MENTERI PEKERJAAN UMUM DAN PERUMAHAN RAKYAT
REPUBLIK INDONESIA

PERATURAN MENTERI PEKERJAAN UMUM DAN PERUMAHAN RAKYAT
REPUBLIK INDONESIA
NOMOR: 17/PRT/M/2016
TENTANG
PENYELENGGARAAN TEKNOLOGI INFORMASI DAN KOMUNIKASI
DI KEMENTERIAN PEKERJAAN UMUM DAN PERUMAHAN RAKYAT

DENGAN RAHMAT TUHAN YANG MAHA ESA

MENTERI PEKERJAAN UMUM DAN PERUMAHAN RAKYAT
REPUBLIK INDONESIA,

Menimbang :

a. bahwa kemajuan teknologi informasi dan komunikasi yang sangat pesat memberi peluang pengelolaan data dan informasi yang cepat dan akurat sehingga perlu dimanfaatkan oleh Kementerian dalam melaksanakan tugas dan fungsinya dalam memberikan pelayanan kepada masyarakat;
b. bahwa penyelenggaraan teknologi informasi dan komunikasi di Kementerian (*e-Government*) perlu kesamaan pemahaman, keserempakan tindak, dan keterpaduan langkah dari seluruh unit organisasi untuk mewujudkan tata kelola pemerintahan yang baik dalam meningkatkan layanan publik yang efektif dan efisien;
c. bahwa berdasarkan pertimbangan sebagaimana dimaksud dalam huruf a dan huruf b, perlu menetapkan Peraturan Menteri tentang penyelenggaraan teknologi informasi dan

komunikasi di Kementerian Pekerjaan Umum dan Perumahan Rakyat.;

Mengingat : 1. Peraturan Pemerintah Nomor 61 Tahun 2010 tentang Pelaksanaan Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik (Lembaran Negara Republik Indonesia Tahun 2010 Nomor 99, Tambahan Lembaran Negara Republik Indonesia Nomor 5149);
2. Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik Indonesia Tahun 2012 Nomor 189, Tambahan Lembaran Negara Republik Indonesia Nomor 5348);
3. Peraturan Presiden Nomor 15 Tahun 2015 tentang Kementerian Pekerjaan Umum dan Perumahan Rakyat (Lembaran Negara Republik Indonesia Tahun 2015 Nomor 16);
4. Peraturan Menteri Komunikasi dan Informatika Nomor 41/PER/ MEN.KOMINFO/11/2007 tentang Panduan Umum Tata Kelola Teknologi Informasi dan Komunikasi Nasional;
5. Peraturan Menteri Komunikasi dan Informatika Nomor 23 Tahun 2013 tentang Pengelolaan Nama Domain (Berita Negara Republik Indonesia Tahun 2013 Nomor 1235);
6. Peraturan Menteri Pekerjaan Umum Nomor 15 Tahun 2015 tentang Organisasi dan Tata Kerja Kementerian Pekerjaan Umum dan Perumahan Rakyat (Berita Negara Republik Indonesia Tahun 2015 Nomor 881);

MEMUTUSKAN:

Menetapkan : PERATURAN MENTERI PEKERJAAN UMUM DAN PERUMAHAN RAKYAT TENTANG PENYELENGGARAAN TEKNOLOGI INFORMASI DAN KOMUNIKASI DI KEMENTERIAN PEKERJAAN UMUM DAN PERUMAHAN RAKYAT.

BAB I

KETENTUAN UMUM

Pasal 1

Dalam Peraturan Menteri ini yang dimaksud dengan:

1. Penyelenggaraan teknologi informasi dan komunikasi di Kementerian Pekerjaan Umum dan Perumahan Rakyat yang selanjutnya disebut sebagai *e-Government* adalah pemanfaatan teknologi informasi dan komunikasi dalam proses pemerintahan.
2. Sistem informasi adalah kesatuan komponen yang terdiri atas lembaga, sumber daya manusia, perangkat keras, perangkat lunak, substansi data dan informasi yang terkait satu sama lain dalam satu mekanisme kerja untuk mengelola data dan informasi.
3. Teknologi informasi dan komunikasi adalah suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan/atau menyebarluaskan informasi.
4. Data adalah kumpulan fakta berupa angka, huruf, gambar, suara, peta, atau citra tentang karakteristik atau ciri-ciri suatu objek.
5. Informasi adalah gabungan, rangkaian dan analisis data yang berbentuk angka, huruf, gambar, suara, peta, atau citra yang telah diolah, yang mempunyai arti, nilai dan makna tertentu.
6. Infrastruktur teknologi informasi dan komunikasi adalah perangkat keras, piranti lunak sistem operasi dan aplikasi, data center serta fasilitas pendukung lainnya, untuk mendukung penyelenggaraan *e-Government*.
7. Data center adalah suatu fasilitas yang digunakan untuk menempatkan sistem komputer dan komponen terkaitnya, seperti sistem telekomunikasi dan sistem repositori.
8. Aplikasi adalah komponen sistem informasi yang digunakan untuk menjalankan fungsi, proses dan

