SALINAN

GUBERNUR DAERAH ISTIMEWA YOGYAKARTA

PERATURAN GUBERNUR DAERAH ISTIMEWA YOGYAKARTA
NOMOR 2 TAHUN 2018
TENTANG
TATA KELOLA TEKNOLOGI INFORMASI DAN KOMUNIKASI

DENGAN RAHMAT TUHAN YANG MAHA ESA

GUBERNUR DAERAH ISTIMEWA YOGYAKARTA,

Menimbang :

a. bahwa tata kelola teknologi informasi dan komunikasi merupakan salah satu unsur penunjang untuk mewujudkan penyelenggaraan pemerintahan yang akuntabel, transparan, efektif, dan efisien guna meningkatkan kualitas pelayanan kepada masyarakat;
b. bahwa perlu dilakukan penataan dalam tata kelola teknologi informasi dan komunikasi agar selaras dengan visi dan misi Pemerintah Daerah;
c. bahwa peraturan perundang-undangan belum mengatur secara terperinci mengenai tata kelola teknologi informasi dan komunikasi;
d. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a, huruf b, dan huruf c, perlu menetapkan Peraturan Gubernur tentang Tata Kelola Teknologi Informasi dan Komunikasi;

Mengingat :

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

2. Undang-Undang Nomor 3 Tahun 1950 tentang Pembentukan Daerah Istimewa Jogjakarta (Berita Negara Republik Indonesia Tahun 1950 Nomor 3) sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 9 Tahun 1955 tentang Perubahan Undang-Undang Nomor 3 Jo. Nomor 19 Tahun 1950 tentang Pembentukan Daerah Istimewa Jogjakarta (Lembaran Negara Republik Indonesia Tahun 1955 Nomor 43, Tambahan Lembaran Negara Republik Indonesia Nomor 827);
3. Undang-Undang Nomor 13 Tahun 2012 tentang Keistimewaan Daerah Istimewa Yogyakarta (Lembaran Negara Republik Indonesia Tahun 2012 Nomor 170, Tambahan Lembaran Negara Republik Indonesia Nomor 5339);
4. Undang-Undang Nomor 23 Tahun 2014 tentang Pemerintahan Daerah (Lembaran Negara Republik Indonesia Tahun 2014 Nomor 244, Tambahan Lembaran Negara Republik Indonesia Nomor 5587), sebagaimana telah diubah 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);
5. Peraturan Pemerintah Nomor 31 Tahun 1950 tentang Berlakunya Undang-Undang Nomor 2, 3, 10 dan 11 Tahun 1950 (Berita Negara Republik Indonesia Tahun 1950 Nomor 58);
6. Peraturan Menteri Komunikasi dan Informatika Nomor: 41/PER/M.KOMINFO/11/2007 tentang Panduan Umum Tata Kelola Teknologi Informasi dan Komunikasi Nasional;

MEMUTUSKAN :

Menetapkan : PERATURAN GUBERNUR TENTANG TATA KELOLA TEKNOLOGI INFORMASI DAN KOMUNIKASI.

BAB I
KETENTUAN UMUM

Pasal 1

Dalam Peraturan Gubernur ini yang dimaksud dengan:

1. Informasi adalah keterangan, pernyataan, gagasan, dan tanda-tanda yang mengandung nilai, makna, dan pesan, baik data, fakta maupun penjelasannya yang dapat dilihat, didengar, dan dibaca yang disajikan dalam berbagai kemasan dan format sesuai dengan perkembangan teknologi informasi dan komunikasi secara elektronik ataupun nonelektronik.
2. Komunikasi adalah proses penyampaian informasi, pesan, ide, gagasan dari satu pihak kepada pihak lain untuk mencapai tujuan tertentu.
3. Teknologi Informasi dan Komunikasi yang selanjutnya disingkat TIK adalah segala kegiatan yang terkait dengan pemrosesan, manipulasi, pengelolaan, dan pemindahan informasi antar media.
4. Tata Kelola TIK adalah kerangka kerja yang mengatur proses perencanaan, pelaksanaan, pemantauan dan evaluasi TIK untuk mendukung visi dan misi Pemerintah Daerah Daerah Istimewa Yogyakarta.
5. Rencana Strategis TIK yang selanjutnya disebut Renstra TIK adalah dokumen yang berisi rencana pengembangan TIK di Pemerintah Daerah Daerah Istimewa Yogyakarta pada periode yang sama dengan periode Rencana Pembangunan Jangka Menengah Daerah Daerah Istimewa Yogyakarta.
6. Integrasi Antar Aplikasi TIK adalah proses menghubungkan atau menyatukan beberapa aplikasi TIK ke dalam sebuah aplikasi TIK.

7. *Application Programming Interface* untuk selanjutnya disingkat API adalah teknologi yang digunakan untuk memfasilitasi pertukaran informasi atau data antara dua atau lebih aplikasi perangkat lunak.
8. *Network Operation Center* untuk selanjutnya disingkat NOC adalah sebuah lokasi terpusat yang digunakan untuk melakukan pengelolaan dan pengawasan jaringan internet dan intranet Pemerintah Daerah Daerah Istimewa Yogyakarta.
9. Kode Sumber adalah suatu rangkaian pernyataan atau deklarasi yang ditulis dalam bahasa pemrograman komputer yang dikembangkan oleh OPD maupun oleh penyedia jasa aplikasi.
10. Keamanan Informasi adalah suatu kondisi dimana terjaganya aspek kerahasiaan, integritas dan ketersediaan dari informasi.
11. *Bandwidth* adalah besaran yang menunjukkan seberapa banyak data yang dapat dilewatkan dalam koneksi melalui sebuah jaringan.
12. *Data Center* adalah sekumpulan fasilitas tersertifikasi yang digunakan untuk penempatan sistem elektronik dan komponen terkait lainnya untuk keperluan penempatan, penyimpanan, dan pengolahan data yang dimiliki dan/atau dikelola oleh Pemerintah Daerah Daerah Istimewa Yogyakarta.
13. Daerah adalah Daerah Istimewa Yogyakarta.
14. Gubernur adalah Gubernur Daerah Istimewa Yogyakarta.
15. Pemerintah Daerah adalah Pemerintah Daerah Daerah Istimewa Yogyakarta.
16. Organisasi Perangkat Daerah yang selanjutnya disingkat OPD adalah Organisasi Perangkat Daerah yang terdiri dari Sekretariat Daerah, Sekretariat DPRD, Badan Perencanaan Pembangunan Daerah, Inspektorat, Satuan Polisi Pamong Praja, Dinas Daerah, Lembaga Teknis Daerah, dan Lembaga Lain.

Pasal 2

(1) Maksud disusunnya Peraturan Gubernur ini yaitu sebagai pedoman bagi OPD dalam pengelolaan TIK.
(2) Tujuan disusunnya Peraturan Gubernur ini yaitu:
    a. mewujudkan keselarasan antara pengelolaan TIK di OPD dengan kebijakan Pemerintah Daerah;
    b. mewujudkan sinkronisasi dan integrasi pengelolaan TIK; dan
    c. memastikan implementasi TIK berjalan dengan baik dan berkelanjutan.

Pasal 3

Ruang lingkup Peraturan Gubernur ini meliputi:
a. perencanaan TIK;
b. pelaksanaan TIK; dan
c. pemantauan dan evaluasi pengelolaan TIK.

BAB II

PERENCANAAN TIK

Pasal 4

(1) Dinas Komunikasi dan Informatika wajib menyusun perencanaan TIK.
(2) Perencanaan TIK sebagaimana dimaksud ayat (1) diwujudkan dalam Renstra TIK untuk jangka waktu 5 (lima) tahun.
(3) Renstra TIK sebagaimana dimaksud pada ayat (2) paling sedikit memuat:
    a. visi misi;
    b. sasaran dan target pengembangan TIK;
    c. kebijakan dan strategi pengembangan TIK;
    d. arsitektur TIK;
    e. proses kerja di masing-masing OPD;
    f. data dan layanan informasi OPD;
    g. rencana integrasi data dan layanan;
    h. rencana pengembangan TIK;
    i. strategi implementasi pengembangan TIK; dan
    j. *roadmap* implementasi TIK di Pemerintah Daerah.

