhadap perangkat yang digunakan melalui:

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

6. Khusus pengamana area fisik di *data center* harus mempertimbangkan hal-hal sebagai berikut:
   a. seluruh perangkat harus ditempatkan di lokasi yang aman, sedemikian rupa sehingga terlindungi dari terjadinya kebakaran, kebocoran, debu, dan sebagainya;
   b. seluruh perangkat di dalam *data center* harus dipelihara, diinspeksi sesuai spesifikasi perawatan berkala oleh pihak yang kompeten dan berwenang sesuai dengan rekomendasi dari pembuat perangkat tersebut;

c. *data center* harus dilengkapi dengan ups, generator listrik cadangan, perangkat pemadam kebakaran, dan diusahakan terdapat perlindungan kejut listrik (petir, tegangan tidak stabil);
d. *data center* dan *disaster recovery center* dilengkapi dengan sistem sensor deteksi asap, air, suhu dan kelembaban, yang dapat terpantau;
e. parameter temperatur dan kelembaban berikut perlu dijaga untuk *data center* meliputi:
   1) temperatur antara 18° - 26° celcius;
   2) kelembaban (rh) antara 40% - 60%.
f. kabel listrik dan jaringan telekomunikasi yang membawa data atau mendukung layanan sistem informasi harus dilindungi dari penyambungan yang tidak sah (penyadapan) atau kerusakan.

BAB X

KEAMANAN OPERASIONAL SISTEM INFORMASI

A. Tujuan

Tujuan dari kebijakan keamanan operasional sistem informasi adalah untuk:

1. memastikan pengoperasian aset pengolahan dan penyimpanan informasi di Pemerintah Provinsi Gorontalo secara benar dan aman;
2. memastikan terlindunginya aset informasi beserta aset pengolahan dan penyimpanan informasi di Pemerintah Provinsi Gorontalo dari ancaman *malware;*
3. melindungi terjadinya kehilangan atas aset informasi;
4. tersedianya catatan (*log*) atas aktivitas sistem informasi sebagai barang bukti; dan
5. mencegah terjadinya eksploitasi atas kelemahan sistem informasi pada Pemerintah Provinsi Gorontalo.

B. Ruang Lingkup

Ruang lingkup dari kebijakan keamanan operasional sistem informasi adalah pengoperasian aset pengolahan dan penyimpanan informasi di lingkungan Pemerintah Provinsi Gorontalo.

C. Kebijakan

1. aktivitas operasional terkait fasilitas pengolahan informasi serta fasilitas komunikasi harus memiliki prosedur yang terdokumentasi dengan baik;
2. prosedur operasional tersebut harus tersedia bagi pengguna yang memerlukannya;
3. seluruh perubahan pada fasilitas pengolahan informasi yang dapat berimplikasi pada keamanan informasi, perlu diperlakukan secara terkendali, mencakup antara lain:
   a. menyusun perencanaan mengenai perubahan yang mungkin

terjadi serta melakukan pengujian terkait terpenuhinya persyaratan keamanan;

b. melakukan kajian atas implikasi keamanan informasi yang mungkin terjadi;

c. mengajukan persetujuan secara formal atas perubahan yang akan dilakukan; dan

d. mencatat seluruh perubahan yang telah dilakukan.

4. kinerja dan utilisasi atas fasilitas pengolahan informasi harus senantiasa dipantau dengan alat bantu peringatan dini, dioptimalkan pemanfaatannya, serta diproyeksikan kebutuhan kapasitasnya untuk masa yang akan datang.

5. untuk mengurangi risiko perubahan tanpa izin atau penyalahgunaan hak akses, pemisahan fasilitas pengembangan, pengujian, dan operasional harus dilakukan.

6. setiap sistem informasi di lingkungan Perangkat Daerah harus terlindungi dari *malware* secara memadai melalui:

   a. instalasi dari perangkat lunak *anti virus* pada sistem informasi;

   b. mem-*block* akses ke *website* yang dapat menimbulkan ancaman kepada sistem informasi;

   c. program peningkatan kesadaran bagi personil organisasi untuk menangani ancaman *malware*; dan

   d. setiap insiden terkait dengan *malware* harus dilaporkan kepada *administrator* sistem dan dikategorikan sebagai insiden keamanan informasi.

7. seluruh aset informasi yang berada di dalam fasilitas pengolahan informasi wajib dilakukan *backup*, dengan persyaratan berikut:

   a. backup mencakup aplikasi, database, dan *system image*;

   b. frekuensi *backup* dilakukan secara harian, bulanan, dan tahunan;

   c. salinan *backup* harus disimpan secara aman sesuai dengan periode retensi. periode retensi *backup* adalah 1 tahun, dimana:

      1) *backup* harian disimpan selama 31 hari;

2) *backup* bulanan disimpan selama 12 bulan;

d. seluruh hasil *backup* harus dilakukan uji *restore* secara berkala;

e. media *backup* disimpan pada perangkat *storage* yang terpisah dari perangkat pengolahan informasi utama;

f. *backup* merupakan tanggung jawab pengelola data center, sedangkan pengujian *restore* merupakan tanggung jawab pemilik aset informasi;

g. parameter *backup* disesuaikan dengan klasifikasi sistem sebagai berikut:

Parameter Backup	**Klasifikasi Sistem**	
	Vital	***Sensitive/ Non-Sensitive***
Cakupan Backup	Aplikasi, Database	Aplikasi, Database
Frekuensi *Backup (Recovery Point Objective)*	Harian	Bulanan
Pengujian *Restore*	Triwulanan	Semesteran

8. sistem harus dikonfigurasi untuk melakukan pencatatan (*logging*) atas seluruh aktivitas pengguna, jaringan, sistem, aplikasi, *error* yang terjadi (*exceptions*). Pemilik aset informasi harus menganalisis *log* terkait pola-pola penggunaan yang tidak wajar.
9. fasilitas pencatatan *log* dan informasi *log* yang dicatat harus dilindungi dari penghapusan dan akses oleh pihak yang tidak berwenang.
10. semua fasilitas pemrosesan informasi yang terhubung ke jaringan internal Perangkat Daerah harus disinkronisasi dengan sumber waktu yang akurat dan telah disepakati.
11. proses dan prosedur untuk mengendalikan instalasi perangkat lunak pada sistem operasional harus ditetapkan dan diimplementasikan untuk memastikan terjaganya kerahasiaan, integritas dan keterseiaan informasi.
12. instalasi software harus dilakukan oleh administrator sistem yang

relevan.

13. pemilik aset informasi wajib melakukan upaya-upaya identifikasi atas kelemahan teknis (*vulnerabilities*) dari seluruh aset informasi dibawah pengelolaannya, serta melakukan tindakan pengendalian yang sesuai untuk meminimalkan resiko atas hilangnya aset informasi. Tindakan pengendalian dapat berupa penonaktifan fitur tertentu, perbaikan/upgrade sistem, aplikasi, atau *patching*.
14. setiap sistem informasi di lingkungan Perangkat Daerah dapat dilakukan proses audit yang mencakup proses verifikasi terhadap sistem informasi dan/atau informasi Perangkat Daerah dengan mempertimbangkan sebagai berikut:
    a. harus direncanakan dan dikelola dengan baik untuk meminimalisasi gangguan terhadap proses bisnis;
    b. setiap proses audit yang membutuhkan akses kepada sistem informasi dan/atau informasi Perangkat Daerah harus disetujui oleh pemilik dari sistem dan/atau informasi tersebut;
    c. hak akses untuk kebutuhan audit harus dibatasi hanya hak akses read only; dan
    d. instalasi dari tools yang digunakan untuk proses audit hanya dapat dilakukan oleh personil yang berwenang yaitu administrator jaringan dan sistem teknologi informasi di Perangkat Daerah, dan harus segera dihapus setelah proses audit telah selesai dilakukan.

BAB XI

KEAMANAN KOMUNIKASI

A. Tujuan

Tujuan dari kebijakan keamanan komunikasi adalah untuk:

1. memastikan perlindungan atas informasi pada jaringan komputer beserta fasilitas pendukung pengolahan informasi;
2. menjaga keamanan informasi yang dipertukarkan, baik di dalam Perangkat Daerah maupun antar Perangkat Daerah eksternal.

B. Ruang Lingkup

Ruang lingkup dari kebijakan keamanan komunikasi adalah untuk:

1. pengendalian jaringan;
2. keamanan layanan jaringan;
3. pemisahan jaringan; dan
4. pertukaran informasi.

C. Kebijakan

1. Jaringan internal Perangkat Daerah harus diamankan untuk menjamin:
   a. pencegahan akses tanpa izin ke jaringan, layanan jaringan dan fasilitas pemrosesan informasi dalam jaringan;
   b. keamanan dari informasi milik organisasi yang dikirimkan melalui jaringan; dan
   c. integritas dan ketersediaan dari layanan jaringan organisasi.
2. Tugas dan tanggung jawab untuk pengelolaan jaringan dan keamanan harus dialokasikan dan apabila memungkinkan dipisahkan dari penanggung jawab opersional sistem aplikasi dan *data center.*
3. Konfigurasi dari jaringan, perangkat aktif dan perangkat keamanan jaringan harus ditinjau secara berkala untuk:
   a. memastikan kesesuaian dengan kondisi terkini; dan

b. mengidentifikasi kerawanan pada jaringan, layanan jaringan dan fasilitas pemrosesan informasi dalam jaringan.

