KEMENTERIAN KOORDINATOR
BIDANG PEREKONOMIAN
REPUBLIK INDONESIA

Kebijakan Internal Sistem Pemerintahan Berbasis Elektronik

KEMENTERIAN KOORDINATOR BIDANG PEREKONOMIAN
REPUBLIK INDONESIA

KATA PENGANTAR

Dengan mengucapkan puji syukur ke hadirat Allah Yang Maha Esa, berkat rahmat dan karunia-Nya penyusunan Kebijakan Internal Sistem Pemerintahan Berbasis Elektronik Kementerian Koordinator Bidang Perekonomian dapat diselesaikan.

Kebijakan Intrernal Sistem Pemerintahan Berbasis Elektronik bagian tak terpisahkan dari Rencana Induk Teknologi Informasi dan Komunikasi (RITIK) Kementerian Koordinator Bidang Perekonomian yang merupakan arah kebijakan dan strategi yang dapat menjadi pedoman umum dalam rangka merencanakan, implementasi, pemantauan, evaluasi dan pengawasan terkait dengan pengembangan Teknologi Informasi dan Komunikasi (TIK) sehingga lebih sistematis, terarah, dan berkesinambungan.

Kebijakan internal SPBE disusun dalam rangka mengatur pelaksanaan Sistem Pemerintahan Berbasis Elektronik (SPBE) untuk mendukung tugas dan fungsi Kementerian Koordinator Bidang Perekonomian lebih efektif dan efisien sehingga menghasilkan birokrasi yang berkinerja tinggi dengan karakteristik integratif, dinamis, transparan, inovatif, dan akuntabel.

Selanjutnya kami mengucapkan terima kasih kepada semua pihak baik dari lingkungan Kementerian Koordinator Bidang Perekonomian maupun unit kerja lain yang terlibat dan memberi masukan dalam penyusunan Kebijakan Internal ini. Masukan dan saran sangat diharapkan untuk penyempurnaan sesuai dengan perubahan teknologi yang berkembang sangat dinamis.

Jakarta, Maret 2021

Kepala Biro Perencanaan
Kementerian Koordinator Bidang Perekonomian

Andie Megantara

DAFTAR ISI

PENDAHULUAN

Peraturan Presiden Republik Indonesia Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik, yang selanjutnya disingkat SPBE, di Instansi Pusat dan Pemerintah Daerah ditujukan untuk mewujudkan proses kerja yang efisien, efektif, transparan, dan akuntabel sehingga dapat menghasilkan birokrasi yang berkinerja tinggi dengan karakteristik integratif, dinamis, transparan, dan inovatif. Agar pelaksanaan SPBE dapat berjalan untuk mencapai tujuannya, maka perlu dilakukan evaluasi secara berkala untuk mengetahui sejauh mana kemajuan dari pelaksanaan SPBE di setiap Instansi Pusat dan Pemerintah Daerah.

Evaluasi SPBE merupakan proses penilaian terhadap pelaksanaan SPBE di Instansi Pusat dan Pemerintah Daerah untuk menghasilkan suatu nilai Indeks SPBE yang menggambarkan tingkat kematangan (*maturity level*) dari pelaksanaan SPBE di Instansi Pusat dan Pemerintah Daerah.

Kementerian Koordinator Bidang Perekonomian merupakan Lembaga Pemerintahan Kementerian Koordinator yang mempunyai tugas menyelenggarakan koordinasi, sinkronisasi, dan pengendalian urusan Kementerian dalam penyelenggaraan pemerintahan di bidang perekonomian. Untuk peningkatan pelaksanaan dan penerapan SPBE, Kementerian Koordinator Bidang Perekonomian menyusun kebijakan internal layanan SPBE. Penyusunan kebijakan ini dilakukan untuk menghasilkan kebijakan tata kelola dan kebijakan layanan SPBE yang terdapat pada domain kebijakan SPBE, yang digunakan sebagai pedoman untuk meningkatan efisiensi dan efektivitas kerja sehingga menghasilkan birokrasi yang berkinerja tinggi dengan karakteristik integratif, dinamis, transparan dan inovatif.

1. KEBIJAKAN INTERNAL STANDAR PENGGUNAAN SURAT ELEKTRONIK

1.1 Tujuan

Kebijakan dan standar ini bertujuan untuk mengatur penggunaan Surat Elektronik dengan menggunakan fasilitas Teknologi Informasi dan Komunikasi (TIK) di Kementerian.

1.2 Ruang Lingkup

Ruang lingkup kebijakan dan standar ini berlaku untuk semua Pengguna Surat Elektronik untuk mengakses Sistem TIK di seluruh Unit Organisasi dan Unit Kerja Kementerian.

1.3 Kebijakan

1. Pimpinan Unit Penyelenggara SPBE Kementerian bertanggung jawab dalam menerapkan kebijakan dan standar penggunaan Surat Elektronik yang diatur dalam Peraturan Menteri Koordinator Bidang Perekonomian ini di lingkungan Kementerian.
2. Unit Penyelenggara SPBE Kementerian bertanggung jawab dalam menerapkan kebijakan dan standar penggunaan Surat Elektronik yang diatur dalam Peraturan Menteri Koordinator Bidang Perekonomian di lingkungan Kementerian.
3. Pengguna bertanggung jawab terhadap penggunaan Surat Elektronik dan wajib mematuhi standar penggunaan Surat Elektronik yang diatur dalam Peraturan Menteri Koordinator Bidang Perekonomian ini.
4. Unit Penyelenggara SPBE Kementerian yang memiliki sistem nama domain masing-masing mengatur hak penggunaan Surat Elektronik, melakukan pengamanan, menjaga integritas, dan ketersediaan fasilitas Surat Elektronik dengan mengacu pada Kebijakan dan Standar Penggunaan Surat Elektronik di Kementerian.
5. Unit Penyelenggara SPBE Kementerian mengatur kapasitas mailbox, jumlah pengiriman atau penerimaan, dan besaran dokumen yang disertakan.
6. Unit Penyelenggara SPBE Kementerian menambahkan pernyataan disclaimer pada setiap Surat Elektronik untuk mencegah tuntutan hukum atas penggunaan Surat Elektronik.
7. Auditor berhak melakukan audit dalam rangka memperoleh bukti pelanggaran hukum pada setiap pesan yang dikirim, diterima, maupun yang disimpan pada sistem Surat Elektronik.

1.4 Standar

1. Tanggung Jawab Pengguna:
   a. Menggunakan fasilitas Surat Elektronik hanya untuk kepentingan kedinasan sesuai dengan tugas, fungsi, dan wewenang;
   b. Menggunakan fasilitas Surat Elektronik sesuai norma hukum dan etika yang berlaku;
   c. Menggunakan fasilitas Surat Elektronik secara bijak dan hemat sesuai tugas dan fungsinya; dan
   d. Memastikan identitas individu dan organisasi penerima informasi melalui konfirmasi sebelum mengirimkan informasi kedinasan.
2. Larangan Pengguna:
   a. Mengirim dan/atau mempublikasikan Surat Elektronik yang berisikan ancaman, penghinaan atau pencemaran nama baik orang lain atau digunakan untuk mengemukakan pandangan dan pendapat pribadi (positif maupun negatif) terhadap sesama pegawai, pimpinan, mitra, dan pihak lainnya yang terkait dengan Kementerian;
   b. Menggunakan fasilitas Surat Elektronik untuk menyebarkan surat berantai atau untuk mengirimkan Surat Elektronik atas nama orang lain;
   c. Mendaftarkan alamat Surat Elektronik kedinasan ke suatu milis di luar kedinasan sesuai dengan ketentuan pembatasan oleh Unit Penyelenggara SPBE Kementerian;
   d. Melakukan pengiriman kembali secara otomatis Surat Elektronik yang diterimanya melalui alamat Surat Elektronik kedinasan ke alamat-alamat Surat Elektronik di luar kedinasan kecuali jika sesuai dengan tugas, fungsi dan wewenang pengguna; dan
   e. Membuka dokumen yang disertakan dalam Surat Elektronik yang berasal dari pihak yang tidak dikenal ataupun seolah-olah dari mitra namun tidak relevan.
3. Klasifikasi Alamat Surat Elektronik:
   a. Alamat Surat Elektronik Individu;
   b. Alamat Surat Elektronik Khusus; dan
   c. Alamat Surat Elektronik Grup/Kegiatan.

4. Kriteria penamaan alamat Surat Elektronik Individu menggunakan nama Akun Individu.
5. Kriteria penamaan alamat Surat Elektronik Khusus menggunakan nama Akun Khusus.
6. Kriteria penamaan alamat Surat Elektronik Grup/Kegiatan:
   a. Bersifat unik untuk setiap alamat Surat Elektronik;
   b. Terdiri dari minimal 6 (enam) karakter dan maksimal 20 (dua puluh) karakter; dan
   c. Disesuaikan dengan nama kegiatan/peruntukannya.
7. Pengguna dapat mengajukan permintaan alamat Surat Elektronik yang sesuai dengan kriteria penamaan surat elektronik kepada Unit Penyelenggara SPBE Kementerian sesuai dengan prosedur permintaan alamat surat elektronik yang telah ditentukan.

1.5 Sanksi Atas Pelanggaran

Pelanggaran terhadap kebijakan dan standar ini dikenakan:

1. Sanksi Teknis berupa penonaktifan Akun dan Kata Sandi sampai dengan ada permintaan resmi untuk mengaktifkan kembali.
2. Sanksi Administratif berupa penindakan sesuai dengan Peraturan Pemerintah Nomor 30 Tahun 1980 tentang Peraturan Disiplin Pegawai Negeri Sipil.

1.6 Istilah yang Digunakan

1. Akun adalah identifikasi pengguna yang diberikan oleh Unit Penyelenggara SPBE Kementerian, bersifat unik dan digunakan bersamaan dengan Kata Sandi ketika akan memasuki Sistem TIK.
2. Alamat Surat Elektronik adalah alamat yang digunakan sebagai tujuan pengiriman surat dalam proses korespondensi dalam sistem surat elektronik.
3. Alamat Surat Elektronik Grup/Kegiatan adalah alamat yang mendistribusikan Surat Elektronik kepada para anggota yang terdaftar.
4. Alamat Surat Elektronik Individu adalah alamat yang digunakan oleh Akun Individu dalam proses korespondensi.

5. Alamat Surat Elektronik Khusus adalah alamat yang digunakan oleh Akun Khusus dalam proses korespondensi.
6. Disclaimer adalah suatu pernyataan yang menerangkan bahwa Kementerian menolak keberadaan, keterlibatan, atau pertanggungjawaban hukum sesuatu hal yang mungkin timbul atas isi dan/atau lampiran suatu Surat Elektronik.
7. Mailbox adalah media penyimpanan Surat Elektronik pada server surat elektronik.
8. Pengguna adalah Pegawai Kementerian dan atau Pihak Ketiga serta tidak terbatas pada Penyelenggara SPBE Kementerian dan Kelompok Kerja yang diberikan hak mengakses Sistem TIK di lingkungan Kementerian.
9. Surat Elektronik (e-mail) adalah metode untuk bertukar pesan secara digital baik dalam jaringan internal maupun melalui jalur internet.
10. Sistem nama domain adalah sistem hirarki penamaan untuk komputer, atau sumber daya yang berpartisipasi pada sistem TIK.
11. Sistem TIK adalah sistem operasi, sistem surat elektronik, sistem aplikasi, sistem basis data, sistem jaringan intranet/internet, dan sebagainya.

2. KEBIJAKAN INTERNAL NAMA DOMAIN DAN SUBDOMAIN

2.1. Tujuan

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

2.2. Ruang Lingkup

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

Setiap pengajuan nama subdomain harus disampaikan kepada Unit Penyelenggara SPBE Kementerian disertai dengan data penanggung jawab portal *web* (*website*), aplikasi berbasis *web* serta pemilik kegiatan.

2.3. Kebijakan

1. Setiap Pimpinan Unit Organisasi bertanggung jawab dalam memantau dan mengawasi penggunaan subdomain di lingkungan Unit Organisasi masing-masing.
2. Setiap Pimpinan Unit Organisasi bertanggung jawab dan mengetahui terhadap penambahan dan perubahan nama subdomain di lingkungan Unit Organisasi masing-masing, dalam hal ini meliputi penambahan, perubahan, dan penghapusan subdomain.
3. Domain dan subdomain yang sudah dibuat menjadi milik Kementerian dan tidak boleh digunakan di luar Kementerian tanpa izin dari pejabat yang berwenang.

2.4. Sistem Penamaan Domain (*Domain Name Server* [DNS])

1. Pengertian DNS
   a. 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*).
   b. DNS merupakan sebuah aplikasi *service* yang bisa digunakan di internet seperti peramban (*web browser*) atau surat elektronik yang menerjemahkan sebuah nama domain ke alamat IP (*IP address*).
   Contoh: yahoo.com → 68.142.197.64
2. Struktur DNS
   DNS merupakan sebuah hirarki pengelompokan domain berdasarkan nama yang terbagi menjadi beberapa bagian, yakni:
   a. Domain Tingkat Pertama (*Root Domain*)
      1) Domain Level Global (*Generic/Global Top Level Domain* (TLD))
      Contoh:.com,.net,.org,.ac,.web,.go
      2) Domain Level Negara (*Country Code Top Level Domain* (ccTLD))
      Contoh:.sg,.au,.id
   b. Domain Tingkat Kedua (*Second Level Domain*)
   Contoh: ekon.go.id

c. Domain Tingkat Ketiga (*Third Level Domain* (*subdomain*))
Contoh: simpeg.ekon.go.id, naskah.ekon.go.id

2.5. Pengelolaan Penamaan Domain

1. Pengelolaan Penamaan Domain meliputi:
   a) Pendaftaran,
   b) Penggunaan,
   c) Penonaktifan,
   d) Perpanjangan,
   e) Penunjukan pejabat,
   f) Perubahan nama domain,
   g) Server nama domain.
2. Nama domain yang dimaksud di atas dibiayai oleh Anggaran Kementerian.
3. Seluruh situs web (*website*) Unit Organisasi dan Unit Kerja serta aplikasi berbasis web pada Kementerian harus menjadi subdomain dari nama domain Kementerian.

2.6. Subdomain di Kementerian

1. Yang berhak mendapatkan nama subdomain:
   a. Unit Organisasi dan Unit Kerja di Kementerian.
   b. Pelayanan publik di Kementerian.
   c. Kegiatan Kementerian.
   d. Aplikasi berbasis web.
2. Permohonan mendapatkan nama subdomain.
   Mengajukan permohonan melalui Unit Penyelenggara SPBE Kementerian dengan mencantumkan dan melampirkan:
   a. Surat permohonan nama subdomain layanan publik/domain khusus.
   b. Peraturan perundang-undangan yang menjadi dasar penyelenggaraan pelayanan publik/penyelenggaraan kegiatan Kementerian.
   c. Penunjukan pejabat nama subdomain.
      1) Surat penunjukan pejabat nama subdomain.
      2) Kartu PNS atau kartu identitas pegawai tetap.
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 Kementerian, dan aplikasi berbasis web.

4. Penataan subdomain untuk kegiatan Kementerian:
   a. Kegiatan Skala Nasional/Internasional: *kegiatan.ekon.go.id*
   b. Kegiatan Internal Kementerian Tingkat Unit Organisasi: *eselonI.ekon.go.id/kegiatan*
   c. Kegiatan Internal Kementerian Tingkat Unit Kerja: *eselonI.ekon.go.id/eselonII/kegiatan*
5. Penataan subdomain untuk aplikasi berbasis web:
   a. Digunakan oleh publik dan lingkungan Kementerian/ aplikasi umum: *aplikasi.ekon.go.id*
   b. Digunakan di lingkungan Unit Organisasi/Unit Kerja/khusus: *aplikasi.eselonI.ekon.go.id*
6. Nama subdomain Unit Organisasi di Kementerian:
   a. Sekretariat : sekretariat.ekon.go.id
   b. Deputi I : deputi1.ekon.go.id
   c. Deputi II : deputi2.ekon.go.id
   d. Deputi III : deputi3.ekon.go.id
   e. Deputi IV : deputi4.ekon.go.id
   f. Deputi V : deputi5.ekon.go.id
   g. Deputi VI : deputi6.ekon.go.id
   h. Deputi VII : deputi7.ekon.go.id
7. Ketentuan lain yang harus diikuti bagi seluruh unit organisasi di Kementerian:
   a. Seluruh basis data (*database*) dan portal web (*website*)/aplikasi berbasis *web* harus disimpan pada *server* yang berada di pusat data (*data center*) Kementerian.
   b. Unit Organisasi wajib melakukan pembinaan dan pengawasan terhadap unit kerja di bawahnya.
   c. Jika terjadi gangguan jaringan komunikasi dan keamanan serta gangguan terkait data dan informasi menjadi tanggung jawab unit organisasi pemilik data dan informasi tersebut dan wajib

menyampaikan kepada Unit Penyelenggara SPBE Kementerian dalam melakukan penanganan gangguan.