(4) Penyusunan Renstra TIK sebagaimana dimaksud pada ayat (2) dilakukan dengan tahapan:

a. Dinas Komunikasi dan Informatika mengumpulkan data dukung yang diperlukan untuk penyusunan Renstra TIK dari OPD;

b. data dukung sebagaimana dimaksud pada huruf a meliputi:

1. Renstra OPD;
2. proses kerja OPD meliputi:
   a. gambaran umum;
   b. identifikasi dan analisis kebutuhan;
   c. perancangan;
   d. pengembangan dan pengujian;
   e. implementasi;
   f. pemantauan dan evaluasi;
   g. pemeliharaan;
3. data dan informasi yang dikelola OPD;
4. sarana dan prasarana TIK yang dimiliki dan dikelola OPD;
5. SOP dan peraturan terkait proses kerja OPD; dan
6. usulan OPD terkait pengembangan TIK.

c. Dinas Komunikasi dan Informatika menyelaraskan dokumen pendukung sebagaimana dimaksud pada huruf b dengan mempertimbangkan:

1. visi misi Pemerintah Daerah sebagaimana tercantum dalam Rencana Pembangunan Jangka Panjang Daerah, Rencana Pembangunan Jangka Menengah Daerah;
2. kesesuaian penerapan TIK dengan perkembangan kebutuhan Pemerintah Daerah; dan
3. kesesuaian dengan perkembangan TIK.

(5) Berdasarkan penyelarasan sebagaimana dimaksud pada ayat (4) huruf c Dinas Komunikasi dan Informatika mengajukan Renstra TIK kepada Gubernur untuk ditetapkan.

Pasal 5

(1) Renstra TIK sebagaimana dimaksud dalam Pasal 4 ayat (2) dapat diubah dengan pertimbangan:
   a. perkembangan teknologi;
   b. perubahan SOTK;
   c. perubahan kebijakan nasional terkait TIK; dan
   d. perubahan Rencana Pembangunan Jangka Menengah Daerah.

(2) Perubahan Renstra TIK dilakukan dengan tahapan:
   a. OPD mengusulkan perubahan Renstra TIK kepada Dinas Komunikasi dan Informatika;
   b. Dinas Komunikasi dan Informatika menganalisis usulan perubahan Renstra TIK;
   c. berdasarkan analisis sebagaimana dimaksud pada huruf b Dinas Komunikasi dan Informatika:
      1. menolak rencana perubahan Renstra TIK
      2. menyetujui rencana perubahan Renstra TIK.
   d. Dalam hal rencana perubahan TIK disetujui, Dinas Komunikasi dan Informatikan mengajukan Perubahan Renstra TIK kepada Gubernur untuk ditetapkan.

BAB III

PELAKSANAAN TIK

Bagian Kesatu

Umum

Pasal 6

(1) Pelaksanaan TIK meliputi:
   a. pelaksanaan investasi TIK;
   b. pelaksanaan pengelolaan aset TIK;
   c. pelaksanaan layanan TIK;
   d. pelaksanaan pengelolaan keamanan informasi;
   e. pelaksanaan pengelolaan risiko dan keberlangsungan bisnis; dan
   f. pelaksanaan kepatuhan dan penilaian internal.

(2) Dalam pelaksanaan TIK sebagaimana dimaksud pada ayat (1), OPD berkoordinasi dengan Dinas Komunikasi dan Informatika.

Bagian Kedua

Pelaksanaan Investasi TIK

Pasal 7

(1) OPD melaksanakan investasi TIK sebagaimana dimaksud dalam Pasal 6 ayat (1) huruf a dengan mempertimbangkan:
   a. capaian program;
   b. kebutuhan program;
   c. keluaran program;
   d. nilai investasi; dan
   e. kerangka acuan kerja.

(2) Dalam melakukan pelaksanaan investasi TIK sebagaimana dimaksud pada ayat (1), OPD melakukan:
   a. analisis kebutuhan;
   b. analisis biaya; dan
   c. analisis manfaat dari belanja TIK yang direncanakan.

(3) Berdasarkan pertimbangan dan analisis sebagaimana dimaksud pada ayat (1) dan ayat (2), OPD mengajukan permohonan rekomendasi pelaksanaan investasi TIK kepada Dinas Komunikasi dan Informatika.

(4) Dinas Komunikasi dan Informatika menganalisis permohonan rekomendasi pelaksanaan investasi TIK dengan mengacu pada Renstra TIK.

(5) Berdasarkan hasil analisis sebagaimana dimaksud pada ayat (4) Dinas Komunikasi dan Informatika:
   a. menerbitkan rekomendasi; atau
   b. menolak permohonan.

(6) Dalam hal permohonan rekomendasi disetujui, OPD mencantumkan pelaksanaan investasi TIK yang berupa daftar kebutuhan investasi dalam rencana kerja anggaran.

(7) Dalam hal permohonan rekomendasi ditolak, OPD melakukan penyesuaian atas pelaksanaan investasi TIK dalam rencana kerja anggaran sesuai saran Dinas Komunikasi dan Informatika.

(8) Format permohonan rekomendasi dan format rekomendasi sebagaimana dimaksud pada ayat (3) dan ayat (5) huruf a tercantum dalam Lampiran Huruf A dan Lampiran Huruf B yang merupakan bagian tidak terpisahkan dari Peraturan Gubernur ini.

Bagian Ketiga

Pelaksanaan Pengelolaan Aset TIK

Pasal 8

(1) OPD melaksanakan pengelolaan aset TIK sebagaimana dimaksud dalam Pasal 6 ayat (1) huruf b meliputi pengelolaan:
   a. sumber daya manusia;
   b. data dan informasi;
   c. aplikasi; dan
   d. infrastruktur.

(2) Pelaksanaan pengelolaan aset TIK sebagaimana dimaksud pada ayat (1) didokumentasikan sesuai dengan format sebagaimana tercantum dalam Lampiran Huruf C yang merupakan bagian tidak terpisahkan dari Peraturan Gubernur ini.

Paragraf 1

Pelaksanaan Pengelolaan Sumber Daya Manusia

Pasal 9

OPD melaksanakan pengelolaan sumber daya manusia sebagaimana dimaksud dalam Pasal 8 huruf a dengan cara:

a. melakukan pemetaan kompetensi TIK personel OPD;
b. pimpinan OPD menunjuk personel pengelola TIK di internal OPD berdasarkan hasil pemetaan sebagaimana dimaksud pada huruf a;
c. membuat analisis kebutuhan pelatihan dengan cara membandingkan antara kebutuhan kompetensi dengan hasil pemetaan kompetensi TIK;
d. membuat rencana program pelatihan peningkatan kompetensi personel; dan
e. memberikan fasilitasi kepada personel yang memiliki kompetensi TIK berupa pelatihan atau pendidikan pengelolaan TIK.

Paragraf 2

Pelaksanaan Tata Kelola Data dan Informasi

Pasal 10

(1) OPD melaksanakan tata kelola data dan informasi sebagaimana dimaksud dalam Pasal 8 huruf b dengan cara:
   a. membuat daftar data dan informasi yang dikelola;
   b. membuat daftar penanggungjawab 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;
   b. internal; dan
   c. rahasia.

(4) Klasifikasi sebagaimana dimaksud pada ayat (3) dilaksanakan sesuai dengan ketentuan peraturan perundang-undangan.

Paragraf 3

Pelaksanaan Pengelolaan Aplikasi TIK

Pasal 11

(1) OPD melaksanakan pengelolaan aplikasi TIK sebagaimana dimaksud dalam Pasal 8 huruf c dengan mengacu pada standar pengelolaan telematika yang disusun dan ditetapkan oleh Kepala Dinas Komunikasi dan Informatika.
(2) Pengelolaan aplikasi TIK sebagaimana dimaksud pada ayat (1) meliputi:
    a. pembangunan dan pengembangan aplikasi;
    b. pemeliharaan aplikasi; dan
    c. pengelolaan Kode Sumber.

Pasal 12

(1) OPD membangun dan mengembangkan aplikasi TIK dengan mengutamakan Integrasi Antar Aplikasi TIK.
(2) Untuk mendukung proses integrasi, OPD wajib menyediakan API dalam pengembangan aplikasi
(3) Selain menyediakan API sebagaimana dimaksud pada ayat (2), OPD yang membangun dan mengembangkan aplikasi TIK membuat dokumentasi pengembangan sistem meliputi:
    a. struktur basis data dan relasinya;
    b. diagram alir data;
    c. fungsi dan modul yang terdapat dalam aplikasi;
    d. spesifikasi teknis aplikasi; dan
    e. manual penggunaan aplikasi.

Pasal 13

OPD melaksanakan pemeliharaan aplikasi dengan cara menjaga, memperbaiki, dan mencegah kerusakan aplikasi.