4. Jaringan internal Perangkat Daerah harus dipisahkan dari jaringan eksternal dengan menggunakan *security gateway* atau *firewall*dan harus dikonfigurasikan untuk:
   a. memfilter *traffic* tanpa izin maupun *traffic* yang mencurigakan; dan
   b. apabila memungkinkan memfilter dan mencegah infeksi *malware* ke jaringan internal;
5. Koneksi ke *security gateway* atau *firewall* harus diotentikasikan, diotorisasi dan diamankan dengan metode pengamanan yang sesuai, misalnya dengan *virtual private network* (VPN), *secure shell* (SSH) atau metode kriptografi.
6. Kebijakan dan log *firewall* harus ditinjau paling sedikit 1 (satu) kali dalam tiga bulan.
7. Koneksi eksternal harus diputuskan secara otomatis setelah tidak aktif selama 5 menit.
8. Akses dari jaringan eksternal yang dilakukan oleh *vendor* pihak ketiga hanya dapat diberikan untuk kebutuhan *troubleshooting*dan harus secara formal disetujui dan didokumentasikan dan harus dibatasi waktunya sesuai dengan kebutuhan dari akses.
9. Jaringan internal Dinas harus disegmentasi baik secara fisik maupun *logical* untuk meningkatkan keamanan dan untuk mengendalikan akses dan *traffic* jaringan berdasarkan kritikalitas dari sistem dalam jaringan Perangkat Daerah.
10. Segmentasi jaringan harus ditinjau paling sedikit 1 (satu) kali dalam tiga bulan untuk menjamin kesesuaian dengan prasyarat keamanan terkini.
11. *Routing* jaringan harus dilakukan berdasarkan pengendalian terhadap alamat sumber dan tujuan.
12. Tanggung jawab untuk merubah *routing* jaringan hanya diberikan kepada administrator jaringan yang diberi izin.

13. Aturan untuk *routing* harus ditinjau paling tidak satu kali dalam tiga bulan untuk mendeteksi dan mengkoreksi adanya kesalahan atau *routing* tanpa otorisasi.
14. Perangkat jaringan harus ditempatkan pada lokasi yang aman untuk menghindari akses tanpa izin dan ancaman fisik maupun lingkungan.
15. Akses, baik fisik maupun *logical* ke perangkat jaringan harus dibatasi untuk tujuan administrasi dan pemeliharaan jaringan.
16. *Port* dan layanan jaringan, baik fisik maupun *logical,* yang tidak digunakan tidak boleh diaktifkan.
17. Akses ke *port* yang digunakan untuk kebutuhan *diagnostic* dan konfigurasi perangkat jaringan dan keamanan jaringan, seperti *console port,* harus sangat dibatasi dan diberikan kepada:
    a. Administrator jaringan dan keamanan jaringan Perangkat Daerah;
    b. Pihak ketiga yang telah disetujui dan bekerja untukkepentingan Perangkat Daerah
    c. aplikasi monitoring jaringan dan keamanan jaringan yang telah disetujui.
18. Semua perangkat jaringan harus dapat diidentifikasi secara fisik maupun *logical* dengan penamaan yang disepakati dan konsisten.
19. Perangkat jaringan yang dimiliki oleh pihak eksternal harus secara memadai dipisahkan dari perangkat jaringan milik Perangkat Daerah.
20. Mekanisme keamanan, tingkat layanan dan prasyarat lain untuk semua layanan jaringan harus diidentifikasi dan dimasukkan kedalam perjanjian layanan jaringan.
21. Akses ke layanan jaringan Perangkat Daerah hanya diberikan kepada personil yang terotorisasi berdasarkan prinsip *need to have.*
22. Penggunaan pihak ketiga penyedia layanan jaringan harus dimonitor untuk menjamin kesesuaian dengan prasyarat

keamanan Perangkat Daerah.

23. Layanan jaringan organisasi harus diamankan menggunakan metode yang dapat mencakup metode otentikasi atau metode kriptografi yang kuat untuk menjamin keamanan dari pengiriman informasi menggunakan jaringan dan layanan jaringan.
24. Terkait aspek pertukaran informasi melalui fasilitas jaringan komunikasi, Perangkat Daerah harus memperhatikan perjanjian kerahasiaan merupakan perikatan formal antara pemilik aset informasi dengan penerima informasi, yang ketentuan didalamnya memuat:
    a. pemberian izin penggunaan informasi dari pemilik aset informasi kepada penerima informasi untuk keperluan dan periode waktu yang spesifik, dimana pihak penerima informasi wajib menjaga kerahasiaan informasi serta mengupayakan pencegahan terjadinya kebocoran atau penyebaran informasi secara tidak sah;
    b. hak dari pemilik aset informasi untuk melakukan audit dan pemantauan aktivitas penerima informasi berkaitan dengan penggunaan informasi sensitif; dan
    c. konsekuensi yang harus ditanggung penerima informasi apabila terjadi pelanggaran atas perjanjian kerahasiaan.

BAB XII

AKUISISI, PENGEMBANGAN DAN PEMELIHARAAN SISTEM

A. Tujuan

Tujuan dari kebijakan akuisisi, pengembangan dan pemeliharaan sistem adalah untuk:

1. Memastikan keamanan informasi sebagai bagian tak terpisahkan dari siklus hidup (*lifecycle)* sistem informasi. Termasuk persyaratan untuk sistem informasi yang menyediakan layanan melalui jaringan publik
2. Memastikan keamanan informasi didesain dan diimplementasikan dalam siklus hidup (*lifecycle*) pengembangan dari sistem informasi.
3. Memastikan perlindungan terhadap penggunaan data untuk pengujian.

B. Ruang Lingkup

Ruang lingkup dari kebijakan keamanan komunikasi adalah untuk:

1. persyaratan keamanan sistem informasi;
2. keamanan dalam proses pengembangan dan *support;*
3. data pengujian.

C. Kebijakan

1. Perangkat Daerah harus menetapkan dan mendokumentasikan secara jelas persyaratan keamanan informasi yang relevan sebelum pengembangan, perluasan, atau pengadaan sistem informasi baru.
2. Persyaratan keamanan harus diidentifikasi secara jelas di dalam dokumen persyaratan dan spesifikasi perangkat lunak (*Software Requirement and Specification*).
3. Spesifikasi ini harus disetujui oleh pemilik informasi, pemilik proses bisnis dan pengembang sistem, sebelum fase pengkodean (*coding*) dalam pengembangan system.

4. Informasi yang digunakan oleh aplikasi Perangkat Daerah yang ditransimisikan melalui jaringan publik (internet) harus diamankan dari aktivitas penipuan, kemungkinan adanya perselisihan kontrak, dan pengungkapan dan/atau perubahan informasi tanpa izin.
5. Pengamanan informasi terhadap informasi yang ditransmisikan melalui sistem informasi yang digunakan dapat mencakup namun tidak terbatas pada:
   a. Proses otentikasi dan otorisasi terhadap pengguna aplikasi;
   b. Perlindungan untuk memastikan kerahasiaan dan integritas informasi yang dipertukarkan melalui jaringan publik;
   c. Perlindungan terhadap *session* transaksi untuk menghindari duplikasi dan/atau modifikasi;
   d. Mengamankan jalur komunikasi antara pihak-pihak yang terlibat
6. Keamanan dalam proses pengembangan dan dukungan yang perlu dipertimbangkan oleh Perangkat Daerah meliputi:
   a. aturan untuk pengembangan sistem harus ditetapkan dan diimplementasikan untuk proses pengembangan sistem di Perangkat Daerah yang mencakup:
      1) pengamanan dari lingkungan pengembangan, seperti pemisahan lingkungan pengembangan baik secara fisik dan/atau logical, pengendalian akses, pengelolaan perubahan;
      2) panduan *secure coding*;
      3) pengedalian versi aplikasi;
      4) penyimpanan dari *source code*;
      5) metode pengujian untuk mengidentifikasi dan memperbaiki *vulnerability*.
7. Perubahan terhadap sistem selama siklus pengembangan sistem harus dikendalikan melalui proses manajemen perubahan yang berlaku di Perangkat Daerah;

8. Apabila platform operasional, misalnya sistem operasi, database dan/atau *middleware*, dari sistem informasi Perangkat Daerah mengalami perubahan, aplikasi kritikal Perangkat Daerah harus ditinjau dan diuji untuk memastikan tidak ada dampak buruk terhadap operasional dan keamanan organisasi;
9. Perangkat Daerah harus menetapkan lingkungan pengembangan yang aman untuk pengembangan dan integrasi sistem Perangkat Daerah. Hal ini dapat mencakup namun tidak terbatas pada:
    a. Pemisahan lingkungan pengembangan baik secara fisik dan/atau logical;
    b. Pengendalian akses;
    c. Perpindahan data dari dan ke lingkungan pengembangan;
10. Perangkat Daerah harus mengawasi aktivitas pengembangan sistem yang dialihdayakan (*outsourced*). Hal ini dapat mencakup:
    a. perjanjian terkait lisensi dan kepemilikan sistem;
    b. pengujian penerimaan sistem untuk menguji kualitas dan akurasi dari sistem;
    c. prasyarat dokumentasi untuk sistem;
    d. perjanjian dengan pihak ketiga sebagai penjamin;
    e. hak untuk melakukan audit proses pengembangan dan kontrol yang diimplementasikan oleh vendor.
11. Pengujian dari fitur keamanan sistem harus dilakukan pada saat pengembangan sistem informasi Perangkat Daerah;
12. Pengujian ini dilakukan berdasarkan prasyarat keamanan sistem yang telah ditetapkan;
13. Kriteria dan jadwal untuk pengujian penerimaan sistem harus ditetapkan untuk sistem informasi baru, *upgrade* dan versi baru dari sistem informasi Perangkat Daerah;
14. Pengujian penerimaan sistem harus dilakukan sesuai dengan kriteria dan jadwal yang ditetapkan.
15. Pengamanan terhadap data hasil pengujian perlu diperhatikan sebagai berikut:

a. data untuk pengujian sistem harus dipilih secara hati-hati untuk menghindari pengungkapan atau perubahan informasi sensitif oleh pihak yang tidak berhak, serta melindung dari kemungkinan kerusakan dan kehilangan informasi;
b. *masking* data harus dilakukan apabila data operasional yang sensitif digunakan untuk keperluan pengujian;
c. data operasional yang digunakan untuk keperluan pengujian harus dihapus segera setelah proses pengujian telah selesai dilaksanakan.