3. KEBIJAKAN INTERNAL LAYANAN *HOSTING*

3.1. Dasar Hukum

1. Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik;
2. Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2018 tentang Informasi dan Transaksi Elektronik;
3. Peraturan Presiden Republik Indonesia Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik;
4. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Republik Indonesia Nomor 59 Tahun 2020 tentang Pemantauan dan Evaluasi Sistem Pemerintahan Berbasis Elektronik;
5. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Republik Indonesia Nomor 5 Tahun 2020 tentang Pedoman Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik.
6. Peraturan Menteri Perencanaan Pembangunan Nasional/Kepala Badan Perencanaan Pembangunan Nasional Republik Indonesia Nomor 16 Tahun 2020 tentang Manajemen Data Sistem Pemerintahan Berbasis Elektronik;
7. Peraturan Presiden Nomor 39 Tahun 2019 tentang Satu Data Indonesia (Lembaran Negara Republik Indonesia Tahun 2019 Nomor 112).

3.2. Pendahuluan

Kebijakan internal layanan *hosting* merupakan kebijakan yang dilaksanakan oleh pengelola dan pengguna layanan *hosting* di Kementerian dalam rangka mewujudkan layanan *hosting* dan sistem informasi yang terpadu dan stabil dengan mempertimbangkan aspek keamanan. Kebijakan ini dapat mengalami perubahan apabila dalam pelaksanaannya atau dalam pengembangan sistem terdapat perubahan birokrasi maupun perubahan kebutuhan dan pembaruan sistem dan jaringan.

3.3. Definisi

1. Konten

   Konten adalah isi atau informasi yang ditampilkan pada portal berupa tulisan, gambar, foto, suara, atau video.

2. Pengguna

   Pengguna merupakan pihak yang mendapatkan layanan *hosting*. Pengguna yang diizinkan merupakan pegawai ASN, unit kerja dan kegiatan insidental yang terkait tugas dan fungsi unit kerja di lingkungan Kementerian.

3. Pengelola

   Unit kerja yang bertanggung jawab atas pengelolaan layanan hosting di Kementerian adalah Unit Penyelenggara SPBE di Kementerian.

4. Penanggung Jawab Administratif

   Pejabat yang bertanggung jawab atas layanan hosting di Kementerian adalah pejabat Eselon II atau yang lebih tinggi pada unit kerja atau kegiatan tingkat nasional/internasional dan kegiatan internal terkait.

5. Penanggung Jawab Teknis

   Penanggung jawab teknis yaitu pegawai ASN yang bertanggung jawab secara teknis atas *hosting* yang bersangkutan dan sebagai kontak teknis yang akan dihubungi oleh Pengelola apabila ada pemberitahuan maupun masalah yang berhubungan dengan teknis. Penanggung jawab teknis merupakan orang yang ditunjuk oleh penanggung jawab administratif untuk mengelola dan memelihara layanan *hosting*.

3.4. Ketentuan Umum

1. *Hosting* yang diberikan adalah *hosting* di jaringan publik Kementerian.
2. Aplikasi untuk manajemen *hosting* yang disediakan adalah CPanel Hosting Management dan bisa berubah sewaktu-waktu sesuai kebijakan Pengelola.
3. *Hosting* yang disediakan mendukung penggunaan *web server* Apache dengan bahasa pemrograman PHP dan *database* MySQL. Dukungan ini bisa berubah sewaktu-waktu sesuai kebijakan Pengelola.

4. Permohonan penambahan domain dan subdomain disampaikan melalui Nota Dinas dari Penanggung Jawab Administratif yang disampaikan kepada Pimpinan Unit Penyelenggara SPBE dengan menyertakan nama subdomain, kontak Penanggung Jawab Teknis serta spesifikasi teknis yang diperlukan.
5. Spesifikasi dan kebutuhan penyimpanan yang diperlukan akan dianalisis oleh Pengelola sesuai dengan kebijakan dan kewajaran permohonan.
6. Layanan *hosting* untuk unit kerja di lingkungan Kementerian berlaku permanen sedangkan untuk kegiatan tingkat nasional/internasional dan kegiatan internal berlaku sesuai dengan kesepakatan dan persetujuan Pengelola dengan Penanggung Jawab Administratif.
7. Penamaan dan pengelolaan konten pada domain dan sub domain sepenuhnya menjadi wewenang Penanggung Jawab Administratif.
8. Wewenang Penanggung Jawab Administratif dalam hal operasional layanan *hosting* dapat didelegasikan kepada Penanggung Jawab Teknis.
9. Pengelola tidak bertanggung jawab atas perselisihan internal yang mungkin terjadi atas wewenang pengelolaan *hosting* pada domain dan subdomain yang didelegasikan. Hingga pimpinan organisasi menentukan lain, pengelola menganggap sah, keterangan dari pendaftaran pertama kali.
10. Jika terjadi *dispute* atau perselisihan, maka layanan domain dan sub domain dapat ditangguhkan sesuai kebijakan Pengelola sampai masalah dapat terselesaikan.
11. Pengguna layanan *hosting* mendapatkan dukungan secara teknis dari Pengelola.
12. Pengelola berhak melakukan tindakan yang perlu seperti mencabut, membekukan, dan lain-lain, atas domain yang telah didelegasikan apabila Penanggung Jawab Administratif maupun Jawab Administratif Teknis tidak mematuhi aturan yang telah ditetapkan.
13. Apabila terdapat pergantian Penanggung Jawab Administrastif maupun Penanggung Jawab Teknis pada domain dan sub domain bersangkutan maka serah terima wewenang penanggung jawab dimaksud akan

dimonitor oleh Penanggung Jawab Administrastif sebelumnya dan disampaikan kepada Pengelola.

3.5. Aturan Layanan Hosting

1. Fitur
   a. Layanan *hosting* yang disediakan untuk pengelolaan domain dan sub domain adalah sesuai dengan kebutuhan masing-masing domain dan sub domain dengan memperhatikan aspek efisiensi dan efektivitas penggunaan *resource* pada *server* Kementerian.
   b. Dukungan teknis untuk pengguna dapat diberikan selama jam dan hari kerja melalui *e-mail,* telpon ataupun kunjungan dari pihak pengguna.
2. Penambahan fitur

   Pengguna dapat mengusulkan penambahan fitur kepada Pengelola melalui Nota Dinas yang memuat justifikasi rasional mengenai latar belakang penambahan fitur.
3. Dukungan

   Pengelola memberikan dukungan berupa *monitoring* dan pendampingan teknis untuk seluruh *hosting* aktif yang dikelola di *server* Kementerian. Kendala yang terjadi terkait operasional layanan *hosting* dapat disampaikan kepada Pengelola untuk ditindaklanjuti.
4. Privasi dan Hak Pribadi pengguna
   a. Pengguna mempunyai hak penuh untuk menggunakan layanan *hosting* dengan memperhatikan kebijakan dan prosedur yang berlaku.
   b. Segala sesuatu yang terkait data pihak pengguna tidak akan dipublikasikan oleh Pengelola ke pihak manapun baik organisasi maupun perorangan yang tidak berkepentingan.
5. Keamanan terhadap *password*
   a. Pengguna bertanggung jawab atas kerahasiaan *username* dan *password* atas akun *hosting* yang dikelola.
   b. Pengelola tidak bertanggung jawab terhadap segala sesuatu yang terjadi pada *username* dan *password* pengguna, termasuk di dalamnya apabila diketahui oleh pihak yang tidak memiliki hak sebagai pengguna.

c. Pengguna disarankan untuk memilih *password* yang mengacu kepada standar faktor keamanan dan menggantinya secara berkala setiap periode tertentu.
d. Apabila pengguna lupa *password*, Penanggung Jawab Administratif maupun Penanggung Jawab Teknis dapat menghubungi Pengelola untuk mendapatkan dukungan teknis untuk melakukan *reset password*.

6. Larangan isi *hosting*
   a. Melanggar atau menyalahi hak orang lain, termasuk tanpa kecuali, hak intelektual, hak paten, merek dagang, rahasia dagang, hak cipta, publisitas atau hak milik lainnya dari pihak ketiga.
   b. Melanggar hukum, mengancam, memfitnah, mencemarkan, memperdaya, menipu, curang atau menimbulkan kebencian pada orang atau golongan tertentu.
   c. Menghina, melecehkan, merendahkan atau mengintimidasi individu atau grup individu berdasarkan agama, jenis kelamin, orientasi seksual, ras, etnis, usia atau cacat fisik.
   d. Melanggar norma kesusilaan, cabul dan pornografi.
   e. Menganjurkan atau menyarankan perbuatan yang melanggar hukum.
   f. Menyinggung, memicu pertentangan dan atau permusuhan antar Suku, Agama, Ras dan Antar Golongan (SARA).
   g. Memuat kata-kata atau gambar-gambar yang berisi dan atau menimbulkan rasa ngeri, kasar, kotor, jorok, dan sumpah serapah.
   h. Menyebarkan ideologi atau ajaran tertentu yang dilarang oleh hukum yang berlaku di wilayah Republik Indonesia.
   i. Mengandung virus atau kode komputer lainnya, *file* atau program yang dapat mengganggu, merusak atau membatasi fungsi dari perangkat lunak (*software*) atau perangkat keras (*hardware*) komputer atau peralatan komunikasi, atau memperbolehkan penggunaan komputer atau jaringan komputer yang tidak sah.
   j. Menguras kemampuan *server* dan berimplikasi kepada kinerja *server* secara keseluruhan.

3.6. Tanggung Jawab

1. Tanggung Jawab Pengelola Layanan Hosting
   a. Pengelola menyediakan layanan *hosting* secara gratis kepada Pengguna di lingkungan Kementerian.
   b. Pengelola menyediakan dukungan teknis termasuk di dalamnya melakukan monitoring, pendampingan, dan *reset password* akun *hosting*.
   c. Pengelola tidak bertanggung jawab atas rusak/ hilangnya data Pengguna secara disengaja atau tidak sengaja yang disebabkan oleh kelalaian Pengguna.
   d. Pengelola menyediakan *backup* harian untuk data Pengguna yang disimpan pada *server*.
   e. Pengelola mempunyai kewenangan untuk melakukan evaluasi dan pemantauan terhadap segala aktivitas pada seluruh domain dan sub domain yang dikelola oleh Kementerian.
   f. Jika terdapat perubahan layanan yang mengharuskan Pengguna melakukan aksi tertentu, Pengelola akan menyampaikan informasi perubahan layanan kepada Pengguna melalui Nota Dinas.
   g. Pengelola tidak menyediakan dukungan teknis terkait operasional pengelolaan konten maupun pengembangan aplikasi yang terdapat pada *hosting*.
   h. Pengelola berhak menolak permohonan penambahan fitur *hosting* dengan mempertimbangkan latar belakang permohonan dan keterbatasan layanan.
   i. Pengelola berhak melakukan pembekuan sementara maupun penutupan permanen layanan *hosting* yang melanggar Kebijakan Layanan Hosting Internal maupun berpotensi mengancam kestabilan layanan *hosting* internal.
2. Tanggung Jawab Pengguna Layanan *Hosting*
   a. Pengguna bertanggung jawab atas kerahasiaan *username* dan *password* akun *hosting* yang dikelola.
   b. Pengguna bertanggung jawab secara hukum sepenuhnya atas seluruh konten pada layanan *hosting* yang dikelola.

c. Pengguna memahami dan setuju untuk tidak menggunakan, menempatkan, mengunduh, menautkan, melekatkan dan/atau menayangkan konten yang terlarang.
d. Pengguna tidak diperbolehkan menjalankan proses yang tidak aman, menguras kemampuan *server*, ataupun yang meningkatkan resiko terbobolnya akun atau *server*.
e. Pengguna tidak diperbolehkan menggunakan layanan *hosting* untuk melakukan tindakan yang bertentangan dengan hukum yang berlaku di wilayah Republik Indonesia maupun hukum internasional.

3.7. Larangan Pengguna *Hosting*

1. Menggunakan *server hosting* untuk kegiatan yang bertentangan dengan hukum yang berlaku di Republik Indonesia.
2. Mengelola konten yang mengandung unsur SARA, pornografi dam pelanggaran terhadap hak cipta.
3. Menggunakan layanan *hosting* untuk tujuan kriminal (*hacking*, *phising*).
4. Menggunakan layanan *hosting* dalam upaya memperkaya atau menguntungkan pribadi maupun golongan.
5. Menyimpan konten yang secara langsung atau tidak langsung mengandung konten yang bersifat ilegal yang dilarang secara hukum.
6. Mencoba merusak maupun mengubah data dan sistem yang berada pada *server hosting* yang bukan merupakan hak dari pengguna bersangkutan, atau melakukan hal-hal yang bisa dikategorikan merugikan sistem informasi Kementerian baik sebagian maupun keseluruhan.
7. Mencoba merusak maupun mengubah data dan sistem *server* milik pihak ketiga lainnya melalui *server hosting* Kementerian.

3.8. Pelanggaran Aturan

1. Pengelola memberi peringatan sebanyak 1 (satu) kali kepada pemilik *hosting* melalui surat resmi maupun Nota Dinas kepada Penanggung Jawab Administratif maupun teknis secepatnya sejak ditemukan adanya pelanggaran Kebijakan Layanan *Hosting* Internal.

2. Apabila peringatan diabaikan, Pengelola dapat menghentikan layanan secara sepihak terhadap Pengguna sampai pihak Pengguna melakukan klarifikasi kepada Pengelola atas pelanggaran yang diindikasikan.
3. Selama pemberhentian layanan, data Pengguna yang ada di *server hosting* menjadi hak Pengelola.

4. KEBIJAKAN INTERNAL INOVASI PROSES BISNIS SPBE

4.1. Dasar Hukum

1. Peraturan Presiden Republik Indonesia Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik;
2. Peraturan Menteri Komunikasi dan Informatika Nomor: 41/PER/MEN.KOMINFO/11/2007 tentang Panduan Umum Tata Kelola Informasi dan Komunikasi Nasional;
3. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Republik Indonesia Nomor 19 Tahun 2018 tentang Penyusunan Peta Proses Bisnis Instansi Pemerintah;
4. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Republik Indonesia Nomor 59 Tahun 2020 tentang Pemantauan dan Evaluasi Sistem Pemerintahan Berbasis Elektronik;
5. Keputusan Menteri Koordinator Bidang Perekonomian Nomor Kep-70/M.EKON/12/2008 tentang Standar Prosedur Operasi (*Standard Operating Procedures*) pada Sekretariat, Staf Ahli, dan Inspektorat Kementerian Koordinator Bidang Perekonomian;
6. Keputusan Menteri Koordinator Bidang Perekonomian Nomor 406 Tahun 2020 tentang Peta Proses Bisnis Kementerian Koordinator Bidang Perekonomian.

4.2. Pendahuluan

Reformasi birokrasi merupakan suatu upaya yang terencana dan sistematis untuk mengubah struktur, sistem, dan nilai - nilai dalam pemerintahan menjadi lebih baik dari sebelumnya. Proses bisnis yang berbelit - belit dan tumpang tindih antara satu unit kerja dengan unit kerja lain akan membuat organisasi menjadi lambat untuk bekerja. Oleh karena itu setiap unit kerja memerlukan peta proses bisnis yang mampu

menggambarkan proses bisnis yang terintegrasi dan saling terkait dalam mencapai visi, misi, dan tujuan Kementerian Koordinator Bidang Perekonomian.