Pasal 14

OPD mengelola Kode Sumber dengan cara:

a. membuat salinan Kode Sumber;
b. memastikan hak cipta Kode Sumber berada pada OPD pemilik aplikasi; dan
c. menyimpan Kode Sumber.

Pasal 15

(1) OPD wajib meletakkan aplikasi pada *Data Center.*

(2) Peletakan aplikasi pada Data Center sebagaimana dimaksud pada ayat (1) dilakukan dengan tahapan:
   a. OPD mengajukan permohonan peletakan aplikasi *Data Center* kepada Dinas Komunikasi dan Informatika;
   b. Dinas Komunikasi dan Informatika melakukan uji keamanan dan kelayakan;
   c. Dinas Komunikasi dan Informatika melakukan analisis hasil dari uji keamanan dan kelayakan; dan
   d. berdasarkan hasil analisis sebagaimana dimaksud pada huruf c, Dinas Komunikasi dan Informatika menentukan:
      1. aplikasi dapat diletakkan di *Data Center*; atau
      2. aplikasi dikembalikan pada OPD yang mengajukan permohonan.

Paragraf 4

Pelaksanaan Tata Kelola Infrastruktur

Pasal 16

(1) Pengelolaan infrastruktur sebagaimana dimaksud dalam Pasal 8 huruf d dilakukan oleh:
   a. Dinas Komunikasi dan Informatika; dan
   b. OPD.

(2) Dinas Komunikasi dan Informatika mengelola infrastruktur TIK untuk seluruh OPD meliputi :
   a. *Data Center* dan perangkat pendukungnya; dan
   b. Jaringan internet dan intranet dari *NOC* Pemerintah Daerah ke OPD.

(3) Pengelolaan infrastruktur TIK sebagaimana dimaksud pada ayat (2) dilakukan dengan cara:
   a. melakukan analisis kebutuhan *Bandwidth* Pemerintah Daerah;
   b. mengatur pembagian *Bandwidth* ke OPD dari NOC; dan
   c. melakukan pengawasan dan pengendalian penggunaan *Bandwidth* Pemerintah Daerah.

Pasal 17

(1) OPD menyediakan dan mengelola infrastruktur TIK untuk kebutuhan OPD meliputi:
   a. perangkat jaringan antara lain:
      1. *hub;*
      2. *router;*
      3. *switch;*
      4. *access point;*
      5. perangkat wifi; dan
      6. kabel jaringan.
   b. perangkat operasional OPD antara lain:
      1. komputer;
      2. laptop/*notebook;*
      3. *printer*;
      4. *scanner*;
      5. cctv; dan
      6. perangkat penyimpan data eksternal.

(2) OPD yang memasang perangkat jaringan dan perangkat operasional yang terhubung ke jaringan wajib berkoordinasi dengan Dinas Komunikasi dan Informatika.

(3) Penyediaan dan pengelolaan infrastruktur TIK mengacu pada standar pengelolaan telematika sebagaimana dimaksud dalam Pasal 11.

Bagian Keempat

Pelaksanaan Layanan TIK

Pasal 18

(1) OPD melaksanakan layanan TIK sebagaimana dimaksud dalam Pasal 6 ayat (1) huruf c dengan cara menyusun prosedur pengelolaan layanan TIK yang dilaksanakan pada masing-masing OPD.

(2) Pengelolaan layanan TIK sebagaimana dimaksud pada ayat (1) merupakan layanan yang diberikan OPD kepada pihak lain dengan memanfaatkan TIK sebagai alat bantu utama.

(3) Prosedur pengelolaan 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 Kelima

Pengelolaan Keamanan Informasi TIK

Pasal 19

(1) OPD melaksanakan pengelolaan keamanan informasi TIK sebagaimana dimaksud dalam Pasal 6 ayat (1) huruf d dengan cara:
   a. menjaga kerahasiaan informasi;
   b. menjaga keutuhan informasi; dan
   c. menjaga ketersediaan informasi.

(2) Penjagaan kerahasiaan informasi sebagaimana dimaksud pada ayat (2) 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) Penjagaan keutuhan informasi sebagaimana dimaksud pada ayat (2) dilakukan melalui:
   a. penerapan metode otentifikasi pada informasi; dan
   b. penerapan teknik/kontrol untuk mendeteksi adanya modifikasi informasi.

(4) Penjagaan ketersediaan informasi sebagaimana dimaksud pada ayat (2) dilakukan melalui:

a. penyediaan *back up* informasi;

b. penyediaan pemulihan sistem informasi; dan

c. penyediaan infrastruktur cadangan.

(5) Rincian lebih lanjut mengenai pengelolaan keamanan informasi TIK mengacu pada Peraturan Gubernur Daerah Istimewa Yogyakarta yang mengatur tentang Sistem Manajemen Keamanan Informasi.

Bagian Keenam

Pengelolaan Risiko dan Keberlangsungan Bisnis TIK

Pasal 20

OPD melaksanakan pengelolaan risiko dan keberlangsungan bisnis sebagaimana dimaksud dalam Pasal 6 ayat (1) huruf e dengan tahapan:

a. identifikasi risiko;
b. analisis risiko;
c. evaluasi risiko; dan
d. penetapan langkah mitigasi dan prioritas pengendalian.

Pasal 21

(1) Berdasarkan pengelolaan risiko sebagaimana dimaksud dalam Pasal 20 OPD wajib menyusun dokumen rencana keberlangsungan bisnis.

(2) Dokumen rencana keberlangsungan bisnis pada ayat (1), paling sedikit memuat:

a. analisis dampak bisnis;
b. analisis risiko; dan
c. penentuan strategi keberlangsungan bisnis.

(3) OPD memastikan rencana keberlangsungan bisnis sebagaimana dimaksud pada ayat (2) melalui uji coba terhadap seluruh sistem dan infrastruktur secara berkala.

Pasal 22

Rincian lebih lanjut mengenai pengelolaan risiko TIK dan penyusunan dokumen keberlangsungan bisnis sebagaimana dimaksud pada ayat (1) tercantum dalam Lampiran Huruf D yang merupakan bagian tidak terpisahkan dari Peraturan Gubernur ini.

Bagian Ketujuh

Pengelolaan Kepatuhan dan Penilaian Internal

Pasal 23

OPD melaksanakan pengelolaan kepatuhan dan penilaian internal sebagaimana dimaksud dalam Pasal 6 ayat (1) huruf f dengan cara :

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

Pasal 24

(1) OPD melakukan pengelolaan kepatuhan dan penilaian internal TIK secara sistematik, terencana, dan terdokumentasi.
(2) Pengelolaan kepatuhan dan penilaian internal TIK sebagaimana dimaksud pada ayat (1) dilakukan untuk melihat tingkat kesesuaian dan keefektifan implementasi pengelolaan TIK yang diterapkan.
(3) Penilaian internal TIK dilakukan oleh personel pengelola TIK sebagaimana dimaksud dalam Pasal 9 huruf b.
(4) Personel pengelola TIK internal OPD melaporkan secara tertulis hasil penilaian internal OPD kepada Kepala OPD dan Dinas Komunikasi dan Informatika setiap tahun.

Pasal 25

Rincian lebih lanjut mengenai kepatuhan dan penilaian internal sebagaimana dimaksud dalam Pasal 23 dan Pasal 24 tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Peraturan Gubernur ini.

BAB IV

PEMANTAUAN DAN EVALUASI

Pasal 26

(1) Dinas Komunikasi dan Informatika melaksanakan pemantauan dan evaluasi terhadap pengelolaan TIK.
(2) Pemantauan dan evaluasi terhadap pengelolaan TIK dilaksanakan melalui proses audit secara sistematis, objektif dan terdokumentasi.
(3) Mekanisme pemantauan dan evaluasi terhadap pengelolaan TIK tercantum dalam Lampiran yang merupakan bagian tidak terpisahkan dari Peraturan Gubernur ini.

BAB V

KETENTUAN PERALIHAN

Pasal 27

OPD yang telah memiliki aplikasi dan perangkat TIK sebelum berlakunya Peraturan Gubernur ini, dalam jangka waktu 1 (satu) tahun wajib menyesuaikan dengan ketentuan dalam Peraturan Gubernur ini.

BAB VI

KETENTUAN PENUTUP

Pasal 28

Peraturan Gubernur ini mulai berlaku pada tanggal diundangkan.

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

Ditetapkan di Yogyakarta

pada tanggal 31 Januari 2018

GUBERNUR

DAERAH ISTIMEWA YOGYAKARTA,

ttd.