BAB XIII

HUBUNGAN KERJA DENGAN PEMASOK (*SUPPLIER*)

A. Tujuan

Tujuan dari kebijakan mengenai hubungan kerja dengan pemasok (*supplier*) adalah untuk memastikan perlindungan atas aset Perangkat Daerah dalam jangkauan akses pemasok dan memelihara tingkat layanan yang dsetujui dari keamanan informasi sesuai dengan perjanjian dengan pemasok.

A. Ruang Lingkup

Ruang lingkup dari kebijakan mengenai hubungan kerja dengan pemasok (*supplier*) adalah para pemasok dalam lingkungan Pemerintah Provinsi Gorontalo.

B. Kebijakan

1. Perangkat Daerah harus mempertimbangkan aspek keamanan informasi dalam hubungan dengan pemasokmulai dari pemilihan, penunjukan, monitoring, evaluasi, sampai dengan terminasi.
2. Pemilihan dari penyedia jasa Perangkat Daerah harus mengikuti kriteria berikut:
   a. kompetensi, pengalaman dan catatan dari organisasi;
   b. kepastian dari kemampuan penyedia jasa untuk menyediakan layanan;
   c. kepastian dari kemampuan penyedia jasa untuk menjaga ketersediaan dari penyediaan layanan pada saat kondisi normal atau kondisi bencana (apabila terjadi bencana alam atau kegagalan dalam penyediaan layanan);
3. Berdasarkan pengelompokan pemasok yang telah bekerjasama, Perangkat Daerah wajib mendefinisikan pembatasan aset dan

aset informasi apa saja yang diperbolehkan untuk diakses oleh setiap kelompok pemasok, serta senantiasa memantau akses yang telah dilakukan.

4. Perangkat Daerah menetapkan persyaratan keamanan informasi bagi setiap pemasok yang mengakses aset informasi, serta senantiasa memantau kepatuhan pemasok terhadap persyaratan tersebut. Pemasok yang menangani aset informasi dengan klasifikasi rahasia perlu menandatangani Perjanjian Kerahasiaan.
5. Kewajiban *supplier* dan tingkat layanan harus ditetapkan secara formal dalam kontrak kerja;
6. Perangkat Daerah harus memastikan pengelolaan *delivery* layanan dari pemasok dengan memperhatikan:
   a. layanan yang diserahkan kepada Perangkat Daerah oleh pihak *supplier* harus secara berkala dipantau, dan ditinjau;
   b. proses pemantauan dilakukan untuk memverifikasi kesesuaian dari tingkat layanan yang diberian dan prasyarat keamanan informasi dengan perjanjian kerja;
   c. proses peninjauan dilakukan untuk mengidentifikasi problem terkait penyediaan layanan dan aspek keamanan informasi dalam penyediaan layanan oleh *supplier*;
   d. peninjauan dari penyediaan layanan oleh supplier harus dilaksanakan paling sedikit satu kali dalam tiga bulan;
7. Perangkat Daerah dapat melakukan audit terhadap penyediaan layanan yang diberikan pemasok
8. Ketentuan dalam pelaksanaan audit kepada pemasok sebagai berikut:
   a. tanggung jawab untuk mengaudit tingkat layanan dimiliki oleh pihak, baik internal maupun eksternal, yang memiliki independensi dari pengguna layanan yang diberikan oleh supplier dan ditunjuk secara formal;
   b. audit terhadap penyediaan layanan oleh supplier harus dilakukan paling sedikit satu kali dalam satu tahun;
   c. setiap ketidaksesuaian yang ditemukan dalam proses peninjauan dan audit harus dikelola dan ditindaklanjuti;
9. Perubahan terhadap layanan yang diberikan oleh supplier harus

dikelola, dengan memperhatikan kritikalitas dari proses bisnis pengguna layanan dan layanan yang diberikan oleh supplier;

10. Perubahan terhadap layanan yang diberikan oleh supplier harus dipastikan tidak akan mengganggu aspek kerahasiaan dari informasi Perangkat Daerah serta integritas dan ketersediaan dari informasi dan layanan Perangkat Daerah;
11. Perubahan terhadap layanan yang diberikan oleh supplier harus disetujui oleh manajemen Perangkat Daerah yang relevan dan diformalisasikan dalam kontrak kerja.

BAB XIV
PENANGANAN INSIDEN KEAMANAN INFORMASI

A. Tujuan

Tujuan dari kebijakan penanganan insiden keamanan informasiadalah untuk memastikan adanya pendekatan yang konsisten dan efektif atas penanganan insiden keamanan informasi.

B. Ruang Lingkup

Ruang lingkup dari kebijakan penanganan insiden keamanan informasi adalah:

1. tanggung jawab dan prosedur;
2. pelaporan atas kejadian insiden keamanan informasi; dan
3. pelaporan atas kelemahan keamanan informasi.

C. Kebijakan

1. Kejadian keamanan informasi adalah sebuah kejadian pada sistem, layanan ataupun jaringan yang dapat mengindikasikan adanya pelanggaran keamanan informasi atau kegagalan keamanan atau kejadian yang mungkin memiliki keterkaitan dengan keamanan informasi.
2. Kelemahan keamanan informasi adalah sebuah kelemahan yang teridentifikasi pada sistem, layanan atau jaringan yang dapat dieksploitasi oleh pihak yang tidak bertanggung jawab dan dapat menyebabkan pelanggaran terhadap kebijakan keamanan informasi.
3. Insiden keamanan informasi adalah kejadian keamanan informasi yang tidak diinginkan dan tidak diperkirakan dimana kejadian tersebut menimbulkan gangguan terhadap operasional bisnis dan mengancam keamanan informasi.
4. Guna memastikan proses penanganan insiden yang responsif dan efektif, perlu dikembangkan berbagai prosedur yang mencakup:

a. perencanaan dan persiapan penanganan insiden;
b. pemantauan, analisis, dan pelaporan atas insiden;
c. pencatatan atas aktivitas penanganan insiden;
d. penanganan bukti forensik;
e. penilaian dan pengambilan keputusan ata insiden dan kelemahan keamanan informasi; dan
f. pemulihan insiden.

5. Seluruh pegawai dan pihak ketiga wajib melaporkan berbagai kejadian insiden keamanan informasi maupun yang masih bersifat dugaan atas kelemahan keamanan informasi sesegera mungkin, sesuai prosedur pelaporan insiden yang berlaku.
6. Setiap kejadian insiden keamanan informasi harus dianalisis, diklasifikasikan, dan ditentukan skala prioritas penanganannya. Penanganan insiden beserta pemulihannya dilakukan berdasarkan klasifikasi dan prioritas yang telah ditetapkan.
7. Perangkat Daerah harus mengklasifikasikan insiden keamanan informasi untuk memprioritaskan penanganan insiden. Klasifikasi insiden tersebut adalah sebagai berikut:
   a. Insiden keamanan informasi diklasifikasikanberdasarkan dampaknya menjadi berikut:
      1) mayor, apabila insiden tersebut menyebabkan terhentinya proses operasional pekerjaan Perangkat Daerah;
      2) minor, apabila insiden tersebut menyebabkan gangguan yang tidak menghentikan proses operasional pekerjaan Perangkat Daerah.
   b. Insiden keamanan informasi diklasifikasikanberdasarkan tingkat kepentingannya menjadi berikut:
      1) *emergency*, apabila insiden tersebut dapat atau telah menghentikan proses operasional Perangkat Daerah dan/atau insiden tersebut mempengaruhi secara langsung pimpinan dalam lingkungan Perangkat Daerah;
      2) normal, apabila insiden tersebut insiden tersebut tidak

menghentikan proses operasional Perangkat Daerah dan/atau insiden

tersebut mempengaruhi secara langsung pimpinan dalam lingkungan Perangkat Daerah.

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

9. Setiap tindakan yang diidentifikasi untuk menangani kejadian, kelemahan dan insiden keamanan informasi harus dikonsultasikan kepada Ketua Tim Penanggulangan dan Pemulihan Insiden GorontaloProv-CSIRT Provinsi Gorontalo dan/atau personil yang kompeten dan relevan dengan kejadian, kelemahan dan insiden keamanan informasi.

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

BAB XV

KELANGSUNGAN USAHA (*BUSINESS CONTINUITY*)

A. Tujuan

Tujuan dari kebijakan mengenai kelangsungan usaha (*business continuity*) adalah untuk memastikan ketersediaan layanan TIK beserta fasilitas pengolahan informasi dalam kondisi darurat dan memulihkan layanan seperti sediakala dalam kondisi kembali normal.

B. Ruang Lingkup

Ruang lingkup dari kebijakan mengenai kelangsungan usaha (*business continuity*) adalah:

1. keberlanjutan keamanan informasi;
2. redundansi fasilitas pengolahan informasi.