Penyusunan proses bisnis bertujuan untuk memberikan pedoman dalam penggunaan data dan informasi, penerapan aplikasi SPBE, keamanan SPBE, dan layanan SPBE serta guna melaksanakan visi dan misi SPBE di lingkungan Kementerian Koordinator Bidang Perekonomian. Dengan adanya proses bisnis sebagai standar pelaksanaan pekerjaan maka akan memudahkan dalam mengendalikan dan mempertahankan kualitas pelaksanaan pekerjaan. Penyusunan proses bisnis terintegrasi dapat dilakukan berdasarkan arsitektur SPBE untuk menganalisa seluruh proses bisnis yang sedang dijalankan baik internal di dalam Kementerian Koordinator Bidang Perekonomian maupun dengan pihak eksternal. Proses bisnis yang saling terkait disusun secara terintegrasi untuk mendukung pembangunan atau pengembangan aplikasi SPBE dan layanan SPBE yang terintegrasi.

4.3. Definisi

1. Proses bisnis atau alur kerja yang dapat berupa proses bisnis makro, meso, ataupun mikro (SOP) adalah sekumpulan tugas atau kegiatan yang terstruktur dan saling terkait dalam pelaksanaan tugas dan fungsi di mana dapat dilakukan secara berurutan ataupun bersamaan oleh manusia atau sistem baik di dalam maupun di luar Kementerian Koordinator Bidang Perekonomian.
2. Integrasi proses bisnis merupakan penyesuaian dan penyatuan antar proses bisnis unit kerja sehingga mencapai satu kesatuan proses bisnis dengan seluruh tugas dan fungsinya. Integrasi proses bisnis juga dapat dilakukan antar proses bisnis instansi pusat, antar pemerintah daerah, dan/atau antar instansi pusat dan pemerintah dalam membangun hubungan alur kerja antar instansi pusat, dan/atau antar instansi pusat dengan pemerintah daerah.
3. Inovasi proses bisnis terintegrasi adalah terobosan atau pembaharuan integrasi proses bisnis yang diinisiasi oleh instansi pusat ataupun daerah.
4. Standardisasi penyusunan proses bisnis merupakan penyusunan proses bisnis yang sesuai dengan pedoman yang telah ditetapkan.

5. Dua tipe utama proses bisnis yaitu proses inti dan proses pendukung. Proses inti adalah proses yang memenuhi kriteria berikut: berperan langsung dalam memenuhi kebutuhan pengguna eksternal, secara langsung berpengaruh terhadap keberhasilan organisasi, dan memberikan respon permintaan dan memenuhi kebutuhan pengguna. Sedangkan proses pendukung adalah proses yang memenuhi kriteria: memenuhi kebutuhan pengguna internal, para pelaku atau fungi di proses inti dan tidak memiliki kaitan langsung dengan nilai manfaat organisasi.

4.4. Inovasi Proses Bisnis SPBE di Kementerian Koordinator Bidang Perekonomian

1. Keterpaduan proses bisnis diterapkan melalui integrasi layanan SPBE dengan sistem elektronik antar instansi pusat.
2. Tahapan penyusunan proses bisnis terintegrasi mengacu pada Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Republik Indonesia Nomor 19 Tahun 2018 tentang Penyusunan Peta Proses Bisnis Instansi Pemerintah.
3. Ruang lingkup penyusunan proses bisnis meliputi seluruh kegiatan di lingkungan Kementerian Koordinator Bidang Perekonomian serta integrasi proses bisnis baik di dalam instansi maupun antar kementerian, lembaga, atau pemerintah daerah sesuai dengan dokumen rencana strategis dan rencana kerja organisasi.
4. Setiap unit kerja wajib menyusun proses bisnis dan Standar Operasional Prosedur dengan berpedoman pada peraturan dan standar yang berlaku di Kementerian Koordinator Bidang Perekonomian.
5. Proses bisnis dituangkan ke dalam dokumen yang terstandardisasi, dikomunikasikan, dipahami, dan diterapkan di seluruh unit kerja di lingkungan Kementerian Koordinator Bidang Perekonomian.
6. Penerapan proses bisnis terintegrasi dipantau, dievaluasi, dan diperbaiki oleh Tim Penilai SPBE dari KemenpanRB secara berkala terhadap perubahan lingkungan, teknologi, dan kebutuhan Kementerian Koordinator Bidang Perekonomian.
7. Kebijakan internal inovasi proses bisnis dipantau, dinilai, dan dievaluasi secara berkala terhadap perubahan lingkungan, teknologi dan kebutuhan

Kementerian Koordinator Bidang Perekonomian oleh Tim Penilai SPBE dari Kementerian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi.

5. KEBIJAKAN INTERNAL ANGGARAN DAN BELANJA TIK

5.1. Dasar Hukum

1. Peraturan Presiden Republik Indonesia Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik;
2. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Republik Indonesia Nomor 59 Tahun 2020 tentang Pemantauan dan Evaluasi Sistem Pemerintahan Berbasis Elektronik;

5.2. Pendahuluan

Manajemen rencana dan anggaran belanja TIK merupakan hal yang penting agar pelaksanaan belanja TIK sesuai dengan kebutuhan dan perencanaan strategis yang tertuang dalam Rencana Induk SPBE Kementerian Koordinator Bidang Perekonomian dan terpadu dengan Rencana Induk SPBE Nasional dan anggaran SPBE. Indikator keberhasilan dari manajemen belanja/investasi TIK adalah digunakannya sumber-sumber pendanaan yang efisien, kesesuaian realisasi penyerapan anggaran TIK dengan realisasi pekerjaan yang direncanakan, dan diperolehnya sumber daya TIK yang berkualitas dengan melalui proses belanja/ investasi TIK yang efisien, cepat, bersih dan transparan.

5.3. Definisi

Perencanaan dan penganggaran TIK adalah proses perencana dan penganggaran untuk belanja Teknologi Informasi dan Komunikasi di instansi pusat atau pemerintah daerah yang disusun sesuai dengan proses perencanaan dan penganggaran tahunan pemerintah berdasarkan ketentuan peraturan perundang-undangan.

5.4. Rencana dan Anggaran Belanja TIK Kementerian Koordinator Bidang Perekonomian

1. Penyusunan rencana dan anggaran belanja TIK disesuaikan dengan rencana induk SPBE, arsitektur SPBE dan peta rencana SPBE Kementerian Koordinator Bidang Perekonomian.
2. Penyusunan rencana dan anggaran belanja TIK didahului dengan pengajuan perencanaan kebutuhan dan penyelenggaraan TIK oleh unit Penyelenggara SPBE Kementerian Koordinator Bidang Perekonomian.
3. Bagian Program dan Anggaran Kementerian Koordinator Bidang Perekonomian melakukan validasi terkait rencana dan anggaran belanja TIK untuk menjamin efektivitas dan efisiensi belanja TIK Kementerian Koordinator Bidang Perekonomian dengan memperhatikan keamanan informasi, ketersediaan, keterpaduan dengan sistem terkait, kemudahan operasional, dan kemudahan pemeliharaan.
4. Anggaran TIK Kementerian Koordinator Bidang Perekonomian meliputi:
   a. sarana dan prasarana TIK seperti perangkat dan aplikasi;
   b. sumber daya manusia seperti honor pelaksanaan kegiatan, narasumber, dan pelatihan;
   c. implementasi TIK seperti biaya infrastruktur, keamanan TIK, pembuatan aplikasi, pengadaan data dan informasi, pemeliharaan, dan sosialisasi.
5. Unit Penyelenggara SPBE Kementerian mengkordinasikan perencanaan, anggaran, dan aset terkait keperluan implementasi TIK di lingkungan Kementerian Koordinator Bidang Perekonomian.
6. Kebijakan internal anggaran belanja TIK dipantau, dinilai, dan dievaluasi secara berkala terhadap perubahan lingkungan, teknologi dan kebutuhan Kementerian Koordinator Bidang Perekonomian oleh Tim Penilai SPBE dari Kementerian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi.

6. KEBIJAKAN INTERNAL PUSAT DATA (*DATA CENTER*)

6.1. Tujuan

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

6.2. Ruang Lingkup

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

6.3. Kebijakan

1. Kementerian menyediakan fasilitas berupa pusat data (*data center*) untuk pengelolaan e-Government.
2. Penyelenggara pusat data (*data center*) Kementerian dilakukan secara terpusat oleh Unit Penyelenggara SPBE Kementerian.
3. Unit Penyelenggara SPBE Kementerian menyediakan layanan penempatan (*hosting*) portal web (*website*) dan aplikasi berbasis web kepada setiap Unit Kerja.
4. Unit Penyelenggara SPBE Kementerian menyediakan layanan pencadangan sistem (*system backup*) untuk aplikasi yang bersifat umum dan aplikasi khusus untuk Unit Kerja.
5. Unit Penyelenggara SPBE Kementerian 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 poin 3
6. Pemilik aplikasi bertanggung jawab akan pengelolaan aplikasi, validitas data, dan pengelolaan hak aksesnya.
7. Dalam keadaan pemilik aplikasi kehilangan hak akses, Unit Penyelenggara SPBE Kementerian dapat membuat hak akses baru berdasarkan surat resmi pemilik aplikasi.
8. Unit Penyelenggara SPBE Kementerian berhak melakukan pengujian aplikasi yang akan ditempatkan (*hosting*) sesuai dengan standar keamanan informasi yang telah ditetapkan.
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 Kementerian dan tidak boleh digunakan di luar Kementerian tanpa izin dari Unit Penyelenggara SPBE Kementerian.

6.4. Standar

1. Pedoman penyelenggaraan pusat data (*data center*) terdiri atas:
   a. Persyaratan Disain Teknis dan Implementasi;
   b. Persyaratan Operasi;
   c. Persyaratan Keberlangsungan Kegiatan.
2. Persyaratan disain teknis dan implementasi pusat data (*data center*) paling sedikit harus memenuhi aspek-aspek sebagai berikut:
   a. 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.
   b. 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.
   c. 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 Unit Penyelenggara SPBE Kementerian.

d. Peringatan Kebakaran, Deteksi Asap, dan Pemadam Kebakaran
   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 preaction.
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.

e. 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.

f. 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).

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

h. 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.

3. Persyaratan operasi pusat data (*data center*) paling sedikit harus memenuhi aspek sebagai berikut:
   a. 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.
   b. 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 peralatan
5) 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.
6) 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.
7) Prosedur tertulis harus tersedia dan mudah diakses untuk menjelaskan secara rinci status peringatan dan bagaimana gangguan sistem ditangani oleh staf pusat data (*data center*).

c. 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.

4. Persyaratan keberlangsungan kegiatan pusat data (data center) paling sedikit harus memenuhi aspek sebagai berikut :
   a. 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.
   b. 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 Unit Penyelenggara SPBE Kementerian oleh pengguna pusat data (*data center*).
      3) Pihak manajemen harus menelaah setiap insiden sebagai berikut:
         a) Insiden yang terjadi
         b) Dimana terjadi
         c) Kapan terjadi
         d) Dampak terhadap penyediaan layanan
         e) Bagaimana mengatasinya
         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 (*startup*) 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.

c. 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.

6.5. Istilah yang Digunakan

1. Pusat data (*data center*) adalah suatu fasilitas yang digunakan untuk menempatkan sistem elektronik dan komponen terkaitnya untuk keperluan penempatan, penyimpanan, dan pengolahan data.
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 Kementerian secara berkesinambungan ketika pusat data (*data center*) mati/rusak karena bencana.

7. KEBIJAKAN INTERNAL INTEGRASI PEMBANGUNAN APLIKASI SPBE

7.1. Tujuan

Kebijakan dan standar ini digunakan sebagai pedoman dalam integrasi pengembangan Aplikasi di lingkungan Kementerian Koordinator Perekonomian agar pelaksanaan integrasi pengembangan Aplikasi dapat dilaksanakan secara efektif dan efisien.

7.2. Ruang Lingkup

Kebijakan dan standar ini berlaku untuk integrasi pengembangan aplikasi di Kementerian koordinator bidang perekonomian yang dilaksanakan secara internal

dan/atau ekternal yang menggunakan pihak ketiga, yang mencakup komponen sistem aplikasi, basis data, dan sistem jaringan.

7.3. Kebijakan

1. Aplikasi harus dikembangkan oleh pemilik proses bisnis sesuai dengan tugas dan fungsinya;
2. Pemilik proses bisnis bertanggung jawab atas aplikasi yang dikembangkan;
3. Penyelenggara integrasi pengembangan aplikasi merupakan pihak yang ditunjuk oleh pemilik proses bisnis untuk mengembangkan aplikasi mulai dari perencanaan hingga implementasinya;
4. Setiap Pimpinan Unit Organisasi bertanggung jawab dalam penerapan Kebijakan dan Standar Integrasi pengembangan Aplikasi di Unit Organisasi masing-masing;
5. Unit Organisasi harus menerapkan Kebijakan dan Standar Integrasi pengembangan Aplikasi di Unit Organisasi masing-masing;
6. Setiap Pimpinan Unit Organisasi bertanggung jawab dalam membangun kompetensi integrasi pengembangan aplikasi bagi pejabat/staf di Unit Organisasi masing-masing untuk mendukung kelancaran integrasi pengembangan aplikasi;
7. Setiap kegiatan integrasi pengembangan aplikasi harus dibentuk tim integrasi pengembangan aplikasi yang sekurang-kurangnya terdiri atas: manajer proyek, sistem analis, pemilik proses bisnis, penguji aplikasi, dan pemrogram (*programmer*);
8. Unit Organisasi harus berkoordinasi dengan Unit Penyelenggara SPBE Kementerian selama proses integrasi pengembangan aplikasi sampai dengan operasionalisasi aplikasi;
9. Unit Penyelenggara SPBE Kementerian sebagai pengatur, pembina dan pengawas TIK di Kementerian memiliki kewenangan untuk memastikan bahwa proses integrasi pengembangan telah sesuai dengan kebijakan dan standar integrasi pengembangan aplikasi;
10. Aplikasi yang telah dikembangkan untuk kepentingan Kementerian dan Unit Organisasi harus ditempatkan di Unit Penyelenggara SPBE Kementerian;

11. Aplikasi yang sudah dikembangkan menjadi milik Kementerian dan tidak boleh digunakan di luar Kementerian tanpa izin dari pejabat yang berwenang.

7.4. Tanggung Jawab

1. Pihak-pihak yang terkait dalam integrasi pengembangan aplikasi terdiri dari:
   a. Pemilik proses bisnis adalah Pimpinan Unit Organisasi atau Pejabat di Kementerian yang memiliki kebutuhan akan adanya aplikasi untuk mendukung berjalannya tugas dan fungsi;
   b. Pengembang aplikasi adalah pegawai pada Unit Organisasi di Kementerian dan/atau Pihak Ketiga yang melaksanakan integrasi pengembangan aplikasi;
   c. Tim pengendalian mutu (*quality assurance*) adalah tim yang ditunjuk oleh pemilik proses bisnis untuk melaksanakan kegiatan pengendalian mutu dalam integrasi pengembangan aplikasi di luar tim pengembang aplikasi;
   d. Pengguna aplikasi;
   e. Unit Penyelenggara SPBE Kementerian.
2. Pemilik proses bisnis mempunyai tanggung jawab terhadap:
   a. Pemberian persetujuan:
      1) Dokumen analisis dan spesifikasi kebutuhan aplikasi serta perubahannya;
      2) Dokumen rancangan tingkat tinggi (*high level design*) dan rancangan rinci (*detail design*);
      3) Dokumentasi integrasi pengembangan aplikasi; dan
      4) Dokumen rencana dan skenario pengujian.
   b. Pelaksanaan *User Acceptance Test* (UAT);
   c. Memastikan bahwa aplikasi yang akan ditempatkan (*hosting*) di pusat data (*data center*) sudah bebas bug dan error;
   d. Pemeriksaan laporan UAT untuk memastikan keluaran yang dihasilkan oleh pengembang aplikasi sesuai dengan dokumen sebagaimana dimaksud pada butir 4.2.1.a;

e. Pemeriksaan dan penandatanganan berita acara analisis hasil pengujian dan juga berita acara hasil tinjauan pasca implementasi aplikasi; dan
f. Memberi masukan kepada pengembang aplikasi terkait integrasi pengembangan dan penyempurnaan aplikasi.
g. Melakukan evaluasi pasca implementasi dan melaporkan hasilnya ke Unit Penyelenggara SPBE Kementerian.