HAMENGKU BUWONO X

Diundangkan di Yogyakarta

pada tanggal 31 Januari 2018

SEKRETARIS DAERAH

DAERAH ISTIMEWA YOGYAKARTA,

ttd.

GATOT SAPTADI

BERITA DAERAH DAERAH ISTIMEWA YOGYAKARTA TAHUN 2018 NOMOR 2

Salinan Sesuai Dengan Aslinya
KEPALA BIRO HUKUM,

ttd.

DEWO ISNU BROTO I.S.
NIP. 19640714 199102 1 001

LAMPIRAN
PERATURAN GUBERNUR
DAERAH ISTIMEWA YOGYAKARTA
NOMOR 2 TAHUN 2018
TENTANG
TATA KELOLA TEKNOLOGI INFORMASI
DAN KOMUNIKASI

A. FORMAT PERMOHONAN REKOMENDASI PELAKSANAAN INVESTASI TIK

	Kop instansi	

SURAT PERMOHONAN REKOMENDASI

No :

Nama investasi :
Instansi :
Bidang/Bagian/UPT :

Capaian program	*(sesuai RKA)*
Kebutuhan Program	*(sesuai RKA)*
Keluaran Program	*(sesuai RKA)*
Nilai Investasi	*(sesuai RKA)*
Kerangka Acuan Kerja	*(Uraikan secara detail tentang:* *a. latar belakang* b. *maksud dan tujuan* c. *standar teknis* d. *keluaran)*
Analisis kebutuhan	a. kebutuhan data dan informasi *(Uraikan mengenai data dan informasi apa saja yang dibutuhkan untuk investasi ini. Misal : Data kependudukan, data kepegawaian, dll)* b. kebutuhan fungsional *(Uraikan secara terinci setiap fungsi yang akan dimiliki oleh investasi ini)*
Analisis biaya	a. Biaya pengadaan *(uraikan estimasi kebutuhan biaya untuk investasi ini mulai dari persiapan hingga siap digunakan (nilai investasi di tahun pengadaan))* b. Biaya operasional dan pemeliharaan *(uraikan estimasi kebutuhan biaya untuk beroperasinya investasi serta perawatan investasi (nilai investasi di tahun anggaran berikutnya))*
Analisis manfaat	*(Uraikan peningkatan output yang akan didapat secara kualitatif dan kuantitatif akibat penggunaan investasi ini)*

Demikian permohonan ini dibuat untuk ditindaklanjuti sebagaimana mestinya.

Yogyakarta, …….
Kepala ……..

(Nama NIP)

B. FORMAT REKOMENDASI PELAKSANAAN INVESTASI TIK

	Kop Diskominfo	

SURAT PERSETUJUAN REKOMENDASI

Nomor :

Berdasarkan Surat Permohonan Rekomendasi Investasi TIK …….. Nomor…….. dari ……, maka rencana investasi ini dapat DISETUJUI/TIDAK DISETUJUI dengan alasan ……..

Yogyakarta, …….

[Kepala]

(Nama NIP)

C. PENGELOLAAN ASET TIK

1. Tabel Matriks Kompetensi SDM

MATRIKS KOMPETENSI SDM

No.	Jabatan/Fungsi	Nama	Keahlian				Analisa Kebutuhan Pelatihan	Program Pelatihan		
			Kebutuhan		Ada Saat Ini					
			Kompetensi	Tingkatan	Kompetensi	Tingkatan		Pelatihan	Tingkatan	Waktu
1	Kepala	Pak X	IT Security Management	Advance	IT Service Management	Intermediate	IT Security Management	IT Security Management	Intermediate	2019
			IT Service Management	Intermediate						

2. Tabel Aset Data dan Informasi

ASET DATA DAN INFORMASI

No.	Data Aset			Tanggung Jawab Aset				Karakteristik Aset			Lokasi Penyimpanan	Ket	Periode Backup	Media Backup
	Nama Informasi	Penanggung jawab	Format (Hard copy/ Soft copy)	Dibuat oleh	Digunakan untuk	Wewenang Modifikasi	Personil Penyimpan	Klasifikasi (Publik/ Internal/ Rahasia)	Distribusi (Ya/Tidak)	Masa Retensi				
1	Pergub X	Kepala Dinas X	Soft copy	Dinas X	Pengelolaan X	Kepala Dinas X	Mr X	Publik	Ya	X Tahun	Server Diskominfo	-	X Tahun sekali	Flash disk
2	Data kependudukan	Kepala Seksi X	Soft copy	Dukcapil X	Pengelolaan data kependudukan	-	Kepala Seksi X	Rahasia	Ya	X Tahun	Server Biro X	-	Setiap hari	Server Diskominfo

3. Tabel Aset Aplikasi

ASET APLIKASI

No	Nama Aplikasi	Bidang/Bagian/ UPTD	Penanggung Jawab Teknis	Alamat aplikasi	Lokasi Hosting	Jenis aplikasi	Deskripsi aplikasi
1	Sistem Informasi X	PDTI	Pak X	Xxxxxxx.jogjaprov.go.id	Data center Pemda	Internal	Sistem ……
2	SPSE	Manajemen Informatika	Pak Z	Lpse.jogjaprov.go.id	Data center Pemda	Pelayanan Publik	Sistem …….

4. Tabel Aset Perangkat TIK

ASET PERANGKAT TIK

No.	Data Asset :				Status Aset :		Spesifikasi Aset :							
	Nama Aset	No Aset	Pengguna	Lokasi	Pemilik	Kondisi	Karakteristik : (Fixed/Mobile)	Merk	Type	Serial Number	Prosesor	RAM	Hard Disk	Tahun Pengadaan
1.	Laptop	MI-06.03.05	Bu A	Seksi	Dinas A	Rusak	Mobile	Lenovo Thinkpad	X200CA	As5400-7629-98757-uj76	Intel Core i5	4096 MB	1 TB	2017
2.	Scanner	MI-06.03	Bidang MI	Bidang	Dinas A	Baik	Fixed	Canon	A20	AS658-90YG	-	-	-	2010

5. Tabel Aset Infrastruktur TIK (dibuat oleh OPD yang memiliki Data Center/Server sendiri)

ASET INFRASTRUKTUR TIK

No.	Data Asset :				Status Aset :		Spesifikasi Aset :							
	Nama Aset	No Aset	Pengguna	Lokasi	Pemilik	Kondisi	Karakteristik : (Fixed/Mobile)	Merk	Type	Serial Number	Prosesor	RAM	Hard Disk	Tahun Pengadaan
1.	Server	MI-06.03.06	Bidang MI	Rak 5	Bidang MI	Rusak	Fixed	CISCO	ICS508	As5400-7629-98757-uj76	Xeon	-	1 TB	2017

D. PENGELOLAAN RISIKO DAN KEBERLANGSUNGAN BISNIS TIK

I. Proses Memahami Kebutuhan Organisasi

Proses ini dilakukan dalam dua tahap, yaitu tahap Analisis Dampak Bisnis (*Business Impact Analysis)* dan Penilaian Risiko (*Risk Assesment).* Detail kedua aktivitas tersebut dijelaskan sebagai berikut:

1. Analisis Dampak Bisnis (*business impact analysis*), yang mencakup:
   a. Identifikasi proses / aktifitas bisnis kritikal
   b. Identifikasi dampak dari gangguan terhadap proses / aktifitas bisnis kritikal
   c. Identifikasi jangka waktu maksimal dimana gangguan terhadap proses / aktifitas bisnis dapat ditoleransi (*maximum tolerable downtime* - MTD).

MTD dapat juga dilihat sebagai jangka waktu dimana apabila proses/aktifitas bisnis tidak dapat dipulihkan, perusahaan akan terkena dampak, baik finansial, operasional maupun reputasi, yang tidak dapat diperbaiki (*irreparably damaged*).