C. Kebijakan

1. Perangkat Daerah harus menetapkan, mendokumentasikan, mengimple-mentasikan dan memelihara proses, prosedur dan kontrol yang diperlukan untuk menjamin keberlanjutan keamanan informasi sesuai prasyarat yang telah ditetapkan pada saat dan setelah terjadinya gangguan besar atau bencana.
2. Perangkat Daerah harus memverifikasi kontrol keberlanjutan keamanan informasi yang telah ditetapkan dan diimplementasikan secara berkala untuk menjamin kesesuaian dan efektivitasnya pada saat dan setelah terjadinya gangguan besar atau bencana.
3. Perangkat Daerah harus menetapkan prasyarat untuk keberlanjutan keamanan informasi dan diintegrasikan dengan prasyarat keberlanjutan bisnis organisasi untuk menjamin keberlanjutan dari keamanan informasi di Perangkat Daerah, pada saat dan setelah terjadinya gangguan besar atau bencana.
4. Prasyarat keamanan informasi dapat diintegrasikan pada siklus proces *business continuity management* (BCM) yang mencakup:

a. memahami kebutuhan organisasi;
b. menentukan strategi BCM;
c. mengembangkan dan mengimplementasikan rencana penanggulangan/ keberlanjutan bisnis;
d. pengujian, pemeliharaan dan peninjauan rencana penanggulangan/ keberlanjutan bisnis;

5. Aspek redundansi harus ditetapkan untuk fasilitas pengolahan informasi dan sarana pendukungnya untuk memastikan ketersediaan dari proses bisnis dan operasional Perangkat Daerah serta pemberian layanan Perangkat Daerah kepada publik.
6. Apabila prasyarat redundan tidak dapat dipenuhi, maka proses alternatif perlu ditetapkan untuk menjamin ketersediaan dari proses bisnis dan operasional Perangkat Daerah serta *delivery* dari layanan Perangkat Daerah kepada publik.
7. Fasilitas pengolahan informasi beserta sarana pendukungnya yang telah memenuhi aspek redundansi harus diuji secara berkala untuk menjamin kesesuaian dari fungsinya.
8. Guna menjamin ketersediaan layanan serta keamanan informasi dalam kondisi darurat (misalnya: bencana alam) pada lokasi utama, perlu adanya redundansi terhadap fasilitas pengolahan informasi yang disebut sebagai fasilitas *backup site*.
9. *Backup site* yang dimaksud dapat berupa lokasi kerja pengganti atau *disaster recovery center* (DRC) bagi alternatif area *data center*.
10. Ketentuan dalam pengelolaan terkait *Backup Site* meliputi:
    a. Lokasi backup site secara geografis memiliki probabilitas kejadian bencana alam yang minimal;
    b. backup site ditujukan sebagai media penyimpanan backup alternatif, serta sebagai fasilitas pengolahan informasi alternatif;
    c. terpenuhinya pemulihan layanan operasional sepenuhnya pada fasilitas *backup site* sesuai kerangka parameter *recovery time objective* (RTO);

d. pengelola *backup site* beserta Pemilik Aset Informasi melakukan uji keberlangsungan secara berkala dibawah koordinasi penanggung jawab kelangsungan bisnis, minimal 1 kali dalam setahun, untuk menguji kesiapan seluruh pihak dalam hal:
   1) memindahkan operasional ke fasilitas *backup site*;
   2) memulihkan operasional aplikasi beserta data sesuai parameter *recovery point objective* (RPO) yang telah ditetapkan.

BAB XVI

KEPATUHAN

A. Tujuan

Tujuan dari kebijakan kepatuhan adalah untuk menghindari pelanggaran kewajiban hukum, undang-undang, peraturan atau kontrak yang terkait keamanan informasi dan persyaratan keamanan dan untuk memastikan keamanan informasi diimplementasikan dan dioperasikan sesuai dengan prosedur dan kebijakan organisasi.

B. Ruang Lingkup

Ruang lingkup dari kebijakan mengenai kepatuhan:

1. kepatuhan dengan prasyarat hukum dan kontraktual;
2. peninjauan keamanan informasi.

C. Kebijakan

1. Pemerintah Provinsi Gorontalo berkomitmen untuk menjaga kepatuhan terhadap setiap prasyarat keamanan informasi yang relevan. Prasyarat keamanan informasi yang dimaksud mencakup prasyarat hukum, regulasi dan kontraktual;
2. Seluruh prasyarat hukum, regulasi dan kontraktual yang terkait dengan keamanan informasi dan berlaku bagi Perangkat Daerah harus diidentifikasikan, didokumentasikan dan dipelihara;
3. Perangkat Daerah harus mematuhi hak atas kekayaan intelektual yang terkait dengan material yang digunakan oleh Perangkat Daerah seperti:
   a. penggunaan perangkat lunak dan material yang bersifat *proprietary* harus mematuhi undang-undang terkait hak atas kekayaan intelektual (haki) yang berlaku;
   b. bukti dari lisensi atau izin resmi harus didapatkan dan disimpan untuk seluruh materi berlisensi /*copyright* yang di-*install*;
   c. lisensi yang bersifat berlangganan/harus diperbaharui dalam jangka waktu tertentu, harus dikelola untuk memastikan

penggunaannya secara legal dan berkesinambungan;

d. penggunaan lisensi dari materi berlisensi/*copyright* harus dikendalikan dengan baik;

4. Dokumen-dokumen penting Perangkat Daerah harus dilindungi dari kehilangan, pemalsuan, kerusakan, atau penyalahgunaan sesuai dengan peraturan perundangan, regulasi, dan persyaratan kontrak dan bisnis;
5. Perangkat Daerah harus memastikan privasi dan perlindungan terhadap informasi terkait dengan pribadi (*personally identifiable information*) sesuai dengan prasyarat hukum, perundangan, regulasi dan kontraktual;
6. Pimpinan Perangkat Daerah harus secara rutin memantau dan meninjau kepatuhan dari personil, proses kerja dan pemrosesan informasi dalam area tanggung jawabnya terhadap kebijakan dan standard keamanan informasi Perangkat Daerah serta prasyarat keamanan informasi yang berlaku;
7. Pada saat terjadi ketidaksesuaian, pimpinan Perangkat Daerah bertanggung jawab untuk menangani ketidaksesuaian yang terjadi sesuai dengan kebijakan terkait penanganan ketidaksesuaian dan peningkatan SMKI;
8. Sistem informasi Perangkat Daerah harus ditinjau untuk menganalisis kepatuhan teknis dengan kebijakan dan standard keamanan yang berlaku serta dengan prasyarat keamanan informasi yang relevan dan berlaku, paling tidak satu kali dalam satu tahun;
9. Apabila diperlukan, peninjauan tersebut dapat melibatkan personil yang memiliki kualifikasi di bidang keamanan informasi untuk mendapatkan pemahaman yang mendalam mengenai risiko keamanan informasi yang mungkin muncul dari pengecualian tersebut.

DITANDA TANGANI SECARA ELEKTRONIK OLEH :

Balai Sertifikasi Elektronik

RUSLI HABIBIE
Gubernur Gorontalo

KARO HUKUM	KADIS	ASISTEN	SEKDA	WAGUB

LAMPIRAN IV PERATURAN GUBERNUR GORONTALO
NOMOR : 57 TAHUN 2019
TANGGAL : 8 November 2019
TENTANG : TATA KELOLA SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK PROVINSI GORONTALO

NAMA DOMAIN DAN SUBDOMAIN

1. UMUM

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

2. RUANG LINGKUP

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

   Setiap pengajuan nama subdomain harus disampaikan kepada Dinas disertai dengan data penanggung jawab portal *web* (*website*), aplikasi berbasis *web* serta pemilik kegiatan yang ditetapkan melalui Surat Keputusan Kepala Perangkat Daerah

3. KEBIJAKAN

   3.1 Setiap Pimpinan Perangkat Daerah bertanggung jawab dalam memantau dan mengawasi penggunaan subdomain di lingkungan masing-masing.

   3.2 Setiap Pimpinan Perangkat Daerah bertanggung jawab dan mengetahui terhadap penambahan dan perubahan nama subdomain di lingkungan masing-masing, dalam hal ini meliputi penambahan, perubahan, dan penghapusan subdomain

   3.3 Domain dan subdomain yang sudah dibuat menjadi milik Pemerintah Daerah Provinsi dan tidak boleh digunakan di luar Pemerintah Daerah Provinsi tanpa izin dari pejabat yang

berwenang.

3.4 Domain dikelola oleh pejabat setingkat eselon IV yang memiliki tupoksi pengelolaan domain dan di bantu oleh staf teknis/fungsional

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

4.1 Pengertian DNS

4.1.1 DNS adalah sistem basis data terdistribusi (*distribute database system*) yang digunakan untuk pencarian nama komputer di jaringan yang menggunakan TCP/IP (*Transmission Control Protocol/ Internet Protocol*).

4.1.2 DNS merupakan sebuah aplikasi service yang bisa digunakan di internet seperti peramban (*web browser*) atau surat elektronik yang menerjemahkan sebuah nama domain ke alamat IP (*IP address*).