3. Pengembang aplikasi mempunyai tanggung jawab terhadap:
   a. Pelaksanaan siklus integrasi pengembangan aplikasi sesuai kebijakan dan standar siklus integrasi pengembangan aplikasi di Kementerian;
   b. Tindak lanjut masukan dari pemilik proses bisnis terkait integrasi pengembangan dan penyempumaan aplikasi;
   c. Pemeriksaan dan penandatanganan berita acara analisis hasil pengujian dan juga berita acara hasil tinjauan pasca implementasi aplikasi;
   d. Penyusunan laporan status dan kemajuan pelaksanaan integrasi pengembangan aplikasi secara berkala serta pelaporan kepada pemilik proses bisnis;
   e. Penyusunan laporan terkait perubahan integrasi pengembangan aplikasi berdasarkan hasil UAT serta pelaporan kepada pemilik proses bisnis; dan
   f. Penyusunan dokumentasi yang merupakan keluaran pada semua tahapan integrasi pengembangan aplikasi.
4. Tim pengendalian mutu (*quality assurance*) mempunyai tanggung jawab terhadap:
   a. Pendampingan dan pengendalian mutu dalam integrasi pengembangan aplikasi;
   b. Penyusunan laporan pengendalian mutu (*quality assurance*) dalam setiap tahapan integrasi pengembangan aplikasi;
   c. Pelaksanaan *User Acceptance Test* (UAT).
5. Pengguna dapat memberi masukkan kepada Pemilik proses bisnis terkait integrasi pengembangan dan penyempurnaan aplikasi.

6. Unit Penyelenggara SPBE Kementerian mempunyai tanggung jawab terhadap:
    a. Pendampingan dalam pelaksanaan pengendalian mutu dalam integrasi pengembangan aplikasi;
    b. Pengaturan, pembinaan, dan pengawasan pelaksanaan integrasi pengembangan aplikasi di Kementerian;
    c. Memastikan bahwa integrasi pengembangan aplikasi baik proses maupun produk yang dihasilkan sesuai dengan standar aplikasi yang berlaku di Kementerian yang ditetapkan oleh Unit Penyelenggara SPBE Kementerian;
    d. Memastikan tidak terjadi redundansi integrasi pengembangan aplikasi untuk produk aplikasi sejenis;
    e. Melakukan monitoring dan evaluasi proses integrasi pengembangan aplikasi dan melaporkan kepada Menteri setiap akhir tahun anggaran.

7.5. Standar

1. Siklus integrasi pengembangan aplikasi terdiri atas:
    a. Proses analisis kebutuhan aplikasi, merupakan proses untuk mengumpulkan dan menganalisis spesifikasi kebutuhan bisnis dan aplikasi secara rinci;
    b. Proses perancangan aplikasi, merupakan proses penyusunan rancangan aplikasi berdasarkan analisis kebutuhan aplikasi dan hasilnya akan digunakan sebagai acuan dalam proses integrasi pengembangan aplikasi;
    c. Proses pengkodean (*coding*) aplikasi, merupakan proses yang dilaksanakan untuk membangun aplikasi sesuai dengan kebutuhan berdasarkan rancangan aplikasi;
    d. Proses pengujian aplikasi, merupakan proses yang dilaksanakan untuk menguji aplikasi yang telah dikembangkan;
    e. Proses implementasi aplikasi, merupakan proses penerapan aplikasi yang telah dikembangkan pada lingkungan operasional; dan
    f. Proses tinjauan pasca implementasi aplikasi, merupakan proses evaluasi yang dilaksanakan sebagai bahan pembelajaran untuk integrasi pengembangan aplikasi selanjutnya.

2. Proses analisis kebutuhan aplikasi
    a. Proses analisis kebutuhan aplikasi meliputi kegiatan:
        1) Pengumpulan, analisis, penyusunan, dan pendokumentasian spesifikasi kebutuhan bisnis dan aplikasi yang mencakup:
            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 integrasi 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.
    b. Proses analisis kebutuhan aplikasi menghasilkan keluaran:
        1) Dokumen analisis dan spesifikasi kebutuhan aplikasi; dan
        2) Dokumen perubahan analisis dan perubahan spesifikasi kebutuhan aplikasi.
3. Proses Perancangan Aplikasi
    a. Sistem aplikasi dan basis data, meliputi kegiatan:
        1) Penyusunan dan pendokumentasian rancangan tingkat tinggi dengan mengacu pada dokumen sebagaimana dimaksud pada poin 2.b.) 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 data 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*).

b. Sistem jaringan pendukung aplikasi, meliputi kegiatan:
   1) Penyusunan dan pendokumentasian rancangan tingkat tinggi dengan mengacu pada dokumen 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 integrasi 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 Kementerian.
3) Menghasilkan keluaran:
   a) Dokumen rancangan tingkat tinggi; dan
   b) Dokumen rancangan rinci.

4. Proses Pengkodean (*coding*) Aplikasi
   a. 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 integrasi 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 Kementerian.

b. Sistem jaringan pendukung aplikasi, meliputi kegiatan:
   1) Pelaksanaan integrasi pengembangan sistem jaringan pendukung aplikasi sesuai dengan rancangan rinci yang telah disetujui;
   2) Pengelolaan perubahan sistem jaringan akibat adanya proses integrasi pengembangan sistem aplikasi;
   3) Penyusunan dokumentasi integrasi pengembangan sistem jaringan pendukung aplikasi:
      a) Formulir perubahan;
      b) Rencana dan laporan hasil integrasi pengembangan jaringan terkait integrasi pengembangan aplikasi;
      c) Dokumentasi setiap tahapan integrasi 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 Informasi di Kementerian;
   5) Menghasilkan keluaran:
      a) Sistem aplikasi dan basis data, serta sistem jaringan pendukung aplikasi sesuai dengan rancangan rinci; dan
      b) Dokumentasi pengernbangan aplikasi.

5. Proses Pengujian Aplikasi
   a. 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

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

6. Proses Implementasi Aplikasi
a. Proses implementasi aplikasi meliputi kegiatan:
1) Penyusunan rencana implementasi aplikasi di lingkungan operasional yang mencakup sekurang-kurangnya:
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.

b. 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) Buku panduan penggunaan aplikasi (*user manual*).

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

d. Proses tinjauan pasca implementasi aplikasi menghasilkan keluaran:

e. Laporan evaluasi pasca implementasi aplikasi;

f. Dokumen tinjauan pasca implementasi aplikasi.

7. Pengendalian Mutu

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

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

c. Menghasilkan keluaran berupa laporan pengendalian mutu.

8. Standar keamanan aplikasi yang dikembangkan harus mengacu pada Kebijakan dan Standar Keamanan Informasi di Kementerian.

7.6. Istilah yang Digunakan

1. *Backup Plan* adalah rencana pemulihan sistem ke kondisi semula sebelum terjadi permasalahan terkait proses implementasi.
2. *Fall-backplan* adalah merupakan rencana alternative (yang menghilangkan dampak negatif) apabila terjadi kegagalan di dalam implementasi TIK.
3. Pengujian integrasi (*integration testing*) adalah pengujian integrasi dari unit-unit dalam suatu aplikasi yang sudah teruji dalam pengujian unit (*unit testing*).
4. Jejak audit (*audit trail*) adalah urutan kronologis catatan audit yang berkaitan dengan pelaksanaan suatu kegiatan.
5. *Joint Application Development* (JAD) adalah integrasi pengembangan aplikasi yang dilaksanakan secara bersama-sama oleh pengembang aplikasi di Kementerian dan pengembang aplikasi dari Pihak Ketiga.
6. Konsep dasar operasional adalah dokumen yang menjelaskan karakteristik kuantitatif dan kualitatif suatu sistem yang dibutuhkan dari sudut pandang calon pengguna aplikasi.
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.
8. Rancangan tingkat tinggi (*high level design*) adalah suatu overview terhadap aplikasi yang memperlihatkan gambaran menyeluruh dari suatu aplikasi.
9. Siklus integrasi pengembangan aplikasi disebut juga sebagai *System Development Life Cycle*/SDLC adalah siklus integrasi pengembangan aplikasi terdiri dari proses analisis kebutuhan, proses perancangan, proses integrasi pengembangan, proses pengujian, proses implementasi, dan proses tinjauan pasca implementasi aplikasi yang dapat dilaksanakan oleh internal, pihak ketiga, atau melalui *Joint Application Development* (JAD).
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.

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.
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 integrasi pengembangan (*roll-out*), dan pengujian akhir (*final acceptance test*).

8. KEBIJAKAN INTERNAL PENGGUNAAN APLIKASI UMUM BERBAGI PAKAI

8.1. Dasar Hukum

1. Peraturan Presiden Republik Indonesia Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik;
2. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Republik Indonesia Nomor 59 Tahun 2020 tentang Pemantauan dan Evaluasi Sistem Pemerintahan Berbasis Elektronik;
3. SNI ISO 27001 Sistem Manajemen Keamanan Informasi.

8.2. Pendahuluan

Penggunaan aplikasi umum SPBE berbagi pakai dilakukan untuk meningkatkan efisiensi belanja TIK khususnya pembangunan aplikasi SPBE dan memudahkan integrasi proses bisnis pemerintahan. Optimalisasi penggunaan aplikasi berbagi pakai dapat menggunakan teknologi komputasi awan, teknologi media sosial, teknologi otomasi dan integrasi, teknologi IoT, dan teknologi analitik data.

8.3. Definisi

Aplikasi umum berbagi pakai adalah aplikasi SPBE yang sama, standar, dan digunakan secara berbagi pakai oleh instansi pusat dan/atau pemerintah daerah, seperti aplikasi naskah dinas elektronik, aplikasi manajemen kepegawaian, aplikasi penganggaran berbasis kinerja, aplikasi pengaduan publik, dan sebagainya.

8.4. Aplikasi Umum Berbagi Pakai di Kementerian Koordinator Bidang Perekonomian

1. Rencana aplikasi umum berbagi pakai yang dilakukan secara keseluruhan dituangkan dalam arsitektur aplikasi di Rencana lnduk SPBE Kementerian Koordinator Bidang Perekonomian.
2. Aplikasi umum berbagi pakai dilakukan melalui:
   a. penyelenggaraan sistem aplikasi perencanaan, penganggaran, pengadaan, akuntabilitas kinerja, dan pemantauan dan evaluasi yang terintegrasi dengan basis data terintegrasi untuk bagi pakai data;
   b. penyelenggaraan sistem aplikasi kearsipan yang terintegrasi dengan basis data terintegrasi untuk bagi pakai data;
   c. penyelenggaraan sistem aplikasi kepegawaian yang terintegrasi dengan basis data terintegrasi untuk bagi pakai data;
   d. penyelenggaraan transaksi layanan kepegawaian dengan basis data terintegrasi untuk bagi pakai data;
   e. penyelenggaraan sistem aplikasi pengaduan pelayanan publik yang terintegrasi dengan basis data terintegrasi untuk bagi pakai data.
3. Aplikasi umum berbagi pakai yang digunakan di lingkungan Kementerian Koordinator Bidang Perekonomian sesuai dengan ketentuan nasional yang berlaku.
4. Jika aplikasi yang sejenis dengan aplikasi umum telah dioperasikan di lingkungan Kementerian Koordinator Bidang Perekonomian sebelum aplikasi umum ditetapkan, maka diharuskan:
   a. melakukan kajian biaya dan manfaat terhadap penggunaan dan pengembangan aplikasi sejenis;
   b. melakukan pengembangan aplikasi sejenis yang disesuaikan dengan proses bisnis dan fungsi pada aplikasi umum; dan
   c. aplikasi umum dan kode sumbemya didaftarkan dan disimpan pada repositori aplikasi SPBE.
5. Penggunaan aplikasi umum berbagi pakai di Kementerian Koordinator Bidang Perekonomian dikendalikan, dinilai secara kuantitatif, dan dievaluasi secara berkala sehingga kinerja aplikasi dapat ditingkatkan secara berkesinambungan oleh Tim Penilai SPBE Kementerian PANRB.

6. Audit aplikasi umum dilaksanakan sesuai dengan ketentuan yang berlaku secara nasional.
7. Kebijakan internal aplikasi umum berbagi pakai dipantau, dinilai, dan dievaluasi secara berkala terhadap perubahan lingkungan, teknologi, dan kebutuhan Kementerian Koordinator Bidang Perekonomian oleh Tim penilai SPBE dari Kementerian PANRB.

9. KEBIJAKAN INTERNAL STANDAR KEAMANAN INFORMASI

9.1. Tujuan

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

9.2. Ruang Lingkup

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

9.3. Kebijakan

1. Setiap Pimpinan Unit Kerja bertanggung jawab mengatur penerapan Kebijakan dan Standar Keamanan Informasi yang ditetapkan dalam Peraturan Menteri ini di Unit masing-masing.
2. Unit Kerja harus menerapkan Kebijakan dan Standar Keamanan Informasi yang ditetapkan dalam kebijakan ini di Unit masing-masing.
3. Setiap Pimpinan Unit Kerja bertanggung jawab mengatur pelaksanaan pengamanan dan perlindungan aset informasi di Unit masing-masing dengan mengacu pada Kebijakan dan Standar Keamanan Informasi di Kementerian yang ditetapkan dalam Peraturan Menteri ini.
4. Unit Penyelenggara SPBE Kementerian dan Unit Kerja bertanggung jawab meningkatkan pengetahuan, keterampilan, dan kepedulian terhadap keamanan informasi pada seluruh pengguna di lingkungan Unit Kerja masing-masing.
5. Unit Penyelenggara SPBE Kementerian dan Unit Kerja menerapkan dan mengembangkan manajemen risiko dalam rangka pelaksanaan pengamanan dan perlindungan aset informasi.
6. Pihak ketiga harus bertanggung jawab untuk melindungi kerahasiaan, keutuhan, dan/atau ketersediaan aset informasi Kementerian.
7. Unit Penyelenggara SPBE Kementerian dan Unit Kerja melakukan evaluasi terhadap pelaksanaan Keamanan Informasi secara berkala untuk menjamin efektivitas dan meningkatkan keamanan informasi.
8. Inspektorat dapat melakukan audit internal Keamanan Informasi di Kementerian untuk memastikan pengendalian, proses, dan prosedur Keamanan Informasi dilaksanakan secara efektif sesuai dengan Kebijakan dan Standar Keamanan Informasi di Kementerian.
9. Unit Penyelenggara SPBE Kementerian dan Unit Kerja menggunakan laporan audit internal Keamanan Informasi untuk meninjau efektivitas penerapan Keamanan Informasi dan melakukan tindak lanjut terhadap temuan auditor.

9.4. Tanggung Jawab

1. Pihak-pihak yang terkait dalam keamanan informasi terdiri dari:
    a. Pemilik aset informasi adalah Pimpinan Unit Kerja yang memiliki kebutuhan akan keamanan informasi untuk mendukung tugas dan fungsinya;
    b. Petugas keamanan informasi adalah pegawai Kementerian dan/atau Pihak Ketiga yang melaksanakan tanggung jawab terkait keamanan informasi;
    c. Tim pengendali mutu keamanan informasi (*information security assurance*) adalah tim yang dibentuk untuk melaksanakan kegiatan penjaminan keamanan informasi;
    d. Pengguna, adalah pegawai dan bukan pegawai Kementerian yang mengakses informasi Kementerian.
2. Pemilik aset informasi mempunyai tanggung jawab terhadap:
    a. Menetapkan target keamanan informasi setiap tahunnya dan menyusun rencana kerja untuk Kementerian, masing-masing Unit Kerja, maupun yang bersifat lintas unit;
    b. Memastikan efektivitas dan konsistensi penerapan Kebijakan dan Standar Keamanan Informasi di Kementerian; dan
    c. Melaporkan kinerja penerapan Kebijakan dan Standar Keamanan Informasi di Kementerian dan pencapaian target kepada tim pengendali mutu keamanan informasi (*information security assurance*).
3. Petugas keamanan informasi mempunyai tanggung jawab terhadap:
    a. Melaksanakan dan mengawasi penerapan Kebijakan dan Standar Keamanan Informasi di Kementerian;
    b. Memberi masukan peningkatan terhadap Kebijakan dan Standar Keamanan Informasi di Kementerian;
    c. Mendefinisikan kebutuhan, merekomendasikan, dan mengupayakan penyelenggaraan pendidikan dan pelatihan keamanan informasi bagi pegawai;
    d. Memantau, mencatat, dan menguraikan secara jelas gangguan keamanan informasi yang diketahui atau laporan yang diterima, dan

menindaklanjuti laporan tersebut sesuai prosedur pelaporan gangguan keamanan informasi; dan

e. Memberi panduan dan/atau bantuan penyelesaian masalah-masalah keamanan informasi.