MTD dapat diidentifikasi dengan cara mengidentifikasi:

a. Jangka waktu maksimal setelah terjadinya (*starting point*) gangguan dimana aktifitas bisnis kritikal harus sudah dimulai;
b. Tingkat minimum operasional dari aktifitas bisnis kritikal yang harus dijalankan;
c. Jangka waktu maksimal setelah terjadinya (*starting point*) gangguan dimana aktifitas normal dari layanan harus sudah dimulai;
d. Identifikasi prioritas untuk pemulihan aktifitas / proses bisnis;
e. Identifikasi ketergantungan yang dimiliki oleh proses / aktifitas bisnis kritikal tersebut baik internal maupun eksternal. Hal ini mencakup layanan, infrastruktur, pihak ketiga penyedia jasa atau *stakeholder* lainnya;
f. Bagi pihak pemasok atau pihak ketiga penyedia jasa, perlu dipastikan bahwa pengaturan kelangsungan bisnis juga mencakup untuk layanan produk dan jasa yang mereka sediakan untuk perusahaan;
g. Menetapkan *recovery time objective* yang merupakan target waktu pemulihan aktifitas bisnis kritikal. RTO yang ditetapkan harus lebih kecil atau paling tidak sama dengan MTD;
h. Memperkirakan sumber daya yang dibutuhkan untuk setiap aktifitas kritikal yang dibutuhkan untuk memulihkan proses / aktifitas bisnis kritikal tersebut. Yang disebut sebagai sumber daya dapat mencakup namun tidak terbatas pada:
   1) Perangkat keras;
   2) Perangkat lunak (*software*/aplikasi);
   3) Sumber daya manusia (personil);
   4) Jaringan komputer dan komunikasi;

5) Data/informasi;
6) Sarana pendukung (*utilities*).

2. Penilaian risiko (*Risk Assesment)*, proses ini dilakukan dengan cara :

Pelaksanaan penilaian risiko dilakukan dengan tahapan :

a. Identifikasi Risiko

Proses identifikasi risiko dilakukan dengan cara:

1) Mengidentifikasi ancaman.

Ancaman didefinisikan sebagai potensi penyebab insiden yang tidak diinginkan yang dapat menyebabkan kerusakan/kerugian bagi organisasi dan sistemnya. Sebuah ancaman dapat menjadi sebuah risiko pabila dikombinasikan dengan kelemahan yang dapat dieksploitasi.

2) Mengidentifikasi kelemahan.

Proses identifikasi kelemahan dilakukan setelah identifikasi ancaman dilakukan. Kelemahan didefinisikan sebagai potensi kekurangan pada proses dan kontrol keamanan yang dapat diekspoitasi oleh satu ancaman atau lebih.

3) Mengidentifikasi dampak.

Identifikasi dampak dilakukan untuk mengetahui potensi kerugian yang ditanggung organisasi apabila risiko yang teridentifikasi terwujud.

b. Analisis Risiko

Untuk mendukung proses analisa terhadap Risiko, OPD perlu memperhatikan signifikansi dampak risiko yang telah diidentifikasi terhadap kondisi OPD serta frekuensi terjadinya risiko. Metode yang dapat digunakan OPD berupa kuantitatif dimana besarnya dampak dan sering tidaknya kejadian (kecenderungan) dapat dijelaskan secara naratif atau dengan pemberian ranking.

Kriteria dampak merupakan parameter untuk menentukan tingkat kerugian terhadap risiko yang terjadi. Contoh kriteria dampak adalah sebagai berikut :

Tingkat Dampak	Operasional	Peraturan / Hukum	Aset Informasi	Reputasi
1 (Ringan)	Penundaan proses bisnis setengah hari	Tidak ada pelanggaran peraturan / hukum	Tidak ada kebocoran atau kehilangan aset informasi	Tidak ada dampak terhadap reputasi OPD / unit kerja
2 (Sedang)	Penundaan proses bisnis 1 hari	Pelanggaran ringan diselesaikan dengan surat	Berdampak pada kebocoran atau kehilangan aset informasi yang bersifat PUBLIK.	Mengganggu kepercayaan sebagian kecil pihak eksternal. Berdampak pada reputasi OPD / unit

		peringatan		kerja 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 INTERNAL.	Mengganggu kepercayaan sebagian besar pihak eksternal. Berdampak pada reputasi OPD / unit kerja dan pemulihan reputasi membutuhkan waktu yang lama
4 (Sangat Berat)	Penundaan proses bisnis 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 OPD / unit kerja dan sangat sulit dilakukan pemulihan reputasi

Kriteria kecenderungan merupakan parameter untuk menentukan tingkat kecenderungan terhadap risiko. Contoh kriteria kecenderungan adalah sebagai berikut :

Tingkat Kecenderungan	**Frekuensi kejadian**
1 (Rendah)	Kejadian tidak lebih dari 2 kali dalam satu tahun
2 (Sedang)	Kejadian terjadi antara 2 – 5 kali dalam satu tahun
3 (Tinggi)	Kejadian terjadi antara 5 – 10 kali dalam satu tahun
4 (Ekstrim)	Kejadian lebih dari 10 kali dalam satu tahun

c. Evaluasi risiko

Evaluasi risiko adalah kegiatan membandingkan hasil dari analisis risiko dengan kriteria risiko yang ditetapkan. Apabila suatu risiko masuk dalam kriteria penerimaan risiko, maka risiko tersebut akan diterima sedangkan risiko yang tidak masuk dalam kriteria penerimaan risiko perlu mendapatkan penanganan. Setiap penanganan risiko harus diberikan prioritas.

Tabel risiko adalah matriks antara nilai dari dampak dan kecenderungan yang menghasilkan tingkat risiko. Contoh tabel risiko adalah sebagai berikut:

		DAMPAK			
		1	2	3	4
KECENDERUNGAN	1				
	2				
	3				
	4				

Keterangan :

Warna hijau : risiko rendah

Warna kuning : risiko sedang

Warna merah : risiko tinggi

Risiko yang masuk kategori rendah akan diterima oleh organisasi, sedangkan risiko yang masuk kategori sedang dan tinggi, perlu ditentukan strategi keberlangungan layanan untuk mengurangi risiko dan dampak bisnis.

II. Menentukan Strategi Kelangsungan Bisnis

Tujuan dari pemilihan strategi kelangsungan bisnis ini adalah untuk mengurangi keseluruhan dampak insiden dengan cara memperpendek waktu gangguan bisnis dan mengurangi intensitas gangguan.

Strategi kelangsungan Bisnis meliputi 3 (tiga) opsi strategi, yaitu:

1. Proteksi terhadap proses bisnis yang menjadi prioritas

   Strategi proteksi merupakan strategi yang dilakukan agar insiden tidak memiliki dampak pada aktivitas bisnis. Strategi ini biasanya dilakukan sebelum terjadi insiden. Beberapa pilihan strategi proteksi antara lain:

   a. Menghilangkan aktivitas bisnis yang berisiko
   b. Mengganti aktivitas bisnis yang berisiko dengan aktivitas alternatif yang minim risiko
   c. Menggandeng pihak ketiga untuk melakukan aktivitas bisnis yang berisiko.

2. Stabilisasi dan Pemulihan proses bisnis

   Strategi stabilisasi dan pemulihan merupakan pilihan strategi yang dilakukan untuk menjamin keberlangsungan aktivitas bisnis apabila terjadi insiden yang mengganggu proses bisnis organisasi. Beberapa pilihan strategi ini antara lain:

   a. Relokasi aktivitas bisnis ke lokasi lain yang tidak terjadi gangguan
   b. Realokasi dan Relokasi sumber daya
   c. Penyiapan Proses alternatif atau Redundansi aktivitas bisnis dan sumberdaya
   d. Menambah skill karyawan agar dapat mengerjakan pekerjaan diluar tugas pokok dan fungsinya

3. Mitigasi

   Pilihan strategi mitigasi untuk mengurangi dampak dan durasi insiden, antara lain:

   a. Asuransi. Contoh dari asuransi misalnya pembelian garansi untuk produk TIK
   b. Restorasi Aset. Perbaikan asset yang terganggu akibat suatu insiden
   c. Berbagai pilihan strategi tersebut dapat dipilih sekaligus untuk satu proses bisnis ataupun dipilih satu saja.

III. Mengembangkan dan mengimplementasikan rencana penanggulangan / kelangsungan bisnis yang mencakup :

1. Menetapkan struktur organisasi dan proses untuk proses tanggap darurat / gangguan berikut alokasi personil yang kompeten sebagai penanggung jawab untuk proses :

   a. Mengkonfirmasi tipe dan cakupan dari kondisi darurat / gangguan tersebut;

b. Memutuskan untuk mengaktifkan rencana tanggap darurat;
c. Mengkoordinasikan serta menjalankan rencana tanggap darurat tersebut;
d. Menyediakan sumber daya yang dibutuhkan untuk proses tanggap darurat;
e. Mengkomunikasikan kondisi tersebut kepada para pemangku kepentingan (*stakeholders*).