Contoh : gorontaloprov.go.id □103.210.34.3

4.2 Struktur DNS

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

4.2.1 Domain Tingkat Pertama (*Root Domain*)

1) Domain Level Global (*Generic/Global Top Level Domain*
(gTLD))
Contoh: .com, .ac, .*web*, .go

2) Domain Level Negara (*Country Code Top Level Domain*
(ccTLD))
Contoh: .sg, .au, .id

4.2.2 Domain Tingkat Kedua (*Second Level Domain*) Contoh: gorontaloprov.go.id

4.2.3 Domain Tingkat Ketiga (*Third Level Domain* (subdomain)) Contoh:

kominfo.gorontaloprov.go.id,

lpse.gorontaloprov.go.id

5. PENGELOLAAN PENAMAAN DOMAIN

5.1 Pengelolaan Penamaan Domain meliputi:

a) Pendaftaran,

b) Penggunaan,

c) Penonaktifan

d) Perpanjangan,

e) Penunjukan pejabat,

f) Perubahan nama domain,

g) *Server* nama domain.

5.2 Nama domain yang dimaksud di atas dibiayai oleh Anggaran Dinas.

5.3 Seluruh situs *web* (*website*) Perangkat Daerah serta aplikasi berbasis *web* pada Perangkat Daerah harus menjadi subdomain dari nama domain Pemerintah Daerah Provinsi.

5.4 Domain resmi Pemerintah Daerah Provinsi adalah gorontaloprov.go.id

5.5 Untuk pengaplikasian penamaan pada jaringan dan perangkat jaringan, server dan kebutuhan lainnya di Data Center, domain resmi lainnya yang dikelola oleh dinas adalah awota.id

6. SUBDOMAIN PEMERINTAH DAERAH PROVINSI

6.1 Yang berhak mendapatkan nama subdomain:

1) Perangkat Daerah.

2) Pelayanan publik di Pemerintah Daerah Provinsi.

3) Kegiatan Pemerintahan Provinsi.

4) Aplikasi berbasis *web*.

6.2 Permohonan mendapatkan nama subdomain.

Mengajukan permohonan melalui Dinas dengan mencantumkan dan melampirkan:

1) Surat permohonan nama subdomain layanan publik/domain khusus.

2) Peraturan perundang-undangan yang menjadi dasar penyelenggaraan pelayanan publik/penyelenggaraan kegiatan Pemerintah Daerah Provinsi.
3) Surat keterangan mengenai pelayanan publik/kegiatan berskala nasional atau internasional.
4) Penunjukan pejabat nama subdomain.
5) Surat penunjukan pejabat nama subdomain yang ditetapkan melalui Keputusan Kepala Perangkat Daerah.
   a. Salinan Kartu PNS atau kartu identitas pegawai tetap.

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

6.4 Penataan subdomain untuk Unit Organisasi dan Unit Kerja di bawahnya:
1) Unit Organisasi : *eselonII*.gorontaloprov.go.id
2) Unit Eselon III : *eselonII*.gorontaloprov.go.id/*produk*

6.5 Penataan subdomain untuk kegiatan Pemerintah Daerah Provinsi :
1) Kegiatan Skala Nasional/Internasional :
   kegiatan.gorontaloprov.go.id
2) Kegiatan Internal Pemerintah Daerah Provinsi :
   eselonII.gorontaloprov.go.id/*kegiatan*
3) Kegiatan Internal Pemerintah Daerah Provinsi Tingkat Unit Kerja:
   eselonII.gorontaloprov.go.id/*kegiatan*

6.6 Penataan subdomain untuk aplikasi berbasis web:
1) Digunakan oleh publik:
   aplikasi.gorontaloprov.go.id atau
   aplikasi.id atau *aplikasi*.go.id
   contoh : *suararakyathulodhalo*.id, awota.id

2) Digunakan di lingkungan Pemerintah Daerah Provinsi:
aplikasi.gorontaloprov.go.id
contoh *simpd.gorontaloprov.go.id*

3) Digunakan di lingkungan Unit Organisasi/Unit Kerja/khusus:
aplikasi.eselonII.gorontaloprov.go.id

6.7 Nama subdomain Perangkat Daerah :
Nama sub domain perangkat daerah, didasarkan pada nama singkatan Perangkat Daerah, contoh :

1) Dinas Komunikasi, Informatika dan Statistik
kominfo-st.gorontaloprov.go.id
2) Badan Kepegawaian Daerah
bkd.gorontaloprov.go.id

6.8 Selain nama domain gorontaloprov.go.id Perangkat Daerah dapat mengusulkan nama domain lainnya (khusus) dengan ketentuan sebagai berikut :

1) Aplikasi tersebut adalah aplikasi untuk pelayanan publik
2) Aplikasi telah memenuhi syarat untuk dihosting di Data Center Dinas
3) Perangkat Daerah mengajukan permohonan nama domain khusus ke Sekreatris Daerah
4) Jika disetujui Sekretaris Daerah, permohonan pengajuan domain ke kementrian komunikasi dan informatika melalui Dinas

6.9 Ketentuan lain yang harus diikuti bagi seluruh Perangkat Daerah di Pemerintahan Daerah Provinsi:

1) Seluruh basis data (*database*) dan portal *web* (*website*)/aplikasi berbasis *web* harus disimpan pada server yang berada di pusat data (*data center*) Pemerintah Daerah Provinsi.
2) Perangkat Daerah wajib melakukan pembinaan dan pengawasan terhadap unit kerja di bawahnya.
3) Jika terjadi gangguan jaringan komunikasi dan keamanan

menjadi tanggung jawab Dinas untuk melakukan perbaikan.

4) Jika terjadi gangguan terkait data dan informasi menjadi tanggung jawab Perangkat Daerah pemilik data dan informasi tersebut dan akan dibantu oleh dinas dalam melakukan perbaikan.

DITANDA TANGANI SECARA ELEKTRONIK OLEH :

RUSLI HABIBIE
Gubernur Gorontalo

LAMPIRAN V PERATURAN GUBERNUR GORONTALO
NOMOR : 57 TAHUN 2019
TANGGAL : 8 November 2019
TENTANG : TATA KELOLA SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK PROVINSI GORONTALO

PORTAL WEB, TATA KELOLA WEB, MEDIA SOSIAL DAN PUSAT PESAN

A. Portal Web

1. Umum

Standar portal *web* (*website*) merupakan kebijakan terkait dalam penyelenggaraan portal *web* (*website*) yang telah mengikuti peraturan yang berlaku. Kebijakan dan standar ini menjadi pedoman bagi penyelenggara portal *web* (*website*) di Pemerintah Provinsi agar lebih terstruktur dan mencerminkan identitas Pemerintah Provinsi.

Standar ini berlaku bagi seluruh pembuatan dan pengembangan portal *web* (*website*) yang dilaksanakan oleh seluruh Perangkat Daerah.

2. Ruang Lingkup

Ruang lingkup dari penataan portal *web* (*website*) meliputi struktur menu, konten serta tata letak (*layout*) portal *web* (*website*) Perangkat Daerah yang harus berkoordinasi dengan Dinas.

3. Kebijakan

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

b. Setiap Pimpinan Perangkat Daerah bertanggung jawab dan mengetahui terhadap penambahan dan perubahan portal web (website) di instansi masing-masing, dalam hal ini meliputi penambahan, perubahan, penghapusan portal web (website).

c. Portal *web* (*website*) yang sudah dibuat menjadi milik Pemerintah Provinsi dan tidak boleh digunakan di luar Pemerintah Provinsi tanpa izin dari pejabat yang berwenang.

4. Tanggung Jawab

Pihak-pihak yang terkait dalam pembuatan dan pengembangan

portal *web* (*website*) terdiri dari:

a. Penanggung jawab portal *web* (*website*) adalah Perangkat Daerah yang mengajukan dan menggunakan portal *web* (*website*).
b. Penanggung jawab portal *web* (*website*) harus melakukan evaluasi terhadap portal *web* (*website*) yang telah dibangun untuk memastikan keberlangsungan portal *web* (*website*) tersebut.
c. Pengguna adalah publik baik eksternal maupun internal Pemerintah Provinsi.

5. Platform Portal *Web* (*Website*)

	Penetapan		Penjelasan
	Berlisensi terbuka (*open source*)	Berlisensi berbayar (*licensed*)	
Web Server	▪ Apache	IIS	Mengacu pada kondisi di Data Center
Basis Data (*Database*)	▪ MySQL ▪ Postgre ▪ Mongodb ▪ Mariadb	▪ MS SQL ▪ MySQL	
Pengkodean (*Coding*)	▪ PHP ▪ Java ▪ HTML5	▪ ASP ▪ ASP.NET	
Sistem Informasi Geografis (SIG)	▪ Quantum GIS ▪ Global Mapper	▪ ArcGIS Desktop/ Server ▪ ErMapper, Envi	
Aplikasi yang dikembangkan	• Memiliki Web Server API (Response JSON/XML) • *Single Sign On* • Harus dapat diakses pada semua browser yang bisa digunakan oleh masyarakat luas, antara lain Internet Explorer, Mozilla Firefox, Chrome, Opera, Safari , dll Responsive/Dapat diakses pada perangkat (*gadget*) yang umum digunakan, antara lain komputer tablet, *smartphone*, dll		

- Data Center menyediakan pusat data (*data center*) untuk penempatan (*hosting*) *website* internal Pemerintah Provinsi dan aplikasinya
- Data Center akan melakukan pengujian terhadap portal *web* (*website*) yang dikembangkan oleh masing-masing Perangkat Daerah

6. Penataan Konten

Pengelolaan konten portal *web* (*website*) berupa perbaikan dan penambahan konten yang dilakukan oleh masing-masing Perangkat Daerah. Kelengkapan informasi yang tersedia di *website* menjadi tanggung jawab masing-masing Perangkat Daerah pemilik *website*.