4. Tim pengendali mutu keamanan informasi (*information security assurance*) mempunyai tanggung jawab terhadap:
   a. Pendampingan dan penjaminan keamanan informasi;
   b. Penyusunan laporan evaluasi pengendali mutu keamanan informasi (*information security assurance*).
5. Pengguna mempunyai tanggung jawab terhadap pemberian masukan kepada pemilik aset informasi dan petugas keamanan informasi terkait keamanan informasi.

9.5. Standar

1. Standar Keamanan Informasi terdiri atas:
   a. Standar Manajemen Keamanan Informasi;
   b. Standar Pengendalian Pengelolaan Aset Informasi;
   c. Standar Pengendalian Keamanan Sumber Daya Manusia;
   d. Standar Pengendalian Keamanan Fisik dan Lingkungan;
   e. Standar Pengendalian Pengelolaan Komunikasi dan Operasional;
   f. Standar Pengendalian Akses;
   g. Standar Pengendalian Keamanan Informasi dalam Pengadaan, Pengembangan, dan Pemeliharaan Sistem informasi;
   h. Standar Pengendalian Pengelolaan Gangguan Keamanan Informasi;
   i. Standar Pengendalian Keamanan Informasi dalam Pengelolaan Kelangsungan Kegiatan; dan
   j. Standar Pengendalian Kepatuhan.
2. Standar Manajemen Keamanan Informasi
   a. Catatan Penerapan Kebijakan dan Standar Keamanan Informasi di Kementerian
      1) Unit Penyelenggara SPBE Kementerian dan Unit Kerja harus menggunakan catatan penerapan Kebijakan dan Standar Keamanan Informasi di Kementerian untuk mengukur kepatuhan dan efektivitas penerapan keamanan informasi.

2) Catatan penerapan Kebijakan dan Standar Keamanan Informasi di Kementerian harus meliputi:
   a) Formulir-formulir sesuai prosedur operasional yang dijalankan;
   b) Catatan gangguan keamanan informasi;
   c) Catatan dari sistem;
   d) Catatan pengunjung di area aman (*secure areas*);
   e) Kontrak dan perjanjian layanan;
   f) Perjanjian kerahasiaan (*confidentiality agreements*); dan
   g) Laporan audit.

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

c. Pengendalian Dokumen
   1) Unit Penyelenggara SPBE Kementerian dan Pemilik Aset Informasi harus mengendalikan dokumen keamanan informasi Kementerian untuk menjaga kemutakhiran dokumen, efektivitas pelaksanaan operasional, menghindarkan dari segala jenis kerusakan, dan mencegah akses oleh pihak yang tidak berwenang.
   2) Unit Penyelenggara SPBE Kementerian dan Pemilik Aset Informasi harus menempatkan dokumen keamanan informasi

Kementerian di semua area operasional sehingga mudah diakses oleh pengguna di unit kerja masing-masing sesuai peruntukannya.

3. Standar Pengendalian Pengelolaan Aset Informasi
   a. Pemilik Aset Informasi menetapkan dan mengkaji secara berkala klasifikasi aset informasi dan jenis perlindungan keamanannya.
   b. Pemilik Aset Informasi menetapkan pihak yang berwenang untuk mengakses aset informasi.
   c. Dalam pengelolaan aset informasi Kementerian, aset informasi diklasifikasikan mengacu kepada peraturan perundangundangan yang berlaku.
4. Standar Pengendalian Keamanan Sumber Daya Manusia
   a. Peran dan tanggung jawab pegawai terhadap keamanan informasi harus menjadi bagian dari penjabaran tugas dan fungsi, khususnya bagi yang memiliki akses terhadap aset informasi;
   b. Pimpinan dari pegawai berkeahlian khusus atau yang berada di posisi kunci (*key person*) harus memastikan ketersediaan pengganti pegawai tersebut dengan kompetensi yang setara apabila pegawai yang bersangkutan mutasi/berhenti;
   c. Peran dan tanggung jawab pegawai terhadap keamanan informasi harus menyertakan persyaratan untuk:
      1) Melaksanakan dan bertindak sesuai dengan tanggung jawabnya terkait keamanan informasi;
      2) Melindungi aset dari akses yang tidak sah, penyingkapan, modifikasi, kerusakan atau gangguan;
      3) Melaksanakan proses keamanan atau kegiatan keamanan informasi sesuai dengan peran dan tanggung jawabnya; dan
      4) Melaporkan kejadian, potensi kejadian, atau risiko keamanan informasi sesuai dengan Kebijakan dan Standar Keamanan Informasi di Kementerian.
   d. Pemeriksaan latar belakang calon pegawai dan pihak ketiga Kementerian harus memperhitungkan privasi, perlindungan data

pribadi dan/atau pekerjaan berdasarkan peraturan perundang-undangan yang berlaku, meliputi:

1) Ketersediaan referensi, dari referensi hubungan kerja, dan referensi pribadi;
2) Pemeriksaan kelengkapan dan ketepatan dari riwayat hidup pemohon;
3) Konfirmasi kualifikasi akademik dan profesional yang diklaim;
4) Pemeriksaan identitas (KTP, paspor atau dokumen sejenis); dan
5) Pemeriksaan lebih rinci, seperti pemeriksaan catatan kriminal.

5. Standar Pengendalian Keamanan Fisik dan Lingkungan
   a. Pengamanan Perangkat
      1) Penempatan dan perlindungan perangkat Penempatan dan perlindungan perangkat harus mencakup:
         a) Perangkat harus diletakkan pada lokasi yang meminimalkan akses yang tidak perlu ke dalam area kerja;
         b) Perangkat pengolah informasi yang menangani informasi sensitif harus diposisikan dan dibatasi arah sudut pandangnya untuk mengurangi risiko informasi dilihat oleh pihak yang tidak berwenang selama digunakan, dan perangkat penyimpanan diamankan untuk menghindari akses oleh pihak yang tidak berwenang;
         c) Perangkat yang memerlukan perlindungan khusus seperti perangkat cetak khusus, perangkat jaringan di luar ruang *server* harus terisolasi;
         d) Langkah-langkah pengendalian dilakukan untuk meminimalkan risiko potensi ancaman fisik, seperti pencurian, api, bahan peledak, asap, air termasuk kegagalan penyediaan air, debu, getaran, efek kimia, gangguan pasokan listrik, gangguan komunikasi, radiasi elektromagnetis, dan perusakan;
         e) Kondisi lingkungan, seperti suhu dan kelembaban harus dimonitor untuk mencegah perubahan kondisi yang dapat mempengaruhi pengoperasian perangkat pengolah informasi;

f) Perlindungan petir harus diterapkan untuk semua bangunan dan filter perlindungan petir harus dipasang untuk semua jalur komunikasi dan listrik; dan

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

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

3) Pengamanan kabel

Perlindungan keamanan kabel mencakup:

a) Pemasangan kabel sumber daya listrik dan kabel telekomunikasi ke perangkat pengolah informasi selama memungkinkan harus terletak di bawah tanah, atau menerapkan alternatif perlindungan lain yang memadai;

b) Pemasangan kabel jaringan harus dilindungi dari penyusupan yang tidak sah atau kerusakan, misalnya dengan menggunakan conduit atau menghindari rute melalui area publik;

c) Pemisahan antara kabel sumber daya listrik dengan kabel telekomunikasi untuk mencegah interferensi;

d) Penandaan/penamaan kabel dan perangkat harus diterapkan secara jelas untuk memudahkan penanganan kesalahan;

e) Penggunaan dokumentasi daftar panel patch diperlukan untuk mengurangi kesalahan; dan

f) Pengendalian untuk sistem informasi yang sensitif harus mempertimbangkan:

- Penggunaan *conduit*;
- Penggunaan ruangan terkunci pada tempat inspeksi dan titik pemutusan kabel;
- Penggunaan rute alternatif dan/atau media transmisi yang menyediakan keamanan yang sesuai;
- Penggunaan kabel fiber optik;

- Penggunaan lapisan elektromagnet untuk melindungi kabel;
- Inisiasi penghapusan teknikal (*technical sweeps*) dan pemeriksaan secara fisik untuk peralatan yang tidak diotorisasi saat akan disambungkan ke kabel; dan
- Penerapan akses kontrol ke panel *patch* dan ruangan kabel.

4) Pemeliharaan perangkat
   a) Perangkat harus dipelihara secara berkala untuk menjamin ketersediaan, keutuhannya (*integrity*), dan fungsinya.
   b) Perangkat harus dipelihara sesuai dengan petunjuk manualnya. Untuk pemeliharaan yang dilakukan oleh pihak ketiga, harus diadakan Perjanjian Tingkat Layanan (*Service Level Agreement*/SLA) yang mendefinisikan tingkat pemeliharaan yang disediakan dan tingkat kinerja yang harus dipenuhi pihak ketiga.
   c) Pemeliharaan terhadap perangkat keras atau piranti lunak dilakukan hanya oleh pegawai yang berwenang.
   d) Dalam hal pemeliharaan perangkat tidak dapat dilakukan di tempat, maka pemindahan perangkat harus mendapatkan persetujuan Pejabat yang berwenang, dan terhadap data yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA yang disimpan dalam perangkat tersebut harus dipindahkan terlebih dahulu.
   e) Otorisasi penggunaan perangkat harus dilakukan secara tertulis dan data-data yang terkait dengan aset informasi yang digunakan, seperti nama pemakai aset, lokasi, dan tujuan penggunaan aset, harus dicatat dan disimpan.
5) Pengamanan perangkat di luar Kementerian.
   Penggunaan perangkat yang dibawa ke luar dari Kementerian harus disetujui oleh Pejabat yang berwenang.
6) Pengamanan penggunaan kembali atau penghapusan/ pemusnahan perangkat.

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

b. Pengamanan Area

1) Seluruh pegawai, pihak ketiga, dan tamu yang memasuki lingkungan Kementerian harus mematuhi aturan yang berlaku di Kementerian.
2) Unit Penyelenggara SPBE Kementerian dan Pemilik Aset Informasi menyimpan perangkat pengolah informasi di ruangan khusus yang dilindungi dengan pengamanan fisik yang memadai antara lain pintu elektronik, sistem pemadam kebakaran, alarm bahaya, dan perangkat pemutus aliran listrik;
3) Akses ke ruang *server*, pusat data, dan area kerja yang berisikan aset informasi yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA harus dibatasi dan hanya diberikan kepada pegawai yang berwenang;
4) Pihak ketiga yang memasuki ruang *server*, pusat data, dan area kerja yang berisikan aset informasi yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA harus didampingi pegawai Unit Penyelenggara SPBE Kementerian dan/atau Unit Kerja sepanjang waktu kunjungan. Waktu masuk dan keluar serta maksud kedatangan harus dicatat dalam buku catatan kunjungan;
5) Kantor, ruangan, dan perangkat yang berisikan aset informasi yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA harus dilindungi secara memadai;
6) Pegawai dan pihak ketiga tidak diizinkan merokok, makan, minum di ruang *server* dan pusat data (*data center*); dan
7) Area keluar masuk barang dan area publik harus selalu dijaga, diawasi dan dikendalikan, dan jika memungkinkan disterilkan dari perangkat pengolah informasi untuk menghindari akses oleh pihak yang tidak berwenang.

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

d. Perlindungan terhadap Ancaman Eksternal dan Lingkungan Perlindungan terhadap ancaman eksternal dan lingkungan harus mempertimbangkan:
   1) Bahan-bahan berbahaya atau mudah terbakar harus disimpan pada jarak yang aman dari area aman (*secure areas*);
   2) Perlengkapan umum, seperti alat tulis, tidak boleh disimpan di dalam area aman (*secure areas*);
   3) Perangkat fallback dan media cadangan (*media backup*) harus diletakkan pada jarak yang aman untuk menghindari kerusakan dari bencana yang mempengaruhi fasilitas utama; dan
   4) Perangkat pemadam kebakaran harus disediakan dan diletakkan di tempat yang tepat dan aman.

6. Standar Pengendalian Pengelolaan Komunikasi dan Operasional
   a. Dokumentasi Prosedur Operasional harus mencakup:
      1) Tata cara pengolahan dan penanganan informasi;
      2) Tata cara menangani kesalahan-kesalahan atau kondisi khusus yang terjadi beserta pihak yang harus dihubungi bila mengalami kesulitan teknis;
      3) Cara memfungsikan kembali perangkat dan cara mengembalikan perangkat ke keadaan awal saat terjadi kegagalan sistem;
      4) Tata cara pencadangan (*backup*) dan penyimpanan ulang (*restore*); dan

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

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

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

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

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

c) Prosedur untuk penggunaan layanan jaringan yang membatasi akses ke layanan jaringan atau aplikasi.

8) Pertukaran Informasi

a) Prosedur pertukaran informasi bila menggunakan perangkat komunikasi elektronik, mencakup:

- Perlindungan pertukaran informasi dari pencegatan, penyalinan, modifikasi, kesalahan penjaluran (*missrouting*), dan perusakan;
- Pendeteksian dan perlindungan terhadap kode berbahaya yang dapat dikirim melalui penggunaan komunikasi elektronik;
- Perlindungan informasi elektronik dalam bentuk lampiran (*attachment*) yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA;
- Pertimbangan risiko terkait penggunaan perangkat komunikasi nirkabel;

b) Pertukaran informasi yang tidak menggunakan perangkat komunikasi elektronik, mengacu pada ketentuan yang berlaku.

c) Pengendalian pertukaran informasi bila menggunakan perangkat komunikasi elektronik, mencakup:

- Pencegahan terhadap penyalahgunaan wewenang pegawai dan pihak ketiga yang dapat membahayakan Organisasi;
- Penggunaan teknik kriptografi;
- Penyelenggaraan penyimpanan dan penghapusan/ pemusnahan untuk semua korespondensi kegiatan, termasuk pesan, yang sesuai dengan ketentuan yang berlaku;
- Larangan meninggalkan informasi sensitif pada perangkat pengolah informasi;
- Pembatasan penerusan informasi secara otomatis;

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

d) Pembangunan kepedulian atas pendaftaran data demografis, seperti alamat surat elektronik atau informasi pribadi lainnya untuk menghindari pengumpulan informasi yang tidak sah; dan

e) Penyediaan informasi internal Kementerian bagi masyarakat umum harus disetujui oleh pemilik informasi dan sesuai dengan ketentuan yang berlaku.

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

a) Kegagalan akses (*access failures*);

b) Pola-pola masuk (*log-on*) yang mengindikasikan penggunaan yang tidak wajar;

c) Alokasi dan penggunaan hak akses khusus (*privileged access capability*);

d) Penelusuran transaksi dan pengiriman dokumen (*file*) tertentu yang mencurigakan; dan

e) Penggunaan sumber daya sensitif.

7. Standar Pengendalian Akses

a. Persyaratan untuk Pengendalian Akses

Pemilik Aset Informasi harus menyusun, mendokumentasikan, dan mengkaji ketentuan akses ke aset informasi berdasarkan kebutuhan

organisasi dan persyaratan keamanan. Persyaratan untuk pengendalian akses mencakup:

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

b. Pengelolaan Akses Pengguna

Unit Penyelenggara SPBE Kementerian dan Pemilik Aset Informasi harus menyusun prosedur pengelolaan hak akses pengguna sesuai dengan peruntukannya. Prosedur pengelolaan akses pengguna harus mencakup:

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

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

c. Pengelolaan Hak Akses Khusus (*privilege management*)

Unit Penyelenggara SPBE Kementerian dan Pemilik Aset Informasi harus membatasi dan mengendalikan penggunaan hak akses khusus. Pengelolaan hak akses khusus harus mempertimbangkan:

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

d. Kajian Hak Akses Pengguna Kajian hak akses pengguna harus mempertimbangkan:
   1) Hak akses pengguna harus dikaji paling sedikit 6 (enam) bulan sekali atau setelah terjadi perubahan pada sistem, atau struktur Organisasi;
   2) Hak akses khusus harus dikaji paling sedikit 6 (enam) bulan sekali dalam jangka waktu lebih sering dibanding jangka waktu pengkajian hak akses pengguna, atau apabila terjadi perubahan pada sistem, atau struktur Organisasi;
   3) Pemeriksaan hak akses khusus harus dilakukan secara berkala, untuk memastikan pemberian hak akses khusus telah diotorisasi.