2. Menetapkan rencana tanggap darurat dan rencana kelangsungan bisnis yang mencakup:
   a. Penentuan personil yang terlibat beserta tugas dan tanggung jawab serta jalur komunikasi antar personil, beserta personil alternatifnya;
   b. Otoritas yang dimiliki oleh personil dalam ruang lingkup rencana tersebut;
   c. Kondisi dan metode untuk pemberlakuan rencana tersebut;
   d. Lokasi pertemuan beserta alternatifnya;
   e. Kondisi dan metode untuk menghubungi stakeholder perusahaan beserta informasi kontak;
   f. Aktifitas yang harus dilakukan pada kondisi darurat dengan titik berat pada proses pengelolaan dampak dari kondisi darurat yang mencakup:
      1) Keselamatan manusia;
      2) Aktifitas strategis dan operasional untuk menanggulangi kondisi darurat;
      3) Mencegah kerugian atau kehilangan aktifitas kritikal tambahan.
      4) Memungkinkan pemulihan dan melanjutkan proses / aktifitas bisnis kritikal.
   g. Informasi yang perlu dicatat terkait dengan gangguan beserta keputusan dan tindakan yang diambil;
   h. Sumber daya yang perlu disediakan untuk proses pemulihan dan kelanjutan proses bisnis kritikal;
   i. Proses-proses bisnis kritikal yang perlu dipulihkan beserta jangka waktu dan tingkat pemulihan. Hal ini perlu disesuaikan dengan skala prioritas yang telah disusun dalam proses analisa dampak bisnis.

IV. Proses Pengujian, pemeliharaan dan peninjauan rencana penanggulangan / kelangsungan bisnis. Proses ini bertujuan untuk memverifikasi kesesuaian dan efektifitas dari proses BCM yang mencakup juga rencana tanggap darurat dan kelangsungan bisnis yang telah ditetapkan. Proses ini juga dilakukan untuk memberikan keyakinan bahwa proses / aktifitas kritikal perusahaan dapat dipulihkan sesuai dengan prasyarat yang telah ditetapkan. Proses ini mencakup :

1. Pengujian rencana penanggulangan / kelangsungan bisnis, yang mencakup aktifitas berikut:
   a. Penyusunan rencana pengujian untuk rencana penanggulangan / kelangsungan bisnis yang mencakup:
      1) Jadwal;
      2) Pihak yang terlibat;

3) Skenario pengujian;
4) Aspek yang diukur dalam proses pengujian beserta metrik pengukuran yang digunakan;
5) Laporan tertulis sebagai hasil pengujian rencana penanggulangan / kelangsungan bisnis.

b. Pelaksanaan pengujian rencana penanggulangan / kelangsungan bisnis. Pengujian rencana ini bertujuan untuk:
1) Menguji dan melatih persiapan pelaksanaan rencana penanggulangan / kelangsungan bisnis;
2) Membandingkan rencana penanggulangan / kelangsungan bisnis dengan pelaksanaannya.

2. Pemeliharaan dan peninjauan rencana penanggulangan / kelangsungan bisnis. Proses ini bertujuan ini untuk :
a. Memastikan kesesuaian, kecukupan dan efektifitas dari rencana penanggulangan / kelangsungan bisnis yang telah disusun;
b. Mengidentifikasi peningkatan dan perubahan dalam rencana penanggulangan / kelangsungan bisnis.

V. Proses pengujian, pemeliharaan, dan peninjauan ini perlu dilakukan minimal 1 kali dalam 1 tahun atau apabila terdapat perubahan besar dalam proses manajemen kelangsungan bisnis dan perusahaan;

VI. Dokumentasi proses pengujian, pemeliharaan dan peninjauan harus dibuat dan dipelihara;

VII. Proses pengujian dilakukan dengan memperhatikan kritikalitas dari proses yang rencana penanggulangan / kelangsungan bisnis akan diuji;

VIII. Proses pengujian dapat mencakup namun tidak terbatas pada proses:
1. *Walktrough*, dimana pengujian dilakukan dengan cara mendiskusikan rencana penanggulangan / kelangsungan bisnis yang telah disusun untuk memastikan bahwa rencana tersebut masih relevan dan dapat digunakan;
2. Simulasi, dimana pengujian dilakukan melalui proses diskusi bersama untuk melihat pemahaman pihak pelaksana rencana penanggulangan / kelangsungan bisnis dengan cara melihat tanggapan pihak pelaksana terhadap skenario pengujian;
3. *Partial test*, dimana pengujian dilakukan terhadap salah satu / sebagian komponen dari rencana penanggulangan / kelangsungan bisnis;
4. *Full test*, dimana pengujian dilakukan terhadap seluruh komponen dari rencana penanggulangan / kelangsungan bisnis.

IX. Format Dokumen Rencana Keberlangsungan Bisnis

1. Tujuan dan Sasaran

Rencana pemulihan dan keberlangsungan bisnis disusun sebagai acuan utama bagi aktivitas yang dilakukan oleh OPD ... setelah terjadinya kondisi darurat / bencana untuk meminimalkan kerusakan dan kerugian bisnis.

2. Ruang Lingkup

Ruang lingkup dari Rencana Pemulihan dan Keberlangsungan Bisnis adalah proses bisnis pengelolaan layanan ... di OPD ....

3. Analisis Dampak Bisnis (Business Impact Analysis)

3.1. Identifikasi Proses Bisnis

No	Proses Bisnis	Deskripsi
1	Sistem Pengelolaan LPSE	Memastikan penyediaan sistem pengadaan barang dan jasa Pemda DIY

3.2. Analisis Dampak Bencana

No	Proses Bisnis	Dampak Finansial	Dampak Operasional
1	Sistem Pengelolaan LPSE	Pengadaan barang dan jasa tertunda, mengganggu penyerapan anggaran	Kegagalan sistem TI yang mendukung operasional LPSE

3.3. Identifikasi "*Maximum Tolerable Of Downtime*"

No	Proses Bisnis	MTD
1	Sistem Pengelolaan LPSE	48 Jam

3.4. Identifikasi Infrastruktur Pendukung dan Penentuan " *Recovery Time Objective*" dan *"Recovery Point Objective" (RPO)*

No	Proses Bisnis	Perangkat Pendukung	RTO	RPO	Sumber daya lain yang dibutuhkan untuk pemulihan
1	Sistem Pengelolaan LPSE	Perangkat Kerja	24 Jam	24 jam	Internal Network, PC / Notebook
		Ruang Kerja	24 Jam	24 jam	Listrik, server, aplikasi, jaringan

4. Risk Assessment dan Pemilihan Strategi Kelangsungan Bisnis

Daftar Risiko

Nomor Dokumen	:	Tanggal Efektif	
Versi	:	Halaman	

No	Proses Bisnis	Identifikasi Risiko			Analisa Risiko			Evaluasi Risiko	Pemilihan Strategi Kelangsungan Bisnis	Kebutuhan Sumber Daya Pemulihan (Dokumen, Teknologi, Penunjang, Finansial)	PIC	Target Waktu	Progress
		Ancaman	Kerawanan	Dampak	Nilai Impact	Nilai Likelihood	Nilai Risiko						
1	LPSE	Kebakaran	Komputer rusak	Data Hilang	4	1	4	Sedang	Relokasi Layanan	Komputer, Ruang Layanan,	Mr X		

Dibuat Oleh

(.....)

Disetujui Oleh;

(.....)