Mengacu pada Undang Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik, konten yang wajib tersedia di portal *web* (*website*) Pemerintah Provinsi dan Perangkat Daerah lainnya adalah sebagai berikut:

a. Profil Pemerintah Provinsi dan Perangkat Daerah, dengan sub konten sebagai berikut :
   1) Sejarah
   2) Tugas dan Struktur Organisasi (bagan)
   3) Info Pejabat
   4) Lokasi Kantor
b. Organisasi, berisikan tautan ke unit-unit di bawahnya, baik Struktural maupun Fungsional.
c. Produk, menjelaskan produk dari masing-masing Perangkat Daerah seperti :
   1) Renstra,
   2) Kebijakan/Strategi,
   3) Rencana program,
   4) Pengelolaan anggaran (DPA, RKA, ringkasan laporan keuangan, lakip, dll),
   5) Peraturan perundang-undangan,
   6) Info kepegawaian (SDM),
   7) SNI/Pedoman,
   8) NSPK/SPM,
   9) Data statistik,

10) Pemetaan/GIS,
11) Kamus/istilah (Glossary),
12) Katalog,
13) Aplikasi,
14) Teknologi Terapan,
15) Jasa layanan,
16) Iklan layanan masyarakat,
17) Spesifikasi,
18) Ilmu pengetahuan dan teknologi, dan lain-lain.

d. Publikasi, merupakan sarana dalam penyampaian informasi seperti :
   1) Majalah,
   2) Buletin,
   3) Jurnal,
   4) Artikel/guntingan berita,
   5) Buku ilmiah, dan lain-lain
e. Berita, merupakan sarana penayangan berita kegiatan seperti Berita Terkini, Berita Terkait, dan Berita Terpopuler.
f. Galeri, merupakan media untuk menayangkan Foto dan Video
g. Layanan Informasi Publik, merupakan wadah bagi saran dan pengaduan serta layanan informasi publik yang dikoordinasi oleh Pejabat Pengelola Informasi dan Dokumentasi (PPID).
h. Layanan Pengadaan Secara Elektronik (LPSE) Pemerintah Provinsi, merupakan layanan pengadaan barang dan jasa.
i. Helpdesk, atau kontak layanan melalui chatting
j. Agenda kegiatan, merupakan kegiatan rutin yang dilaksanakan setiap tahun atau peristiwa (*event*) besar lainnya seperti Seminar, Kolokium, dll.
k. Fasilitas/dukungan, merupakan sarana untuk menayangkan pelayanan jasa seperti laboratorium, perpustakaan, sumber daya manusia, dukungan teknis.
l. Selain konten yang tersebut di atas, hal lain yang perlu disiapkan pada portal *web* (*website*) yang dibangun oleh masing-masing Perangkat Daerah adalah sebagai berikut :

1) Navigasi kembali ke portal *web* (*website*) Pemerintah Provinsi dan ke portal *web* (*website*) Perangkat Daerah;
2) Peta situs (*Site Map*);
3) Fasilitas pencari;
4) Kontak berupa alamat, nomor telepon, dan surat elektronik;
5) Catatan kaki (*footer*);
6) Hak Cipta;
7) Fasilitas dua Bahasa (Bahasa Indonesia dan Bahasa Inggris).

7. Penentuan Tata Letak (*Layout*)
   a. Menentukan tata letak (*layout*) secara proporsional sesuai dengan kaidah estetika pada penempatan elemen-elemennya;
   b. Menyesuaikan dengan resolusi layar yang biasa digunakan oleh pengguna (minimal resolusi 1024 x 768 piksel);
   c. Menyertakan kontras bentuk, ukuran, posisi, warna dan huruf;
   d. Menggunakan tekstur yang halus dan tidak kompleks untuk latar belakang;
   e. Responsive, otomatis menyesuaikan dengan ukuran layar pengguna
   f. Secara umum tata letak (*layout*) untuk portal *web* (*website*) Pemerintah Provinsi terdiri dari beberapa bagian utama, yaitu :
      1) Navigasi untuk kembali ke halaman utama portal *web* (*website*) Pemerintah Provinsi;
      2) Tajuk (*header*) utama sebagai identitas Perangkat Daerah;
      3) Navigasi utama yang telah dikelompokkan;
      4) Berita utama kelembagaan (20-30% dari seluruh konten portal *web* (*website*));
      5) Menu pendukung lainnya;
      6) Catatan kaki (*footer*);
      7) Hak cipta;
      8) Fasilitas dua Bahasa (Bahasa Indonesia dan Bahasa Inggris).

8. Penataan Tayangan

   Standardisasi tayangan dalam pembuatan dan pengembangan portal *web* (*website*) Pemerintah Provinsi dapat menjadi acuan bagi seluruh portal *web* (*website*) Perangkat Daerah di Pemerintah Provinsi.

a. Penentuan warna
   1) Menentukan warna dengan kombinasi yang serasi dan sesuai dengan identitas Pemerintah Provinsi.
   2) Tidak menggunakan kombinasi warna yang menyebabkan tulisan sulit terbaca.
   3) Menggunakan maksimum 4 warna dasar yang mendukung, jika membutuhkan warna lainnya, menggunakan turunan warna dari warna-warna yang telah dipilih.
b. Penggunaan huruf
   1) Tidak menggunakan huruf yang harus diunduh dulu, gunakan huruf standar yang terdapat pada semua peramban (*browser*).
   2) Tidak menggunakan jenis huruf terlalu banyak, pilih jenis huruf yang mudah dibaca.
   3) Tidak menggunakan huruf kapital terlalu banyak.
   4) Tidak memberi garis bawah tulisan.
   5) Mengatur jarak spasi antar baris dan jarak spasi antar huruf.
   6) Membuat kombinasi kontras yang jelas antara huruf dan latar belakang atau antara huruf dan gambar.
   7) Penggunaan huruf yang tidak standar harus dalam bentuk grafis agar bisa ditampilkan seragam di semua peramban (*browser*).
c. Penggunaan gambar, suara, dan video
   1) Menggunakan gambar tipe SVG, JPG, dan PNG.
   2) Menggunakan suara tipe MP3 dan WAV.
   3) Menggunakan video tipe MP4.
   4) Gambar harus sesuai dengan artikel yang ditayangkan.
   5) Peletakan gambar, suara, dan video harus proporsional dengan ketajaman yang cukup dan dimensi tidak terlalu besar.
   6) Ukuran file gambar, suara, dan video dikoordinasikan dengan Dinas.
   7) Menggunakan atribut "alt" dalam tag "img src" agar muncul keterangan dari gambar yang tidak bisa tayang
d. Penggunaan bahasa
   1) Menggunakan bahasa dan istilah yang mudah dimengerti.

2) Menggunakan simbol sebagai pengganti bahasa.
3) Tidak membuat narasi yang terlalu panjang.

e. Ketentuan lain
1) Merancang menu navigasi utama yang mudah ditemukan.
2) Meletakkan alamat kontak dengan jelas.
3) Meletakan modul chat yang di kelola oleh bidang yang memiliki tupoksi penyebarluasan informasi dan dibantu oleh PPID
4) Meletakan kontak media sosial
5) Mencantumkan peta situs (site map) di halaman depan.
6) Menyiapkan tautan sesuai dengan informasi yang ada.

B. Tata Kelola Web

1. Umum

Tata kelola portal *web* merupakan kebijakan terkait dalam penyelenggaraan portal *web* (*website*) khususnya pengelolaan portal *web* (*website*) di Pemerintah Provinsi dan Perangkat Daerah. Tata kelola ini untuk dijadikan sebagai pedoman bagi pengelola portal *web* (*website*) di Pemerintah Provinsi agar mudah dalam melakukan koordinasi dan komunikasi.

Standar ini berlaku bagi seluruh pengelola portal *web* (*website*) yang dilaksanakan oleh seluruh Perangkat Daerah.

2. Ruang Lingkup

Ruang lingkup dari tata kelola portal *web* (*website*) meliputi penetapan penanggung jawab pengelola portal *web* (*website*) dan konten pada Perangkat Daerah.

3. Kebijakan

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

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

(website).

c. Portal *web* (*website*) yang sudah dibuat menjadi milik Pemerintah Provinsi dan tidak boleh digunakan di luar Pemerintah Provinsi tanpa izin dari pejabat yang berwenang.

4. Tanggung Jawab

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

a. Penanggung jawab portal *web* (*website*) adalah Perangkat Daerah di lingkungan Pemerintah Provinsi.

b. Penanggung jawab portal *web* (*website*) harus melakukan pemutakhiran konten portal *web* (*website*) secara rutin atau setiap ada perubahan pada konten dan kode sumbernya.

c. Penanggung jawab portal *web* (*website*) melakukan evaluasi terhadap portal *web* (*website*) yang telah dibangun untuk memastikan keberlangsungan portal *web* (*website*) tersebut.

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

5. Platform *Website*

a. Penyelenggara *website*

Pemeliharaan infrastruktur portal *web* (*website*) Pemerintah Provinsi dilakukan secara berkelanjutan dan melibatkan seluruh Perangkat Daerah di Pemerintah Provinsi dan lebih diperkuat melalui "Kerabat *Website*".