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

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

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

e) Mendapat persetujuan Pejabat yang berwenang/ atasan langsung pegawai.

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

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

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

b. Pengolahan Data pada Aplikasi

1) Pemeriksaan data masukan harus mempertimbangkan:

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

- Diluar rentang/batas nilai-nilai yang diperbolehkan;
- Karakter tidak valid dalam field data;
- Data hilang atau tidak lengkap;
- Melebihi batas atas dan bawah volume data; dan
- Data yang tidak diotorisasi dan tidak konsisten.

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

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

d) Menampilkan pesan yang sesuai dalam menanggapi kesalahan validasi;

e) Prosedur untuk menguji kewajaran dari data masukan;

f) Menguraikan tanggung jawab dari seluruh pegawai yang terkait dalam proses perekaman data; dan

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

2) Menyusun daftar pemeriksaan (*check list*) yang sesuai, mendokumentasikan proses pemeriksaan, dan menyimpan hasilnya secara aman. Proses pemeriksaan mencakup:
   a) Pengendalian sesi (*session*) atau tumpak (*batch*), untuk mencocokkan data setelah perubahan transaksi;
   b) Pengendalian saldo (*balancing*) untuk memeriksa data sebelum dan sesudah transaksi;
   c) Validasi data masukan yang dihasilkan sistem;
   d) Keutuhan dan keaslian data yang diunduh/ diunggah (*download/upload*);
   e) Hash tools dari rekaman (*record*) dan dokumen (*file*);
   f) Aplikasi berjalan sesuai dengan rencana dan waktu yang ditentukan;
   g) Program dijalankan dalam urutan yang benar dan menghentikan sementara jika terjadi kegagalan sampai masalah diatasi; dan
   h) Sistem mampu membuat dan mengeluarkan catatan aktivitas pengelolaan internal.
3) Pemeriksaan data keluaran harus mempertimbangkan:
   a) Kewajaran dari data keluaran yang dihasilkan;
   b) Pengendalian rekonsiliasi data untuk memastikan kebenaran pengolahan data;
   c) Menyediakan informasi yang cukup untuk pengguna atau sistem pengolahan informasi untuk menentukan akurasi, kelengkapan, ketepatan, dan klasifikasi informasi;
   d) Prosedur untuk menindaklanjuti validasi data keluaran;
   e) Menguraikan tanggung jawab dari seluruh pegawai yang terkait proses data keluaran; dan
   f) Sistem mampu membuat dan mengeluarkan catatan aktivitas dalam proses validasi data keluaran.

c. Pengendalian dan Penggunaan Kriptografi Pengembangan dan penerapan sistem kriptografi untuk perlindungan informasi harus mempertimbangkan:
   1) Kondisi dari suatu kegiatan yang menentukan bahwa informasi harus dilindungi, seperti risiko kegiatan, media pengiriman informasi, tingkat perlindungan yang dibutuhkan;
   2) Tingkat perlindungan yang dibutuhkan harus diidentifikasi berdasarkan penilaian risiko, antara lain jenis, kekuatan, dan kualitas dari algoritma enkripsi yang akan digunakan;
   3) Keperluan enkripsi untuk perlindungan informasi SANGAT RAHASIA, RAHASIA, dan TERBATAS yang melalui perangkat bergerak (*mobile computing*), media lepas pasang (*removable media*), atau jalur komunikasi;
   4) Pengelolaan kunci kriptografi (*kriptografi key*), seperti perlindungan kunci kriptografi (*kriptografi key*), pemulihan informasi ter-enkripsi dalam hal kehilangan atau kerusakan kunci kriptografi (*kriptografi key*); dan
   5) Dampak penggunaan informasi ter-enkripsi, seperti pengendalian terkait pemeriksaan suatu konten, kecepatan pemrosesan pada sistem.

d. Keamanan Dokumen (*File*) Sistem
   1) Pengembangan prosedur pengendalian piranti lunak pada sistem operasional harus mempertimbangkan:
      a) Proses pemutakhiran piranti lunak operasional, aplikasi, kumpulan program (*library program*) hanya boleh dilakukan oleh administrator sistem terlatih setelah melalui proses otorisasi;
      b) Sistem operasional hanya berisi program aplikasi yang dapat dieksekusi (*executable*) yang telah diotorisasi, tidak boleh berisi kode program (*source code*) atau penjalan kode program (*compiler*);

c) Aplikasi dan piranti lunak sistem operasi hanya dapat diimplementasikan setelah melewati proses pengujian yang ekstensif;
d) Sistem pengendalian konfigurasi harus digunakan untuk mengendalikan seluruh piranti lunak yang telah diimplementasikan beserta dokumentasi sistem;
e) Strategi *rollback* harus tersedia sebelum suatu perubahan diimplementasikan;
f) Catatan audit harus dipelihara untuk menjaga kemutakhiran catatan (*library*) program operasional;
g) Versi terdahulu dari suatu aplikasi harus tetap disimpan untuk keperluan kontinjensi; dan
h) Versi lama dari suatu piranti lunak harus diarsip, bersama dengan informasi terkait dan prosedur, parameter, konfigurasi rinci, dan piranti lunak pendukung.

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

3) Pengendalian akses ke kode program (*source code*) harus mempertimbangkan:
a) Kode program (*source code*) tidak boleh disimpan pada sistem operasional;
b) Pengelolaan kode program (*source code*) dan catatan (*library*) harus mengikuti prosedur yang telah ditetapkan;

c) Akses Unit Penyelenggara SPBE Kementerian terhadap kode program (*source code*) dan catatan (*library*);

d) Proses pemutakhiran kode program (*source code*) dan item terkait, serta pemberian kode program (*source code*) kepada programmer hanya dapat dilakukan setelah melalui proses otorisasi;

e) Daftar (*listing*) program harus disimpan dalam area aman (*secure areas*);

f) Catatan audit dari seluruh akses ke kode program (*source code*) *library* harus dipelihara; dan

g) Pemeliharaan dan penyalinan kode program (*source code*) library harus mengikuti prosedur pengendalian perubahan.

e. Keamanan dalam proses pengembangan dan pendukung (*support process*)

1) Prosedur pengendalian perubahan sistem operasi dan piranti lunak, mencakup:

a) Memelihara catatan persetujuan sesuai dengan kewenangannya;

b) Memastikan permintaan perubahan diajukan oleh pihak yang berwenang;

c) Melakukan kaji ulang (*review*) untuk memastikan bahwa tidak ada penurunan kualitas prosedur pengendalian dan integritas akibat permintaan perubahan;

d) Melakukan identifikasi terhadap piranti lunak, informasi, basis data, dan perangkat keras yang perlu diubah;

e) Mendapatkan persetujuan formal dari pihak yang berwenang sebelum pelaksanaan perubahan;

f) Memastikan pihak yang berwenang menerima perubahan yang diminta sebelum dilakukan implementasi;

g) Memastikan bahwa dokumentasi sistem mutakhir dan dokumen versi sebelumnya diarsip;

h) Memelihara versi perubahan aplikasi;

i) Memelihara jejak audit perubahan aplikasi;

j) Memastikan dokumentasi penggunaan dan prosedur telah diubah sesuai dengan perubahan yang dilaksanakan; dan

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

2) Prosedur kajian teknis aplikasi setelah perubahan sistem operasi dan/atau piranti lunak, mencakup:

a) Melakukan kaji ulang untuk memastikan bahwa tidak ada penurunan kualitas prosedur pengendalian dan integritas akibat permintaan perubahan;

b) Memastikan rencana dan anggaran yang mencakup kaji ulang dan pengujian sistem dari perubahan sistem operasi;

c) Memastikan pemberitahuan perubahan sistem informasi dilakukan dalam jangka waktu yang tepat untuk memastikan tes dan kaji ulang telah dilaksanakan sebelum implementasi; dan

d) Memastikan bahwa perubahan telah diselaraskan dengan rencana kelangsungan kegiatan.

3) Kebocoran informasi Pengendalian yang dapat diterapkan untuk membatasi risiko kebocoran informasi, antara lain:

a) Melakukan pemantauan terhadap sistem dan aktivitas pegawai dan pihak ketiga, sesuai dengan ketentuan yang berlaku; dan

b) Melakukan pemantauan terhadap aktivitas penggunaan komputer personal (*desktop*) dan perangkat bergerak (*mobile*).

4) Pengembangan piranti lunak oleh pihak ketiga harus mempertimbangkan:

a) Perjanjian lisensi, kepemilikan kode program (*source code*), dan Hak Atas Kekayaan Intelektual (HAKI);

b) Hak untuk melakukan audit terhadap kualitas dan akurasi pekerjaan;

c) Persyaratan kontrak mengenai kualitas dan fungsi keamanan aplikasi;

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

5) Pengelolaan Kerentanan Teknis, mencakup:

a) Penunjukan fungsi dan tanggung jawab yang terkait dengan pengelolaan kerentanan teknis termasuk di dalamnya pemantauan kerentanan, penilaian risiko kerentanan, patching, registrasi aset, dan koordinasi dengan pihak terkait;

b) Pengidentifikasian sumber informasi yang dapat digunakan untuk meningkatkan kepedulian terhadap kerentanan teknis;

c) Penentuan rentang waktu untuk melakukan aksi terhadap munculnya potensi kerentanan teknis. Apabila terjadi kerentanan teknis yang butuh penanganan maka harus diambil tindakan sesuai kontrol yang telah ditetapkan atau melaporkan kejadian tersebut melalui pelaporan kejadian dan kelemahan keamanan informasi;

d) Pengujian dan evaluasi penggunaan patch sebelum proses instalasi untuk memastikan patch dapat bekerja secara efektif dan tidak menimbulkan risiko yang lain. Apabila patch tidak tersedia, harus melakukan hal sebagai berikut:

- Mematikan layanan (*services*) yang berhubungan dengan kerentanan;
- Menambahkan pengendalian akses seperti firewall;
- Meningkatkan pengawasan untuk mengidentifikasi atau mencegah terjadinya serangan atau kejadian;
- Meningkatkan kepedulian terhadap kerentanan teknis;

e) Penyimpanan catatan audit (*audit log*) yang memuat prosedur dan langkah-langkah yang telah diambil;

f) Pemantauan dan evaluasi terhadap pengelolaan kerentanan teknis harus dilakukan secara berkala; dan

g) Pengelolaan kerentanan teknis diutamakan terhadap sistem informasi yang memiliki tingkat risiko tinggi.

9. Standar Pengendalian Pengelolaan Gangguan Keamanan Informasi
    a. Pelaporan Kejadian dan Kelemahan Keamanan Informasi
        1) Gangguan keamanan informasi antara lain:
            a) Hilangnya layanan, perangkat, atau fasilitas TIK;
            b) Kerusakan fungsi sistem atau kelebihan beban;
            c) Perubahan sistem di luar kendali;
            d) Kerusakan fungsi piranti lunak atau perangkat keras;
            e) Pelanggaran akses ke dalam sistem pengolah informasi TIK;
            f) Kelalaian manusia; dan
            g) Ketidaksesuaian dengan ketentuan yang berlaku.
        2) Pegawai dan pihak ketiga harus melaporkan kepada Unit Penyelenggara SPBE Kementerian dan Unit Kerja sesegera mungkin pada saat menemui kelemahan atau terjadi gangguan keamanan informasi dalam sistem atau layanan TIK Kementerian.
        3) Pelaporan gangguan harus mencakup:
            a) Proses umpan balik yang sesuai untuk memastikan bahwa pihak yang melaporkan kejadian keamanan informasi mendapatkan pemberitahuan penanganan masalah;
            b) Formulir laporan gangguan keamanan informasi untuk mendukung tindakan pelaporan dan membantu pelapor mengingat kronologis kejadian keamanan informasi;
            c) Perilaku yang benar dalam menghadapi gangguan keamanan informasi, antara lain:
                - Mencatat semua rincian penting gangguan dengan segera, seperti jenis pelanggaran, jenis kerusakan, pesan pada layar, atau anomali sistem; dan
                - Segera melaporkan gangguan ke pihak berwenang sebelum melakukan tindakan penanganan sendiri.
        4) Sebagai referensi yang digunakan dalam proses penanganan pelanggaran disiplin bagi pegawai dan pihak ketiga yang melakukan pelanggaran keamanan informasi.

b. Pengelolaan Gangguan Keamanan Informasi dan Perbaikannya

1) Unit Penyelenggara SPBE Kementerian dan Pemilik Aset Informasi masing-masing harus menyusun prosedur dan menguraikan tanggung jawab pegawai, terkait dalam rangka memastikan gangguan keamanan informasi dapat ditangani secara cepat dan efektif.

2) Prosedur pengelolaan gangguan keamanan informasi harus mempertimbangkan:

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

- Kegagalan sistem informasi dan hilangnya layanan;
- Serangan program yang membahayakan (*malicious code*);
- Serangan;
- Kesalahan akibat data tidak lengkap atau tidak akurat;
- Pelanggaran kerahasiaan dan keutuhan; dan
- Penyalahgunaan sistem informasi.

b) Untuk melengkapi rencana kontijensi, prosedur harus mencakup:

- Analisis dan identifikasi penyebab gangguan;
- Mengkarantina atau membatasi gangguan;
- Perencanaan dan pelaksanaan tindakan korektif untuk mencegah gangguan berulang;
- Komunikasi dengan pihak-pihak yang terkena dampak pemulihan gangguan; dan
- Pelaporan tindakan ke pihak berwenang.

c) Jejak audit dan bukti serupa harus dikumpulkan dan diamankan untuk:

- Analisis masalah internal;
- Digunakan sebagai bukti forensik yang berkaitan dengan potensi pelanggaran kontrak atau peraturan atau persyaratan dalam hal proses pidana atau perdata; dan

- Digunakan sebagai bahan tuntutan ganti rugi pada pihak ketiga yang menyediakan piranti lunak dan layanan.

d) Tindakan untuk memulihkan keamanan dari pelanggaran dan perbaikan kegagalan sistem harus dikendalikan secara hati-hati dan formal, prosedur harus memastikan bahwa:

- Hanya pegawai yang sudah diidentifikasi dan berwenang yang diizinkan akses langsung ke sistem dan data;
- Semua tindakan darurat yang diambil, didokumentasikan secara rinci;
- Tindakan darurat dilaporkan kepada pihak berwenang; dan
- Keutuhan sistem dan pengendaliannya dikonfirmasikan dengan pihak-pihak terkait sesegera mungkin.

3) Peningkatan penanganan gangguan keamanan informasi

a) Seluruh gangguan keamanan informasi yang terjadi dan tindakan mengatasinya harus dicatat dalam suatu basis data dan/atau buku catatan pelaporan gangguan keamanan informasi, dan akan menjadi masukan pada proses peningkatan penanganan gangguan keamanan informasi.

b) Seluruh catatan gangguan keamanan informasi akan dievaluasi dan dianalisis untuk perbaikan dan pencegahan agar gangguan keamanan informasi tidak terulang.

4) Pengumpulan Bukti Pelanggaran

Unit Penyelenggara SPBE Kementerian dan Pemilik Aset Informasi harus mengumpulkan, menyimpan, dan menyajikan bukti pelanggaran terhadap Kebijakan dan Standar Keamanan Informasi di Kementerian.