5. Koordinator Pemulihan

Fungsi	Nama	Telepon (HP)
Ketua Pemulihan	**Kepala Dinas Kominfo**	**081xxx**
Koordinator Pemulihan Fasilitas	**Kepala Bidang Manajemen Informatika**	**081xxx**
Koordinator Sistem Keamanan	**Kepala Seksi Aplikasi dan Keamanan Informasi**	**085xxx**
Koordinator Fungsi Manajemen IT	**Kepala Seksi Pengembangan *E-Goverment***	**081xxx**

6. Rencana Pemulihan Bisnis

6.1. Skenario Bencana

6.1.1. Kebakaran di Area Fasilitas Data Center (SK-1)

No	Aktivitas	Kegiatan Sebelumnya	PIC	Keterangan
SK1-1	Segera memberitahukan bagian Keamanan Gedung terkait kebakaran di area fasilitas data center		Personil yang melihat api pertama kali;	
SK1-2	• Tim penanggulangan kebakaran akan melakukan pemeriksaan terhadap area dimana alarm kebakaran telah aktif. • Jika api masih dalam tahap awal, cobalah memadamkan api tanpa membahayakan diri dengan alat pemadam api yang tersedia	SK1-1	Tim Penanggulangan Kebakaran: - Keamanan Gedung - PIC Perawatan Data Center (Pihak Ketiga)	
SK1-3	Evakuasi personil menuju titik kumpul yang telah ditentukan	SK1-1		
SK1-4	Melacak keberadaan dan kondisi personil dengan menggunakan mekanisme grup Whatsapp Bidang MI dan LPSE	SK1-3		
SK1-5	Melaporkan kebakaran kepada dinas pemadam kebakaran apabila kebakaran tidak dapat ditangani oleh tim penanggulangan kebakaran	SK1-3	Tim Penanggulangan Kebakaran: - Keamanan Gedung - PIC Perawatan Data Center (Pihak Ketiga)	Untuk Nomor telepon Dinas pemadam kebakaran : 0274-587101
SK1-6	Menghubungi Kepala Dinas mengenai insiden yang terjadi	SK1-3	Kabid Manajemen Informatika	
SK1-7	Melaporkan terjadinya kebakaran kepada instansi terkait yang menempatkan perangkat di area fasilitas data center	SK1-5	Admin Data Center	

No	Aktivitas	Kegiatan Sebelumnya	PIC	Keterangan
SK1-8	Memastikan bahwa kebakaran telah sepenuhnya dipadamkan dan lokasi terjadinya kebakaran telah aman untuk diperiksa.	SK1-5	Kabid Manajemen Informatika	Keputusan diberikan oleh dinas pemadam kebakaran
SK1-9	Memeriksa kerusakan pada gedung dan perangkat	SK1-7	Kabid Manajemen Informatika	
SK1-10	Mempersiapkan jalur yang tidak terpengaruh oleh kebakaran untuk pengoperasian fasilitas data center.	SK1-8	Admin Data Center	
SK1-11	Memeriksa kondisi fasilitas data center	SK1-9	Admin Data Center	
SK1-12	Memberi laporan kepada KaBid Mi dan rekomendasi langkah pemulihan yang bisa dilakukan	SK1-11	Admin	
SK1-13	Menyatakan kondisi darurat dan memerintahkan aktivasi BCP	SK1-12	Kabid MI	
SK1-14	Mobilisasi personil menuju DRC untuk mempersiapkan pemulihan layanan Bidang MI	SK1-13	Semua personil	
SK1-15	Mengkoordinasikan penyediaan perangkat kerja	SK1-13	Sekretariat Diskominfo DIY	
SK1-16	Instalasi perangkat lunak	SK1-15	Personil MI	
SK1-17	Melakukan restore sistem dan data di DRC	SK1-13	Admin Data Center	
SK1-18	Pengalihan jaringan ke DRC	SK1-13	Admin Jaringan	
SK1-19	Melakukan pengujian pada fasilitas data center yang telah diperbaiki	SK1-17 & SK1-18	Admin Data Center	
SK1-20	Pengujian kesiapan penyelenggaraan layanan Bidang MI dan LPSE	SK1-19	Personil MI dan LPSE	
SK1-21	Menyatakan dilaksanakannya layanan Bidang MI dan LPSE dalam kondisi darurat	SK1-20	Kepala Bidang MI	
SK1-22	Menkomunikasikan terjadinya gangguan dan lokasi pengganti Bidang MI dan LPSE kepada pengguna	SK1-21	Kepala Dinas	

6.1.2. Kebakaran di Ruang Kerja (SK-2)

No	Aktivitas	Kegiatan Sebelumnya	PIC	Keterangan

6.1.3. Listrik Padam di Data Center

No	Aktivitas	Kegiatan Sebelumnya	PIC	Keterangan

7. Checklist Pengujian Pemulihan Bisnis

7.1. Skenario Bencana

7.1.1. Kebakaran di Area Fasilitas Data Center (SK-1)

No	Aktivitas	Kegiatan Sebelumnya	PIC	Estimasi Durasi	Aktual Durasi	Keterangan
SK1-1	Segera memberitahukan bagian Keamanan Gedung terkait kebakaran di area fasilitas data center		Personil yang melihat api pertama kali;	**5 Menit**		
SK1-2	• Tim penanggulangan kebakaran akan melakukan pemeriksaan terhadap area dimana dimana alarm kebakaran telah aktif. • Jika api masih dalam tahap awal, cobalah memadamkan api tanpa membahayakan diri dengan alat pemadam api yang tersedia	SK1-1	Tim Penanggulangan Kebakaran: - Keamanan Gedung - PIC Perawatan Data Center (Pihak Ketiga)	**15 Menit**		
SK1-3	Evakuasi personil menuju titik kumpul yang telah ditentukan	SK1-1	Seluruh Personil	**10 Menit**		
SK1-4	Melacak keberadaan dan kondisi personil dengan menggunakan mekanisme grup Whatsapp Bidang MI dan LPSE	SK1-3	Kepala Seksi	**10 Menit**		

No	Aktivitas	Kegiatan Sebelumnya	PIC	Estimasi Durasi	Aktual Durasi	Keterangan
SK1-5	Melaporkan kebakaran kepada dinas pemadam kebakaran apabila kebakaran tidak dapat ditangani oleh tim penanggulangan kebakaran	SK1-3	Tim Penanggulangan Kebakaran: - Keamanan Gedung - PIC Perawatan Data Center (Pihak Ketiga)	**5 Menit**		Untuk Nomor telepon Dinas pemadam kebakaran : 0274-587101
SK1-6	Menghubungi Kepala Dinas mengenai insiden yang terjadi	SK1-3	Kabid Manajemen Informatika	**5 Menit**		
SK1-7	Melaporkan terjadinya kebakaran kepada instansi terkait yang menempatkan perangkat di area fasilitas data center	SK1-5	Admin Data Center	**1 x 24 Jam**		
SK1-8	Memastikan bahwa kebakaran telah sepenuhnya dipadamkan dan lokasi terjadinya kebakaran telah aman untuk diperiksa.	SK1-5	Kabid Manajemen Informatika	**15 Menit**		Keputusan diberikan oleh dinas pemadam kebakaran
SK1-9	Memeriksa kerusakan pada gedung dan perangkat	SK1-7	Kabid Manajemen Informatika	**15 Menit**		
SK1-10	Mempersiapkan jalur yang tidak terpengaruh oleh kebakaran untuk pengoperasian fasilitas data center.	SK1-8	Admin Data Center	**30 Menit**		
SK1-11	Memeriksa kondisi fasilitas data center	SK1-9	Admin Data Center	**15 Menit**		
SK1-12	Memberi laporan kepada KaBid Mi dan rekomendasi langkah pemulihan yang bisa dilakukan	SK1-6	Admin Data Center	**1 Jam**		
SK1-13	Menyatakan kondisi darurat dan memerintahkan aktivasi BCP	SK1-12	Kepala Bidang MI	**1 Jam**		
SK1-14	Mobilisasi personil menuju DRC untuk mempersiapkan pemulihan layanan Bidang MI	SK1-13	Semua personil	**1 jam**		
SK1-15	Mengkoordinasikan penyediaan perangkat kerja	SK1-13	Sekretariat Diskominfo DIY	**3 Jam**		
SK1-16	Instalasi perangkat lunak	SK1-15	Personil MI	**1 Jam**		

No	Aktivitas	Kegiatan Sebelumnya	PIC	Estimasi Durasi	Aktual Durasi	Keterangan
SK1-17	Melakukan restore sistem dan data di DRC	SK1-13	Admin Data Center	**2 Jam**		
SK1-18	Pengalihan jaringan ke DRC	SK1-13	Admin Jaringan	**1 Jam**		
SK1-19	Melakukan pengujian pada fasilitas data center yang telah diperbaiki	SK1-17 & SK1-18	Admin Data Center	**10 Menit**		
SK1-20	Pengujian kesiapan penyelenggaraan layanan Bidang MI dan LPSE	SK1-19	Personil MI dan LPSE	**10 Menit**		
SK1-21	Menyatakan dilaksanakannya layanan Bidang MI dan LPSE dalam kondisi darurat	SK1-20	Kepala Bidang MI	**5 Menit**		
SK1-22	Menkomunikasikan terjadinya gangguan dan lokasi pengganti Bidang MI dan LPSE kepada pengguna	SK1-21	Kepala Dinas	**1 Jam**		

7.1.2. Kebakaran di Ruang Kerja (SK-2)

No	Aktivitas	Kegiatan Sebelumnya	PIC	Estimasi Durasi	Aktual Durasi	Keterangan

7.1.3. Listrik Padam di Data Center

No	Aktivitas	Kegiatan Sebelumnya	PIC	Estimasi Durasi	Aktual Durasi	Keterangan

E KEPATUHAN DAN PENILAIAN INTERNAL

I. Pelaksanaan

1. Seluruh peraturan hukum, regulasi dan kontraktual yang terkait dengan tata kelola TIK dan berlaku bagi organisasi harus diidentifikasikan, didokumentasikan dan dipelihara;
2. Metode, kontrol dan alokasi tanggung jawab yang dimiliki organisasi untuk memenuhi peraturan tersebut harus diidentifikasi, didokumentasikan dan dipelihara;
3. Peninjauan secara berkala harus dilakukan untuk mengidentifikasi:
   a. Peraturan baru;
   b. Perubahan terhadap peraturan yang sudah ada;
   c. Perubahan terhadap metode, kontrol, serta alokasi tanggung jawab yang dimiliki organisasi untuk memenuhi peraturan tersebut.
4. Aktivitas monitoring berkala harus dilakukan untuk memantau kepatuhan organisasi terhadap peraturan tata kelola TIK.
5. OPD menentukan periode pelaksanaan pengelolaan kepatuhan dan penilaian internal.