Penyediaan jaringan teknologi informasi dan komunikasi di Pemerintah Provinsi disiapkan dan dikelola oleh Dinas dengan didukung oleh seluruh Perangkat Daerah dan Unit Kerja. Pemanfaatan jaringan teknologi informasi dan komunikasi ini dilaksanakan di seluruh Perangkat Daerah Pemerintah Provinsi Secara umum pengelolaan infrastruktur jaringan teknologi informasi dan komunikasi dan portal *web* (*website*) Pemerintah Provinsi melibatkan antara lain:

1) Dinas

a) Penanggungjawab jaringan teknologi informasi dan

komunikasi portal *web* (*website*) Pemerintah Provinsi dan Perangkat Daerah

b) Penanggung jawab sistem portal *web* (*website*) Pemerintah Provinsi (www.gorontaloprov.go.id)

c) Pengelola tayangan pengumuman, agenda kegiatan Pemerintah Provinsi, tayangan informasi Pemerintah Provinsi di luar berita dan publikasi kontributor konten portal *web* (*website*) Pemerintah Provinsi

d) Penanggung jawab konten portal *web* (*website*) Pemerintah Provinsi (www.gorontaloprov.go.id) berupa berita utama Pemerintah Provinsi, galeri foto dan video Pemerintah Provinsi, Saran dan Pengaduan, Layanan Informasi Publik, Pelayanan Publik dan *Helpdesk*

2) Perangkat Daerah melalui PPID

a) Penanggung jawab sistem portal *web* (*website*) Perangkat Daerah

b) Penanggung jawab berita dan konten portal *web* (*website*) Perangkat Daerah

c) Kontributor konten portal *web* (*website*) Pemerintah Provinsi

d) *Help desk* layanan chat pada website

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

b. Matriks tugas dan tanggung jawab pemeliharaan portal *web* (*website*) Pemerintah Provinsi

Tugas			Pelaksana
Top Level Management and *Policy maker* / Pembuat kebijakan			
1	Pengelola *web* utama (*Webmaster*)	Menentukan kebijakan, mengelola dan menjaga portal *web* (*website*)	Dinas
			Dinas, Penanggung jawab

2.	Administrator *web* (*Web Administrator*)	Proses manajemen	portal *web* (*website*) Perangkat Daerah
3	Administrator Konten (*Content Administrator*)	Penentuan kebijakan konten	Dinas
Content Management / Pengelola konten *web*			
4.	Penulis (*Author*)	Membangun konten portal *web* (*website*)	Dinas, PPID Perangkat Daerah, Penanggungjawab portal
5.	Penyunting (*Editor*)	Merawat konten portal *web* (*website*)	Dinas
Web Development / Pengembang *website*			
6	Pengembang *web* (*Web Developer*)	Membangun portal *web* (*website*)	
a.	Arsitek *web* (*Web Architect*)	Desain portal *web* (*website*)	Dinas, Perangkat Daerah
b.	Pemogram *web* (*Web Programmer*)	Membuat aplikasi	Dinas, Perangkat Daerah
c.	Administrator Basis Data (*Database Administrator*)	Merancang basis data (*database*) aplikasi	Dinas, Perangkat Daerah
d.	Desainer grafis/ Desainer multimedia (*Graphic Designer/ Multimedia Designer*)	Membuat grafis, gambar, tipografi, animasi, dan multimedia	Dinas, Perangkat Daerah

1) Pengelola *web* utama (*webmaster*)

Pengelola web utama (webmaster) bertanggung jawab sebagai berikut:

a) Merencanakan, mengembangkan, mengelola, dan mengevaluasi portal *web* (*website*) secara berkelanjutan.

b) Menyusun Prosedur Operasional Standar Pengelolaan portal *web* (*website*),

c) Menetapkan persyaratan teknis portal *web* (*website*),

d) Menentukan situs terkait,

e) Memberikan pelayanan dan perawatan yang berkaitan

dengan portal *web* (*website*),

f) Memelihara dan melakukan pembaharuan kode web

2) Administrator *web* (*web Administrator*)

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

a) Membantu *webmaster* dalam merencanakan, mengembangkan, mengelola, dan mengevaluasi portal *web* (*website*) secara berkelanjutan serta menyusun Prosedur Operasional Standar,

b) Mengelola hak akses pengguna ke portal *web* (*website*),

c) Melakukan koordinasi dengan Perangkat Daerah dan Unit Kerja terkait dalam pengelolaan portal *web* (*website*),

d) Melakukan cadangan (*back up*) sistem dan data.

3) Administrator konten (*content administrator*)

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

a) Membuat, menyiapkan, dan mengelola konten baru untuk setiap Perangkat Daerah dan unit kerja,

b) Menyusun Prosedur Operasional Standar penyusunan konten portal *web* (*website*).

4) Penulis (*author*)

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

5) Penyunting (*editor*)

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

6) Pengembang *web* (*web developer*)

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

a) Merencanakan dan membangun dalam pengembangan portal *web* (*website*).

b) Membuat Petunjuk Teknis Penggunaan portal *web* (*website*).

Pengembang *web* (*web developer*) terdiri atas:

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

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

- Membuat rancangan dan menentukan struktur bagian- bagian portal *web* (*website*) yang akan dibuat.
- Menentukan skema/hierarki tautan (*link-link*) yang akan dibuat, dan layanan yang akan diberikan ke publik serta menentukan pola portal *web* (*website*).

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

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

- Membuat dan melakukan pengaturan (*setup*) layanan interaktif dalam lingkungan portal web (*website*),
- Menjalankan program-program yang ada dalam portal web (*website*).

c. Administrator basis data (*database administrator*)

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

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

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

c. Pengelola Portal *Web* (*Website*) Pemerintah Provinsi

Susunan dan tugas pokok serta fungsi pengelola portal *web*

(*website*) Pemerintah Provinsi ditetapkan oleh Gubernur Melalui Keputusan Gubernur.

C. Media Sosial

1. Umum

Media Sosial dan menjadi salah satu sarana dalam rangka meningkatkan pelayanan informasi kepada masyarakat dan juga dapat digunakan untuk menggali dan mengumpulkan informasi secara langsung dari masyarakat. Pelayanan Informasi publik melalui media sosial memerlukan ketentuan yang dapat dijadikan pedoman oleh Dinas selaku penanggung jawab akun Media Sosial Pemerintah Provinsi dan Perangkat Daerah selaku penanggung jawab akun Media Sosial Perangkat Daerah.

2. Ruang Lingkup

Ruang lingkup pengelolaan Media Sosial Pemerintah Provinsi meliputi penetapan penanggungjawab dan pengelola Media Sosial Provinsi dan Perangkat Daerah, penataan konten dan kalender konten media sosial.

3. Tujuan dan Sasaran

Pedoman pengelolaan media sosial bertujuan untuk :

a. Menciptakan keterbukaan, komunikasi yang efektif dan interaktif, serta saling menguntungkan antara instansi dan pemangku kepentingan dalam penyelenggaran informasi publik Pemerintah Provinsi
b. Meningkatkan pelayanan informasi di Perangkat Daerah untuk menghasilkan layanan informasi yang berkualitas; dan
c. Menjamin terwujudnya tujuan penyelenggaraan keterbukaan informasi sesuai ketentuan peraturan perundang-undangan

Sasaran Pedoman Pengelolaan Media Sosial meliputi :

a. Tercapainya kesamaan pemahaman pengelolaan media sosial sebagai salah satu piranti hubungan masyarakat di pemerintah Provinsi;

b. Terselenggaranya hubungan yang harmonis dan saling menguntungkan antara Pemerintah Provinsi dan media;
c. Terwujudnya keterpanduan pengelolaan media sosial secara optimal, efektif dan efisien; dan
d. Terciptanya media sosial yang menghasilkan reputasi instansi yang semakin baik.

4. Kebijakan
   a. Penunjukan akun media sosial resmi instansi dan penunjukan petugas dan pejabat yang bertanggung jawab terhadap pengelolaan media sosial, ditetapkan dengan Keputusan Gubernur
   b. Peraturan Gubernur ini dimaksudkan sebagai pedoman dan acuan bagi instansi dalam mengelola media sosial
   c. Gubernur melalui dinas membentuk Tim Kerja Media Sosial Provinsi Gorontalo
5. Tanggung Jawab

   Pihak-pihak yang memiliki tanggungjawab pengelolaan Media Sosial adalah :
   a. Dinas wajib membentuk Tim Kerja Media Sosial yang terdiri dari Unsur Dinas dan Perangkat Daerah
   b. Tim Kerja Media Sosial terdiri dari Ketua, Wakil Ketua, Sekretaris, Penyelia dan Anggota
6. Asas

   Pengelolaan Media Sosial dilaksanakan berdasarkan asas:
   a. Faktual, yaitu informasi yang disampaikan melalui Media Sosial berlandaskan pada data dan fakta yang jelas dengan mempertimbangan kepentingan umum;
   b. Keikutsertaan dan keterlibatan, yaitu penyampaian informasi melalui media sosial yang diarahkan untuk mendorong keikutsertaan dan keterlibatan khalayak dengan cara memberikan komentar, tanggapan dan masukan kepada Pemerintah Provinsi;
   c. Dapat diakses dengan mudah dan diketahui oleh siapa saja,

kapan saja, dimana saja dalam menyampaikan pesan secara benar, jujur dan apa adanya.

7. Prinsip

Pengelolaan Media Sosial menggunakan prinsip :

a. Kredibel, yaitu menjaga kredibilitas sehingga informasi yang disampaikan akurat, berimbang, keterwakilan;
b. Integritas, yaitu menunjukan sikap jujur dan menjaga etika;
c. Profesional, yaitu memiliki pendidikan, keahlian dan keterampilan di bidangnya;
d. Responsif, yaitu menanggapi masukan dengan cepat dan tepat;
e. Terintegrasi, yaitu menyeleraskan penggunaan media sosial dengan komunikasi lainnya, baik yang berbasis internet maupun yang tidak berbasis internet; dan
f. Keterwakilan, yaitu pesan yang disampaikan mewakili kepentingan instansi, bukan kepentingan pribadi.