10. Standar Pengendalian Keamanan Informasi dalam Pengelolaan Kelangsungan Kegiatan

a. Pemilik Aset Informasi harus mengelola proses kelangsungan kegiatan pada saat keadaan darurat di Unit Kerja masing-masing.

b. Pemilik Aset Informasi harus mengidentifikasi risiko, dan menganalisis dampak yang diakibatkan pada saat terjadi keadaan darurat untuk menjamin kelangsungan kegiatan.
c. Pemilik Aset Informasi harus menyusun dan menerapkan Rencana Kelangsungan Kegiatan untuk menjaga dan mengembalikan kegiatan operasional dalam jangka waktu yang disepakati dan level yang dibutuhkan.
d. Pemilik Aset Informasi harus memelihara dan memastikan rencana-rencana yang termuat dalam Rencana Kelangsungan Kegiatan masih sesuai, dan mengidentifikasi prioritas untuk kegiatan uji coba.
e. Pemilik Aset Informasi harus melakukan uji coba Rencana Kelangsungan Kegiatan secara berkala untuk memastikan Rencana Kelangsungan Kegiatan dapat dilaksanakan secara efektif.
f. Pengelolaan Kelangsungan Kegiatan pada saat Keadaan Darurat Komponen yang harus diperhatikan dalam mengelola proses kelangsungan kegiatan:
    1) Identifikasi risiko dan analisis dampak yang diakibatkan pada saat terjadi keadaan darurat;
    2) Identifikasi seluruh aset informasi yang menunjang proses kegiatan kritikal;
    3) Identifikasi sumber daya, mencakup biaya, struktur Organisasi, teknis pelaksanaan, pegawai dan pihak ketiga;
    4) Memastikan keselamatan pegawai, dan perlindungan terhadap perangkat pengolah informasi dan aset Organisasi;
    5) Penyusunan dan pendokumentasian Rencana Kelangsungan Kegiatan sesuai dengan Rencana Strategi (Renstra) Kementerian; dan
    6) Pelaksanaan uji coba dan pemeliharaan Rencana Kelangsungan Kegiatan secara berkala.
g. Proses identifikasi risiko mengikuti ketentuan mengenai Penerapan Manajemen Risiko di Kementerian.
h. Proses analisis dampak kegiatan harus melibatkan pemilik proses bisnis dan dievaluasi secara berkala.

i. Penyusunan Rencana Kelangsungan Kegiatan mencakup:
   1) Prosedur saat keadaan darurat, mencakup tindakan yang harus dilakukan serta pengaturan hubungan dengan pihak berwenang;
   2) Prosedur fallback, mencakup tindakan yang harus diambil untuk memindahkan kegiatan kritikal atau layanan pendukung ke lokasi kerja sementara, dan mengembalikan operasional kegiatan kritikal dalam jangka waktu sesuai dengan standar ketersediaan data yang ditetapkan;
   3) Prosedur saat kondisi telah normal (*resumption*), adalah tindakan mengembalikan kegiatan operasional ke kondisi normal;
   4) Jadwal uji coba, mencakup langkah-langkah, dan waktu pelaksanaan uji coba serta proses pemeliharaannya;
   5) Pelaksanaan pelatihan dan sosialisasi dalam rangka meningkatkan kepedulian dan pemahaman proses kelangsungan kegiatan dan memastikan proses kelangsungan kegiatan dilaksanakan secara efektif;
   6) Tanggung jawab dan peran setiap Petugas Pelaksana Pengelolaan Proses Kelangsungan;
   7) Daftar kebutuhan aset informasi kritikal dan sumber daya untuk dapat menjalankan prosedur saat keadaan darurat, fallback, dan saat kondisi telah normal (*resumption*).

j. Uji Coba Rencana Kelangsungan Kegiatan harus dilaksanakan untuk memastikan setiap rencana yang disusun dapat dilakukan/dipenuhi pada saat penerapannya. Kegiatan uji coba Rencana Kelangsungan Kegiatan ini mencakup:
   1) Simulasi terutama untuk Pelaksana Pengelolaan Proses Kelangsungan Kegiatan;
   2) Uji coba pemulihan (*recovery*) sistem informasi untuk memastikan sistem informasi dapat berfungsi kembali;
   3) Uji coba proses pemulihan (*recovery*) di lokasi kerja sementara untuk menjalankan proses bisnis secara paralel;
   4) Uji coba terhadap perangkat dan layanan yang disediakan oleh pihak ketiga; dan

5) Uji coba keseluruhan mulai dari Organisasi, petugas, peralatan, perangkat, dan prosesnya.

11. Standar Pengendalian Kepatuhan

a. Kepatuhan terhadap Peraturan Perundangan yang terkait Keamanan Informasi

1) Seluruh pegawai dan pihak ketiga harus menaati peraturan perundangan yang terkait dengan keamanan informasi.

2) Unit Penyelenggara SPBE Kementerian dan Pemilik Aset Informasi harus mengidentifikasi, mendokumentasikan, dan memelihara kemutakhiran semua peraturan perundangan yang terkait dengan sistem keamanan informasi.

3) Hak Atas Kekayaan Intelektual Piranti lunak yang dikelola Unit Penyelenggara SPBE Kementerian dan Pemilik Aset Informasi harus mematuhi ketentuan penggunaan lisensi. Penggandaan piranti lunak secara tidak sah tidak diizinkan dan merupakan bentuk pelanggaran.

4) Perlindungan terhadap rekaman Rekaman milik Kementerian harus dilindungi dari kehilangan, kerusakan atau penyalahgunaan.

5) Pengamanan Data

Unit Penyelenggara SPBE Kementerian dan Pemilik Aset Informasi melindungi kepemilikan dan kerahasiaan data. Data hanya digunakan untuk kepentingan yang dibenarkan oleh peraturan perundangan dan kebijakan yang ditetapkan.

b. Kepatuhan Teknis

Unit Penyelenggara SPBE Kementerian dan Pemilik Aset Informasi harus melakukan pemeriksaan kepatuhan teknis secara berkala untuk menjamin efektivitas standar dan prosedur keamanan informasi yang ada di area operasional.

c. Kepatuhan terhadap Hak Kekayaan Intelektual

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

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

d. Kepatuhan terhadap Kebijakan dan Standar

Hal yang perlu dilakukan jika terdapat ketidakpatuhan teknis meliputi:

1) Menentukan dan mengevaluasi penyebab ketidakpatuhan;
2) Menentukan tindakan yang perlu dilakukan berdasarkan hasil evaluasi agar ketidakpatuhan tidak terulang kembali;
3) Menentukan dan melaksanakan tindakan perbaikan yang sesuai; dan
4) Mengkaji tindakan perbaikan yang dilakukan.

e. Kepatuhan Teknis

Sistem informasi harus diperiksa secara berkala untuk memastikan pengendalian perangkat keras dan piranti lunak telah diimplementasikan secara benar. Kepatuhan teknis juga mencakup pengujian penetrasi (*penetrating testing*) untuk mendeteksi

kerentanan dalam sistem, dan memeriksa pengendalian akses untuk mencegah kerentanan tersebut telah diterapkan.

9.6. Istilah yang Digunakan

1. Akun adalah identifikasi pengguna yang diberikan oleh unit Pengelola TIK, bersifat unik dan digunakan bersamaan dengan kata sandi ketika akan memasuki sistem TIK.
2. Akun khusus adalah akun yang diberikan oleh unit Pengelola TIK sesuai kebutuhan tetapi tidak terbatas pada pengelolaan TIK (baik berupa aplikasi atau sistem), dan kelompok kerja (baik berupa acara kedinasan, tim, atau unit kerja).
3. Aset fisik adalah jenis aset yang memiliki wujud fisik, misalnya perangkat komputer, perangkat jaringan dan komunikasi, media lepas pasang (*removable media*), dan perangkat pendukung lainnya.
4. Aset tak berwujud adalah jenis aset yang tidak memiliki wujud fisik, misalnya pengetahuan, pengalaman, keahlian, citra, dan reputasi. Aset ini mempunyai umur lebih dari satu tahun (aset tidak lancar) dan dapat diamortisasi selama periode pemanfaatannya, yang biasanya tidak lebih dari empat puluh tahun.
5. adalah sebuah tabung atau saluran untuk melindungi kabel yang biasanya terbuat dari baja.
6. Data adalah catatan atas kumpulan fakta yang mempunyai arti baik secara kualitatif maupun kuantitatif.
7. *Denial of service* adalah suatu kondisi di mana sistem tidak dapat memberikan layanan secara normal, yang disebabkan oleh suatu proses yang tidak terkendali baik dari dalam maupun dari luar sistem.
8. Direktori adalah hirarki atau *tree structure*.
9. Informasi adalah hasil pemrosesan, manipulasi, dan pengOrganisasian data yang dapat disajikan sebagai pengetahuan. Catatan: dalam penggunaannya, data dapat berupa informasi yang menjadi data baru, sebaliknya informasi dapat berfungsi sebagai data untuk menghasilkan informasi baru.
10. *Fallback* adalah suatu tindakan pembalikan/menarik diri dari posisi awal.

11. Fasilitas adalah sarana untuk melancarkan pelaksanaan fungsi atau mempermudah sesuatu.
12. Fasilitas utama adalah sarana utama gedung atau bangunan, seperti pusat kontrol listrik, CCTV.
13. Hak akses khusus adalah akses terhadap sistem informasi sensitif, termasuk di dalamnya dan tidak terbatas pada sistem operasi, perangkat penyimpanan (*storage devices*), dokumen pada server (*file server*), dan aplikasi-aplikasi sensitif, hanya diberikan kepada pengguna yang membutuhkan dan pemakaiannya terbatas dan dikontrol.
14. Hash totals adalah nilai pemeriksa kesalahan yang diturunkan dari penambahan satu himpunan bilangan yang diambil dari data (tidak harus berupa data numerik) yang diproses atau dimanipulasi dengan cara tertentu.
15. Jejak audit (*audit trails*) adalah urutan kronologis catatan audit yang berkaitan dengan pelaksanaan suatu kegiatan.
16. Kata sandi adalah serangkaian kode yang dibuat pengguna, bersifat rahasia dan pribadi yang digunakan bersamaan dengan Akun Pengguna.
17. Keamanan informasi adalah perlindungan aset informasi dari berbagai bentuk ancaman untuk memastikan kelangsungan kegiatan, menjamin kerahasiaan, keutuhan, dan ketersediaan aset informasi.
18. Koneksi eksternal (*remote access*) adalah suatu akses jaringan komunikasi dari luar organisasi ke dalam organisasi.
19. Kriptografi adalah ilmu yang mempelajari cara menyamarkan informasi dan mengubah kembali bentuk tersamar tersebut ke informasi awal untuk meningkatkan keamanan informasi. Dalam kriptografi terdapat dua konsep utama yakni enkripsi dan dekripsi.
20. Kode berbahaya (*malicious code*) adalah semua macam program yang membahayakan termasuk makro atau script yang dapat diesekusi dan dibuat dengan tujuan untuk merusak sistem komputer.
21. Cakram utama (*master disk*) adalah media yang digunakan sebagai sumber dalam melakukan instalasi piranti lunak.
22. Perangkat bergerak (*mobile computing*) adalah penggunaan perangkat komputasi yang dapat dipindah (*portabel*) misalnya komputer jinjing

(*notebook*) dan telepon selular untuk melakukan akses, pengolahan data dan penyimpanan.

23. Pemilik aset informasi adalah unit kerja yang memiliki kewenangan terhadap aset informasi.
24. Perangkat jaringan adalah peralatan jaringan komunikasi data seperti modem, hub, switch, router, dan lain-lain.
25. Piranti lunak adalah kumpulan beberapa perintah yang dieksekusi oleh mesin komputer dalam menjalankan pekerjaannya.
26. Perangkat pendukung adalah peralatan pendukung untuk menjamin beroperasinya perangkat keras dan perangkat jaringan serta untuk melindunginya dari kerusakan. Contoh perangkat pendukung adalah Uninterruptible Power Supply (UPS), pembangkit tenaga listrik/generator, antena komunikasi.
27. Perangkat pengolah informasi adalah setiap sistem pengolah informasi, layanan atau infrastruktur. Contoh perangkat pengolah informasi adalah komputer, faksimili, telepon, mesin fotocopy.
28. Perjanjian escrow adalah perjanjian dengan pihak ketiga atau pembuat aplikasi untuk memastikan apabila pihak ketiga tersebut tidak beroperasi/bangkrut (mengalami *failure*) maka Kementerian berhak untuk mendapatkan kode program (*source code*).
29. Perjanjian kerahasiaan adalah perikatan antara para pihak yang mencantumkan bahan rahasia, pengetahuan, atau informasi yang mana pihak-pihak ingin berbagi satu sama lain untuk tujuan tertentu, tetapi ingin membatasi akses dengan pihak lain.
30. Pihak berwenang adalah pihak yang mempunyai kewenangan terkait suatu hal, seperti kepolisian, instansi pemadam kebakaran, dan penyedia jasa telekomunikasi/internet.
31. Pihak ketiga adalah semua unsur di luar pengguna unit TIK Kementerian yang bukan bagian dari Kementerian, misal mitra kerja Kementerian (seperti: konsultan, penyedia jasa komunikasi, pemasok dan pemelihara perangkat pengolah informasi), dan kementerian/lembaga lain.
32. Proses pendukung (*support processes*) adalah proses-proses penunjang yang mendukung suatu proses utama yang terkait. Contoh proses

pendukung dalam pengembangan (*development*) adalah proses pengujian piranti lunak, proses perubahan piranti lunak.

33. Rencana Kontijensi adalah suatu rencana ke depan pada keadaan yang tidak menentu dengan skenario, tujuan, teknik, manajemen, pelaksanaan, serta sistem penanggulangannya telah ditentukan secara bersama untuk mencegah dan mengatasi keadaan darurat.
34. *Rollback* adalah sebuah mekanisme yang digunakan untuk mengembalikan sistem ke kondisi semula sebelum perubahan diimplementasikan. Mekanisme ini biasanya terdapat pada sistem basis data.
35. *Routing* adalah sebuah mekanisme yang digunakan untuk mengarahkan dan menentukan rute/jalur yang akan dilewati paket dari satu perangkat ke perangkat yang berada di jaringan lain.
36. Manajemen Keamanan Informasi adalah sistem manajemen yang meliputi kebijakan, organisasi, perencanaan, penangung jawab, proses, dan sumber daya yang mengacu pada pendekatan risiko bisnis untuk menetapkan, mengimplementasikan, mengoperasikan, memantau, mengevaluasi, mengelola, dan meningkatkan keamanan informasi.
37. Sanitasi (*sanitized*) adalah proses pembersihan data dan informasi sehingga tidak ada ada data dan informasi yang dapat diambil kembali dari perangkat keras tersebut.
38. Sistem informasi adalah serangkaian perangkat keras, piranti lunak, sumber daya manusia, serta prosedur dan/atau aturan yang diorganisasikan secara terpadu untuk mengolah data menjadi informasi yang berguna untuk rnencapai suatu tujuan.
39. Sistem TIK adalah sistem operasi, sistem surat elektronik, sistem aplikasi, sistem basis data, sistem jaringan intranet/internet, dan sebagainya.
40. Administrator sistem (*system administrator*) adalah akun khusus untuk mengelola sistem informasi.
41. Perangkat jarak jauh (*teleworking*) adalah penggunaan teknologi telekomunikasi untuk memungkinkan pegawai bekerja di suatu lokasi yang berada di luar kantor untuk mengakses jaringan internal kantor.

10. KEBIJAKAN INTERNAL PENYELENGGARA SPBE KEMENTERIAN

10.1. Dasar Hukum

1. Peraturan Presiden Republik Indonesia Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik;
2. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Republik Indonesia Nomor 59 Tahun 2020 tentang Pemantauan dan Evaluasi Sistem Pemerintahan Berbasis Elektronik;
3. Peraturan Menteri Komunikasi dan Informatika Nomor: 41/PER/MEN.KOMINFO/11/2007 tentang Panduan Umum Tata Kelola Informasi dan Komunikasi Nasional;
4. Peraturan Menteri Koordinator Bidang Perekonomian Nomor 9 Tahun 2020 Tentang Organisasi dan Tata Kerja Kementerian Koordinator Bidang Perekonomian;

10.2. Pendahuluan

Berdasarkan Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik instansi pusat dan pemerintah daerah wajib menerapkan kebijakan Sistem Pemerintahan Berbasis Elektronik (SPBE). Pasal 60 disebutkan bahwa Kementerian Koordinator Bidang Perekonomian perlu menunjuk koordinator SPBE yang bertugas melakukan koordinasi berkesinambungan terkait kebijakan SPBE di Kementerian Koordinator Bidang Perekonomian dengan Kementerian Pendayagunaan Aparatur Negara dan Reformasi Birokrasi. Untuk menunjang hal tersebut, perlu dibentuk penyelenggara SPBE Kementerian Koordinator Bidang Perekonomian yang bertujuan untuk mencapai penyelenggaraan SPBE yang efektif, efisien, dan berkesinambungan.

10.3. Definisi

Penyelenggara SPBE Kementerian Koordinator Bidang Perekonomian terdiri atas Tim Pengarah dan Tim Koordinasi.