II. Pengelolaan Kepatuhan

1. Tingkat Kepatuhan

Dalam menentukan tingkat kepatuhan terhadap peraturan, perlu adanya matriks untuk selanjutnya dijadikan penentu tindak lanjut kepatuhan. Contoh matriks tingkat kepatuhan adalah sebagai berikut :

Tingkat Kepatuhan	Operasional
0	Tidak terlaksana
1	Dalam perencanaan
2	Diterapkan sebagian
3	Diterapkan menyeluruh

2. Format Identifikasi Pemenuhan Kepatuhan

IDENTIFIKASI DAN EVALUASI **PEMENUHAN KEPATUHAN TERHADAP PERATURAN**						Nomor		
						Tanggal		
						Halaman		
No	PERATURAN	BAB	PASAL	URAIAN	TINGKAT KEPATUHAN	KET	TINDAKLANJUT	PIC
1	UU No. 11 Tahun2008 tentang Informasi dan Transaksi Elektronik	I	1	Tanda Tangan Elektronik adalah tandatangan yang terdiri atas Informasi Elektronik yang dilekatkan, terasosiasi atau terkait dengan Informasi Elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi.	3	Sudah dilaksanakan sesuai dengan aturan yang berlaku	dilaksanakan secara kontinyu	Verifikator
				(1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun. (2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apapun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik		Sudah dilaksanakan sesuai dengan aturan yang berlaku	dilaksanakan secara kontinyu	Admin System
2	Perpres 54 Tahun 2010 tentang Pengadaan Barang/Jasa Pemerintah	XIII	112	K/L/D/I wajib menayangkan rencana Pengadaan dan pengumuman Pengadaan di website K/L/D/I …….	3	…….	…….	…….
3								

III. Penilaian Internal

1. Tahapan penilaian internal

a. Pembuatan daftar periksa umum yang berisi poin-poin yang masuk dalam penilaian
b. Menyusun jadwal penilaian
c. Melakukan konfirmasi jadwal dengan pihak yang terkait dengan penilaian
d. Penyiapan dokumen untuk pencatatan penilaian
e. Melakukan penilaian
f. Mengumpulkan data dukung penentu penilaian
g. Melaporkan hasil penilaian kepada atasan

2. Matriks penilaian

Dalam menentukan status implementasi tata kelola TIK, perlu adanya matriks untuk dijadikan penentu nilai. Contoh matriks penilaian adalah sebagai berikut :

Nilai	Status
0	Tidak terlaksana
1	Dalam perencanaan
2	Diterapkan sebagian
3	Diterapkan menyeluruh

3. Format penilaian

	Kop instansi	

PENILAIAN INTERNAL TATA KELOLA TIK

Nomor :

Penilai Internal :

Pelaksanaan Investasi TIK

No.	Penerapan	Status	Nilai	Data dukung
1	Apakah investasi TIK yang dijalankan sudah mendapat rekomendasi dari Diskominfo DIY?	Diterapkan Menyeluruh	3	Surat Persetujuan Rekomendasi Nomor …../…

Pelaksanaan Pengelolaan Aset TIK

No.	Penerapan	Status	Nilai	Data dukung
1	Apakah sudah memiliki matriks kompetensi SDM?	Diterapkan Sebagian	2	Form matrik Kompetensi SDM hanya berisi ……
2	Apakah sudah memiliki daftar data dan informasi?	…….	…..	……

Pelaksanaan Pengelolaan ……..

No.	Penerapan	Status	Nilai	Data dukung

F. LAMPIRAN MEKANISME PEMANTAUAN DAN EVALUASI PENGELOLAAN TIK

1. Pemantauan dan Evaluasi Pengelolaan TIK dilaksanakan melalui audit.
2. Pelaksanaan audit dilakukan oleh auditor yang memiliki kompetensi yang memadai serta memiliki objektifitas dan imparsialitas terhadap proses audit
3. Tahapan audit tata kelola TIK:
    a. Auditor menyiapkan daftar periksa
    b. Auditor menyusun jadwal audit
    c. Auditor melakukan konfirmasi jadwal dengan OPD terkait sebelum proses audit dilaksanakan
    d. Auditor melakukan persiapan audit
    e. Auditor mencatat dan merekapitulasi temuan audit
    f. Auditor melaporkan dan mengkomunikasikan hasil audit
    g. OPD menetapkan koreksi dan tindak lanjut temuan audit
    h. Auditor melakukan verifikasi untuk menentukan tindakan korektif telah diimplementasikan dengan baik
    i. Auditor melaporkan penutupan/penyelesaian temuan audit kepada Kepala Dinas
4. Temuan audit diklasifikasikan berdasarkan kritikalitas dan cakupan dari temuan tersebut menjadi:
    a. Major, dalam hal pengelolaan TIK tidak berjalannya sama sekali sebuah proses tata kelola TIK atau apabila sebuah temuan dapat menyebabkan dampak buruk terhadap proses atau sistem kritikal OPD;
    b. Minor, ketidaksesuaian ini mengindikasikan sebuah kealpaan / problem kecil yang tidak mengindikasikan bahwa sebuah proses tata kelola TIK tidak berjalan sama sekali; atau apabila sebuah temuan tidak akan menyebabkan dampak buruk terhadap proses atau sistem kritikal OPD;
    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 tersebut.
5. Dalam hal hasil audit major dapat ditindaklanjuti dengan Perubahan Renstra TIK.
6. Dalam hal hasil audit minor atau peluang untuk perbaikan perlu dilakukan rencana tindak lanjut dalam jangka waktu yang telah disepakati.
7. Sebuah laporan formal hasil audit harus disiapkan oleh Auditor setelah setiap proses audit;

1. Formulir Jadwal Audit OPD

	Kop Diskominfo	

Jadwal Audit Dinas A
Nomor :

Instansi :

Tanggal	Waktu	Auditor	Proses	Dasar Aturan
19 Jan 2019	09:00	NE	Opening Meeting	
	09:30		**Perencanaan TIK**	Bab II Pasal …. Pergub Tata Kelola TIK

2. Formulir Rencana Tindak Lanjut Hasil Temuan

	Kop Diskominfo	

Rencana Tindak Lanjut Ketidaksesuaian

No:	8633726				**OPD:**	Dinas A
Diisi oleh Auditor			**Diisi oleh OPD**			
No	**Tanggal**	**Deskripsi Ketidaksesuaian**	**Koreksi**	**Analisa Sumber Permasalahan**	**Rencana Tindak Lanjut**	
					Rencana perbaikan	**Penanggungjawab**	**Tanggal Target Penyelesaian**
1	25/11/2017	**Area: Bab …. Pasal ….. Ayat ……** OPD tidak mengajukan permohonan rekomendasi pelaksanaan investasi TIK (major)	Merubah proses kerja	Belum mempelajari Pergub Tata Kelola TIK secara menyeluruh	Melakukan review prosedur dan proses kerja, membuat permohonan rekomendasi	Pak A	16 Dec 2017

GUBERNUR
DAERAH ISTIMEWA YOGYAKARTA,
ttd.
HAMENGKU BUWONO X

Salinan Sesuai Dengan Aslinya
KEPALA BIRO HUKUM,
ttd.
DEWO ISNU BROTO I.S.
NIP. 19640714 199102 1 001