8. Manfaat dan Sasaran

Pengelolaan Media Sosial bermanfaat untuk meningkatkan pengertian dan pemahaman penggunaan media sosial pada instansi dalam :

a. Menyebarluaskan informasi Pemerintah Provinsi agar menjangkau masyarakat;
b. Membangun peran Aparatur Sipin Negara dan masyarakat melalui media sosial;
c. Mensosialisasikan strategi dan tujuan pembangunan dimasa depan;
d. Meningkatkan kesadaran dan peran serta masyarakat terhadap kebijakan dan program Pemerintah Provinsi; dan
e. Menggali aspirasi, opini, dan masukan masyarakat terhadap kebijakan dan program Pemerintah Provinsi.

9. Strategi Pengelolaan Media Sosial

Pengelolaan Media Sosial dilakukan dengan strategi merancang pesan yang tepat untuk khalayak sasaran dan menyebarluaskan

pada media sosial yang telah ditetapkan pada masing-masing instansti.

Pengelolaan media sosial dilaksanakan dengan langkah-langkah sebagai berikut :

a. Menentukan khalayak sasaran yang tepat sesuai dengan segmentasi teknografis;
b. Memilih dan membuat akun media sosial yang sesuai dengan khalayak sasaran;
c. Menunjuk akun media sosial resmi Pemerintah Provinsi dan Perangkat Daerah.
d. Menunjuk petugas dan pejabat yang bertanggung jawab terhadap pengelolaan Media Sosial yang disebut dengan Tim Kerja Media Sosial Pemerintah Provinsi
e. Membuat dan mengunggah pesan dengan melakukan tagging;
f. Memantau percakapan;
g. Menjawab komentar, masukan atau pertanyaan khalayak
h. Menganalisis dan menyarikan seluruh masukan khalayak sebagai umpan balik bagi pembuatan/perbaikan kebijakan;
i. Memberikan rekomendasi tindak lanjut kegiatan, program atau kebijakan sesuai dengan masukan dan aspirasi khalayak; dan
j. Menyebarluaskan kebijakan dan tindak lanjut pelaksanaan program.

10. Jenis-Jenis Media Sosial Resmi Pemerintah Provinsi
    a. Microblog, yakni situs media sosial yang memungkinkan para penggunanya menyampaikan pesan pendek, diantaranya adalah situs mikroblog twitter. akun resmi Pemerintah Provinsi untuk microblog twitter adalah @ProvGorontalo atau twitter.com/ProvGorontalo
    b. Situs Media Sharing, yakni situs yang memungkinkan pengguna menyebarkan konten berupa gambar dan video seperti instagram dan youtube. Akun resmi Pemerintah Provinsi adalah youtube.com/ProvinsiGorontalo dan instagram.com/ProvinsiGorontalo

c. Situs Jejaring Sosial, yaitu situs yang menghimpun anggotanya berdasarkan kesamaan tertentu seperti kesamaan minat, hobi, sekolah dan asal usul. Akun resmi Pemerintah Provinsi adalah facebook.com/PemerintahProvinsiGorontalo

11. Konten

Konten dan Pesan yang disebut juga dengan kalemder Konten akan dibuat dan diunggah pada Media Sosial antara lain :

a. Informasi terkait kegiatan Pemerintah Provinsi dan Perangkat Daerah;
b. Isu aktual yang terjadi di Provinsi Gorontalo
c. Kebijakan Pemerintah Pusat dan Kebijakan Pemerintah Provinsi
d. Informasi Pemerintah Pusat
e. Informasi mengenai kondisi negara dan kejadian
f. Informasi hari-hari nasional dan kegiatan nasional

12. Laporan

a. Tim Kerja Media Sosial Provinsi wajib membuat dan menyediakan laporan layanan informasi melalui media sosial, paling sedikit 1 laporan dalam 1 tahun
b. Laporan memuat diantaranya :
   1) Gambaran umum kebijakan pelayanan informasi melalui media sosial yang dimiliki;
   2) Jumlah khalayak
   3) Pembahasan mengenai isi pesan;
   4) Komentar tentang isi pesan;
   5) Jumlah sharing dan pesan yang dikirimkan;
   6) Jumlah pesan yang diteruskan
   7) Kendala eksternal dan internal dalam pelaksanaan layanan informasi; dan
   8) Rekomendasi dan rencana tindak lanjut untuk meningkatkan kualitas pelayanan informasi melalui media sosial.

13. Kerja Media Sosial Provinsi Gorontalo sebagaimana dimaksud pada Diktum KESATU terdiri dari Pengarah, Penanggung jawab, dan Pelaksana, mempunyai tugas sebagai berikut :

a. PENGARAH

1) Memberikan arahan dan menetapkan kebijakan serta rencana pelaksanaan program pengelolaan Media Sosial Provinsi Gorontalo;
2) Melakukan pengawasan terhadap pelaksanaan program pengelolaan media sosial Provinsi Gorontalo.

b. PENANGGUNG JAWAB
1) Bertanggungjawab dan melaporkan pelaksanaan kegiatan kepada Kepala Dinas Komunikasi, Informatika dan Statistik Provinsi Gorontalo;
2) Menetapkan teknis pelaksanaan program pengelolaan media sosial Provinsi Gorontalo;
3) Memastikan pelaksanaan program pengelolaan media sosial Provinsi Gorontalo;
4) Melakukan pengawasan dan evaluasi program pengelolaan media sosial Provinsi Gorontalo.

c. PELAKSANA, terdiri atas :
a. KETUA
1) Mengkoordinasikan pelaksanaan program pengelolaan sosial media;
2) Mengkoordinasikan informasi yang akan disebarluaskan dengan OPD untuk mendapatkan data dan informasi yang akurat;
3) Melakukan koordinasi dalam memberikan data dan informasi dari pertanyaan, saran keluhan yang ada di media sosial, twitter, facebook, instagram, telegram, whatsapp dan youtube Pemerintah Provinsi Gorontalo;
4) Melakukan pengawasan dalam pengelolaan media sosial Provinsi Gorontalo dan tindak lanjut hasil pelaporan.

b. WAKIL KETUA
1) Melakukan rapat koordinasi dengan OPD di lingkungan Pemerintah Provinsi Gorontalo untuk membahas Kalender Konten Media Sosial;
2) Menyusun dan menyampaikan laporan hasil pengelolaan media sosial Provinsi Gorontalo kepada pimpinan untuk menjadi bahan tindak lanjut;

3) Memproses hasil pengelolaan media sosial Provinsi Gorontalo untuk ditindaklanjuti.

c. SEKRETARIS

1) Membuat notulen dari hasil Rapat koordinasi dengan OPD di lingkungan Pemerintah Provinsi Gorontalo untuk membahas Kelander Konten Media Sosial
2) Membuat laporan hasil pengelolaan media sosial Provinsi Gorontalo kepada pimpinan untuk menjadi bahan tindak lanjut;
3) Menyiapkan materi Media Sosial Provinsi Gorontalo
4) Menghimpun bahan informasi publik terkait Pemerintah Provinsi Gorontalo, yang dianggap penting untuk disebarkan melalui konten media sosial.

d. PENYELIA

1) Mengelola dan menyimpan user kredential media sosial, berupa *username, password, email* dan nomor telepon yang terhubung dengan media sosial Provinsi Gorontalo;
2) Melakukan konfigurasi pengamanan akun media sosial Provinsi Gorontalo;
3) Melakukan konfigurasi koneksi akun media sosial Provinsi Gorontalo dengan media lainnya (website dan aplikasi sejenis);
4) Mengaktifasi akun media sosial di setiap perangkat pelaksana Tim Kerja Media Sosial Provinsi Gorontalo;
5) Menonaktifkan akun media sosial di setiap perangkat pelaksana Tim Kerja Media Sosial Provinsi Gorontalo yang tidak lagi menjalankan tugas dalam Surat Keputusan ini;
6) Memeriksa dan menghapus serta melaporkan konten publikasi yang tidak sesuai dengan kebutuhan dan tujuan media sosial Provinis Gorontalo.

e. ANGGOTA

1) Memberikan pelayanan informasi kepada publik/masyarakat luas di Media Sosial twitter, facebook, instagram, telegram, whatsapp dan youtube Provinsi Gorontalo;
2) Melakukan pengelolaan media sosial Provinsi Gorontalo meliputi pembuatan konten kata, konten gambar dan konten videografis;

3) Mengumpulkan bahan informasi publik terkait Provinsi Gorontalo, yang dianggap penting untuk disebarkan melalui konten media sosial;
4) Membuat saran-saran yang berkaitan dengan pengelolaan media sosial Provinsi Gorontalo kepada pimpinan;
5) Memonitor isu-isu seputar Provinsi Gorontalo di media sosial dan melaporkan isu-isu yang dirasa dan dinilai strategis atau berpotensi kritis kepada pimpinan;
6) Menyebarluaskan lebih lanjut informasi yang telah dipublikasikan melalui media sosial twitter, facebook, instagram, telegram, whatsapp dan youtube Provinsi Gorontalo dengan akun media sosial pribadi

DITANDA TANGANI SECARA ELEKTRONIK OLEH :

RUSLI HABIBIE
Gubernur Gorontalo