10.4. Tim Pengarah SPBE Kementerian Koordinator Bidang Perekonomian

1. Keanggotaan tim pengarah SPBE Kementerian Koordinator Bidang Perekonomian terdiri atas:
   a. Ketua : Menteri Koordinator Bidang Perekonomian;
   b. Sekretaris : Sekretaris Kementerian;
   c. Anggota : Pejabat Pimpinan Tinggi Pratama di lingkungan Kementerian Koordinator Bidang Perekonomian.
2. Tim Pengarah SPBE Kementerian Koordinator Bidang Perekonomian mempunyai tugas memberikan arahan kebijakan dan penerapan SPBE Kementerian Koordinator Bidang Perekonomian.
3. Tim Pengarah SPBE Kementerian Koordinator Bidang Perekonomian menyelenggarakan fungsi :
   a. memfasilitasi perencanaan dan implementasi inisiatif program dan kegiatan SPBE;
   b. memfasilitasi penerapan tata kelola dan manajemen SPBE;
   c. memfasilitasi proses koordinasi, kerja sama, atau integrasi penerapan SPBE dengan pihak-pihak eksternal dalam dan luar negeri;
   d. melakukan perbaikan dan pengembangan atas hasil rekomendasi pemantauan dan evaluasi penerapan SPBE;
   e. mengatur pemantauan, penilaian, dan evaluasi kebijakan SPBE secara berkala terhadap perubahan peraturan perkembangan teknologi dan/atau kebutuhan Kementerian; dan
   f. mengatur pelaksanaan manajemen perubahan kebijakan SPBE.
4. Dalam melaksanakan tugasnya tim pengarah dapat mengikutsertakan pihak akademisi dan/atau Masyarakat Teknologi Informasi dan Komunikasi untuk menghasilkan birokrasi Kementerian Koordinator Bidang Perekonomian yang integratif, dinamis, transparan, dan inovatif, serta peningkatan kualitas pelayanan publik yang terpadu, efektif, responsif, dan adaptif.

10.5. Tim Koordinasi SPBE Kementerian Koordinator Bidang Perekonomian

1. Keanggotaan tim koordinasi SPBE Kementerian Koordinator Bidang Perekonomian terdiri atas :
   a. Koordinator : Sekretaris Kementerian Koordinator Bidang Perekonomian;
   b. Ketua I : Pejabat Pimpinan Tinggi Madya pada satuan kerja yang menyelenggarakan tugas dan fungsi di bidang teknologi informasi dan komunikasi;
   c. Ketua II : Pejabat Pimpinan Tinggi Madya pada satuan kerja yang menyelenggarakan tugas dan fungsi di bidang tata laksana;
   d. Kelompok Kerja : Pejabat/Pegawai pada satuan kerja yang menyelenggarakan layanan SPBE dan Pejabat/Pegawai pada satuan kerja lainnya apabila diperlukan.
2. Anggota Kelompok Kerja berasal dari satuan kerja yang menyelenggarakan tugas dan fungsi di bidang layanan administrasi pemerintahan berbasis elektronik dan/atau menyelenggarakan tugas dan fungsi di bidang layanan publik berbasis elektronik.
3. Tim koordinasi SPBE mempunyai tugas:
   a. mengarahkan, memantau, dan mengevaluasi pelaksanaan SPBE; dan
   b. melakukan koordinasi dengan tim koordinasi SPBE Nasional untuk pelaksanaan SPBE yang melibatkan lintas instansi Pusat dan Pemerintah Daerah.

11. KEBIJAKAN INTERNAL MANAJEMEN SPBE

11.1. Dasar Hukum

1. Peraturan Presiden Republik Indonesia Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik;
2. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Republik Indonesia Nomor 59 Tahun 2020 tentang Pemantauan dan Evaluasi Sistem Pemerintahan Berbasis Elektronik;

3. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Republik Indonesia Nomor 5 Tahun 2020 tentang Pedoman Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik.
4. Peraturan Menteri Perencanaan Pembangunan Nasional/Kepala Badan Perencanaan Pembangunan Nasional Republik Indonesia Nomor 16 Tahun 2020 tentang Manajemen Data Sistem Pemerintahan Berbasis Elektronik;
5. Peraturan Presiden Nomor 39 Tahun 2019 tentang Satu Data Indonesia.

11.2. Pendahuluan

Berdasarkan Peraturan Presiden Republik Indonesia Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik instansi pusat dan pemerintah daerah wajib menerapkan kebijakan Sistem Pemerintahan Berbasis Elektronik (SPBE) dan sesuai dengan Pasal 46 dijelaskan bahwa instansi pusat dan pemerintah daerah melaksanakan Manajemen Sistem Pemerintahan Berbasis Elektronik (SPBE).

11.3. Definisi

Manajemen SPBE adalah serangkaian proses untuk mencapai penerapan SPBE yang efektif, efisiem dan berkesinambungan, serta layanan SPBE yang berkualitas.

11.4. Manajemen SPBE

Serangkaian proses sebagaimana yang dimaksud pada poin 11.3 dapat dijelaskan sebagai berikut:

1. Manajemen Risiko

   Manajemen Risiko SPBE adalah pendekatan sistematis yang meliputi proses, pengukuran, struktur, dan budaya untuk menentukan tindakan terbaik terkait Risiko SPBE. Permasalahan penerapan SPBE dan tren revolusi TIK 4.0 melahirkan sejumlah risiko yang dapat berpengaruh terhadap pencapaian tujuan SPBE. Manajemen risiko bertujuan menjamin keberlangsungan SPBE dengan meminimalkan dampak risiko dalam SPBE melalui proses:

   a. Identifikasi;

   b. Analisis;

c. Pengendalian;

d. Pemantauan dan Evaluasi terhadap Risiko dalam SPBE.

2. Manajemen Keamanan Informasi

Keamanan Informasi adalah terjaganya kerahasiaan (*confidentiality*), keutuhan (*integrity*), ketersediaan (*availability*), keaslian, dan kenirsangkalan (*non-repudiation*) informasi. Manajemen keamanan informasi bertujuan untuk menjamin keberlangsungan SPBE dengan meminimalkan dampak risiko keamanan informasi melalui proses sebagai berikut:

a. Penetapan ruang lingkup;

b. Penetapan penanggung jawab;

c. Perencanaan;

d. Dukungan pengoperasian;

e. Evaluasi kinerja; dan

f. Perbaikan berkelanjutan terhadap keamanan informasi dalam SPBE.

3. Manajemen Data

Manajemen Data adalah proses pengelolaan data mencakup perencanaan, pengumpulan, pemeriksaan dan penyebarluasan yang dilakukan secara efektif dan efisien sehingga diperoleh data yang akurat, mutakhir, dan terintegrasi. Penerapan Manajemen Data SPBE dilakukan untuk menjamin terwujudnya data yang akurat, mutakhir, terintegrasi, dan dapat diakses sebagai dasar perencanaan, pelaksanaan, evaluasi dan pengendalian pembangunan nasional. Manajemen SPBE sebagaimana yang dimaksud dilaksanakan dengan sasaran agar Instansi Pusat dan Pemerintahan Daerah mampu mencapai hal-hal sebagai berikut:

a. Mampu memahami kebutuhan data;

b. Mendapatkan, menyimpan, melindungi dan memastikan integritas data;

c. Meningkatkan kualitas data secara terus menerus; dan

d. Memaksimalkan penggunaan data dan hasil yang efektif dari penggunaan data.

Manajemen Data SPBE dilaksanakan melalui serangkaian proses pengelolaan, dijelaskan sebagai berikut;

a. Pengelolaan Arsitektur Data;
b. Data Induk dan Data Referensi;
c. Basis Data; dan
d. Kualitas Data.

4. Manajemen Aset Teknologi Informasi dan Komunikasi

Manajemen aset teknologi informasi dan komunikasi bertujuan untuk menjamin ketersediaan dan optimalisasi pemanfaatan aset teknologi informasi dan komunikasi dalam SPBE melalui proses:

a. Perencanaan;
b. Pengadaan;
c. pengelolaan; dan
d. penghapusan perangkat keras dan perangkat lunak yang digunakan dalam SPBE.

5. Manajemen Sumber Daya Manusia

Manajemen sumber daya manusia bertujuan untuk menjamin keberlangsungan dan peningkatan mutu layanan dalam SPBE melalui proses:

a. Perencanaan;
b. Pengembangan;
c. Pembinaan, dan pendayagunaan sumber daya manusia dalam SPBE.

Manajemen sumber daya manusia memastikan ketersediaan dan kompetensi sumber daya manusia untuk pelaksanaan Tata Kelola SPBE dan Manajemen SPBE. Dimana setiap pegawai Kementerian wajib memiliki kompetensi dasar di bidang teknologi informasi dan komunikasi yang dapat diperoleh melalui pelatihan dasar-dasar teknologi informasi dan komunikasi.

Unit Penyelenggara SPBE Kementerian dan seluruh Unit Kerja di lingkungan Kementerian yang memiliki layanan mandiri wajib

menyediakan sumber daya manusia sesuai dengan ketentuan peraturan perundang-undangan.

Unit kerja yang membidangi fungsi di bidang kepegawaian melalui koordinasi dengan Unit Penyelenggara SPBE Kementerian melakukan pengembangan budaya kerja, pemberdayaan, dan peningkatan kompetensi sumber daya manusia di bidang teknologi informasi dan komunikasi.

6. Manajemen Pengetahuan

   Manajemen pengetahuan bertujuan untuk meningkatkan kualitas Layanan SPBE dan mendukung proses pengambilan keputusan dalam SPBE melalui proses:

   a. pengumpulan;
   b. pengolahan;
   c. penyimpanan;
   d. penggunaan dan
   e. alih pengetahuan dan teknologi yang dihasilkan dalam SPBE.

7. Manajemen Perubahan

   Manajemen perubahan bertujuan untuk menjamin keberlangsungan dan meningkatkan kualitas Layanan SPBE melalui pengendalian perubahan yang terjadi dalam SPBE melalui proses:

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

8. Manajemen Layanan SPBE

   Manajemen Layanan SPBE bertujuan untuk menjamin keberlangsungan dan meningkatkan kualitas layanan SPBE kepada Pengguna SPBE melalui proses berikut:

a. Pelayanan Pengguna SPBE

Merupakan kegiatan pelayanan terhadap keluhan, gangguan, masalah, permintaan, dan perubahan Layanan SPBE dari Pengguna SPBE.

b. Pengoperasian Layanan SPBE

Merupakan kegiatan pendayagunaan dan pemeliharaan Infrastruktur SPBE dan Aplikasi SPBE.

c. Pengelolaan Aplikasi SPBE

Merupakan kegiatan pembangunan dan pengembangan aplikasi yang berpedoman pada metodologi pembangunan dan pengembangan Aplikasi SPBE.

12. KEBIJAKAN INTERNAL AUDIT TEKNOLOGI INFORMASI DAN KOMUNIKASI

12.1. Tujuan

Dalam rangka memastikan keandalan dan keamanan teknologi informasi dan komunikasi di Lingkungan Kementerian Koordinator Bidang Perekonomian dilakukan audit teknologi informasi dan komunikasi secara berkala.

12.2. Ruang Lingkup

Audit teknologi informasi dan komunikasi terdiri atas:

1. Audit infrastruktur SPBE Kementerian Koordinator Bidang Perekonomian;
2. Audit aplikasi SBPE Kementerian Koordinator Bidang Perekonomian; dan
3. Audit keamanan SPBE Kementerian Koordinator Bidang Perekonomian.

12.3. Standar

Audit teknologi informasi dan komunikasi dilakukan dengan melakukan pemeriksaan hal pokok teknis pada:

1. Penerapan tata kelola dan manajemen teknologi informasi dan komunikasi;
2. Fungsionalitas teknologi informasi dan komunikasi;
3. Kinerja teknologi informasi dan komunikasi yang dihasilkan; dan
4. Aspek teknologi informasi dan komunikasi lainnya.

Audit teknologi informasi dan komunikasi dilaksanakan oleh unit kerja yang memiliki tugas dan fungsi penyelenggaraan audit internal Kementerian dan/atau lembaga pelaksana audit teknologi informasi dan komunikasi pemerintah dan/atau lembaga pelaksana audit teknologi informasi dan komunikasi yang terakreditasi sesuai dengan ketentuan peraturan perundang-undangan.

12.4. Ketentuan Pelaksanaan Audit Teknologi Informasi dan Komunikasi

1. Pengendalian Audit

   Unit Penyelenggara SPBE Kementerian dan Unit Kerja bersama dengan Unit Kerja yang memiliki tugas dan fungsi penyelenggaraan audit internal Kementerian membuat perencanaan persyaratan, ruang lingkup, dan kegiatan audit yang melibatkan pemeriksaan sistem operasional untuk mengurangi kemungkinan risiko gangguan yang dapat terjadi terhadap penyelenggaraan layanan SPBE Kementerian selama proses audit.
2. Perlindungan Terhadap Alat Bantu (*tools*) Audit

   Penggunaan alat bantu (baik piranti lunak maupun perangkat keras) untuk mengetahui kelemahan keamanan, memindai (*scanning*) kata sandi, atau untuk melemahkan dan menerobos sistem keamanan inforrnasi tidak diizinkan kecuali atas persetujuan Pimpinan Unit Penyelenggara SPBE Kementerian.
3. Proses audit sistem informasi harus memperhatikan hal berikut :
   a. Persyaratan audit harus disetujui oleh Pimpinan Unit Penyelenggara SPBE Kementerian dan Pemilik Aset Informasi;
   b. Ruang lingkup pemeriksaan/audit harus disetujui dan dikendalikan oleh Pimpinan Unit Penyelenggara SPBE Kementerian dan Pemilik Aset Informasi;
   c. Pemeriksaan piranti lunak dan data harus dibatasi untuk akses baca saja (*read-only*);
   d. Selain akses baca saja hanya diizinkan untuk salinan dari dokumen (*file*) sistem yang diisolasi, yang harus dihapus bila audit telah selesai, atau diberikan perlindungan yang tepat jika ada kewajiban

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

e. Sumber daya untuk melakukan pemeriksaan harus secara jelas diidentifikasi dan tersedia;

f. Persyaratan untuk pengolahan khusus atau tambahan harus diidentifikasi dan disepakati;

g. Semua akses harus dipantau dan dicatat untuk menghasilkan jejak audit, dan untuk data dan sistem informasi sensitif harus mempertimbangkan pencatatan waktu (*timestamp*) pada jejak audit;

h. Semua prosedur, persyaratan, dan tanggung jawab harus didokumentasikan; dan

i. Auditor harus independen dari kegiatan yang diaudit.

13. KEBIJAKAN INTERNAL INFRASTRUKTUR PENDUKUNG SPBE

13.1. Tujuan

Penggunaan Infrastruktur Pendukung SPBE Kementerian Koordinator Bidang Perekonomian bertujuan untuk meningkatkan meningkatkan efisiensi, keamanan, dan kemudahan integrasi dalam rangka memenuhi kebutuhan Infrastruktur Pendukung SPBE internal Kementerian Koordinator Bidang Perekonomian, dan penggunaan tersebut dilakukan secara berbagi pakai.

13.2. Ruang Lingkup

Infrastruktur Pendukung SPBE Kementerian terdiri atas:

1. Jaringan Intra Kementerian Koordinator Bidang Perekonomian; dan
2. Sistem Penghubung Layanan Kementerian Koordinator Bidang Perekonomian.

13.3. Definisi

1. Jaringan Intra Kementerian Koordinator Bidang Perekonomian adalah jaringan tertutup yang menghubungkan antar simpul jaringan unit kerja di lingkungan Kementerian Koordinator Bidang Perekonomian;

2. Sistem Penghubung Layanan Kementerian Koordinator Bidang Perekonomian adalah perangkat intergrasi/ penghubung untuk melakukan pertukaran data antar Layanan SPBE Kementerian.

13.4. Standar

1. Infrastruktur pendukung SPBE Kementerian diselenggarakan oleh Unit Penyelenggara SPBE Kementerian;
2. Pembangunan dan pengembangan infrastruktur pendukung SPBE Kementerian dilakukan selaras dengan Rencana Induk Teknologi Informasi dan Komunikasi Kementerian Koordinator Bidang Perekonomian;
3. Infrastruktur pendukung SPBE Kementerian sesuai dengan standar perangkat, standar interoperabilitas, standar keamanan sistem informasi, dan standar lainnya berdasarkan ketentuan peraturan perundang-undangan;
4. Penggunaan infrastruktur pendukung SPBE Kementerian dilakukan secara berbagi pakai di lingkungan Kementerian.