mekanisme kerja yang mendukung pelaksanaan *e-Government.*

9. Aplikasi umum adalah aplikasi *e-Government* yang dapat digunakan oleh seluruh unit organisasi di Kementerian.
10. Aplikasi khusus adalah aplikasi *e-Government* yang digunakan untuk memenuhi kebutuhan unit organisasi tertentu sesuai dengan tugas dan fungsinya.
11. Sumber daya informatika adalah sumber daya dalam bentuk perangkat keras, piranti lunak, dan sumber daya manusia yang terkait dengan teknologi informasi dan komunikasi.
12. Cetak biru *(blue print)* adalah dokumen perencanaan yang menjadi acuan penyelenggaraan *e-Government*.
13. Portal web adalah kumpulan situs web yang berisi informasi elektronik yang dapat diakses publik.
14. Situs web adalah kumpulan halaman web yang berisi topik yang saling terkait berupa informasi elektronik yang dapat diakses publik.
15. Interoperabilitas adalah kemampuan dua sistem atau dua komponen atau lebih untuk bertukar informasi dan untuk menggunakan informasi yang telah dipertukarkan.
16. Nama Domain adalah alamat internet penyelenggara negara, orang, badan usaha, dan/atau masyarakat, yang dapat digunakan dalam berkomunikasi melalui internet, yang berupa kode atau susunan karakter yang bersifat unik untuk menunjukkan lokasi tertentu dalam internet.
17. Hak cipta adalah hak eksklusif pencipta yang timbul secara otomatis berdasarkan prinsip deklaratif setelah suatu ciptaan diwujudkan dalam bentuk nyata tanpa mengurangi pembatasan sesuai dengan ketentuan peraturan perundang-undangan.
18. Akses adalah kegiatan melakukan interaksi dengan sistem elektronik yang berdiri sendiri atau dalam jaringan.
19. Badan Usaha adalah perusahaan perseorangan atau perusahaan persekutuan, baik yang berbadan hukum maupun yang tidak berbadan hukum.

20. Repositori adalah sistem pengkoleksian berkas siap pakai dan siap cetak dari berbagai macam sistem informasi dari berbagai unit kerja sehingga dapat diproses menjadi suatu informasi turunan atau agregat secara terintegrasi.
21. Pusat Data dan Teknologi Informasi yang selanjutnya disebut Pusdatin adalah unit kerja di Kementerian yang mempunyai tugas melaksanakan pembinaan, pengembangan, pengelolaan dan penyediaan data infrastruktur bidang pekerjaan umum dan perumahan rakyat serta penyelenggaraan sistem informasi dalam rangka mendukung manajemen Kementerian.
22. Kementerian adalah Kementerian Pekerjaan Umum dan Perumahan Rakyat.
23. Menteri adalah Menteri Pekerjaan Umum dan Perumahan Rakyat.

Pasal 2

(1) Peraturan Menteri ini dimaksudkan sebagai pedoman penyelenggaraan *e-Government* Kementerian.
(2) Peraturan Menteri ini bertujuan untuk mencapai tata kelola pemerintahan yang baik melalui penerapan *e-Government* Kementerian.

Pasal 3

Lingkup pengaturan dalam Peraturan Menteri ini meliputi:
a. infrastruktur teknologi informasi dan komunikasi;
b. nama domain Kementerian;
c. aplikasi;
d. data dan informasi;
e. portal *web* Kementerian;
f. surat elektronik (*e-mail*) Kementerian;
g. tata kelola; dan
h. evaluasi.

BAB II

INFRASTRUKTUR TEKNOLOGI INFORMASI DAN KOMUNIKASI

Pasal 4

(1) Infrastruktur teknologi informasi dan komunikasi yang digunakan dalam *e-Government* harus sesuai dengan standar teknologi, interoperabilitas, dan keamanan informasi.
(2) Ketentuan standar teknologi sebagaimana dimaksud pada ayat (1) harus memperhatikan teknologi yang terbuka, mudah diperoleh di pasaran, mudah memperoleh dukungan ketika dibutuhkan, dan mudah dikembangkan (*scalable*).
(3) Ketentuan standar interoperabilitas sebagaimana dimaksud pada ayat (1) mengacu pada standardisasi format data yang akan dipertukarkan untuk mempermudah dalam hal pengelolaan, pengaksesan data, berbagi data dalam rangka memberikan pelayanan informasi yang lebih efektif dan efisien.
(4) Ketentuan standar keamanan informasi sebagaimana dimaksud pada ayat (1) tercantum dalam lampiran I yang merupakan bagian tidak terpisahkan dari Peraturan Menteri ini.

Pasal 5

(1) Kementerian menyediakan fasilitas berupa *data center* dalam penyelenggaraan *e-Government*.
(2) Data center sebagaimana dimaksud pada ayat (1) dikelola oleh Pusdatin.
(3) Ketentuan *data center* sebagaimana dimaksud pada ayat (1) tercantum dalam lampiran II yang merupakan bagian tidak terpisahkan dari Peraturan Menteri ini.

BAB III

NAMA DOMAIN DAN SUBDOMAIN KEMENTERIAN

Pasal 6

(1) Nama domain resmi Kementerian adalah pu.go.id.
(2) Penanggung jawab domain Kementerian adalah Pusdatin.
(3) Nama subdomain dapat digunakan oleh Unit Organisasi dan Unit Kerja di Kementerian serta aplikasi berbasis *web*.
(4) Penggunaan nama subdomain dikoordinasikan oleh Pusdatin.
(5) Penanggung jawab subdomain adalah Unit Organisasi atau Unit Kerja di Kementerian yang mengajukan dan menggunakan nama subdomain.
(6) Penanggung jawab subdomain harus melakukan evaluasi pemanfaatan subdomain untuk memastikan keberlangsungan *website*, aplikasi atau kegiatan yang menggunakan subdomain.
(7) Ketentuan nama domain dan sub domain sebagaimana dimaksud pada ayat (1) dan (2) tercantum dalam lampiran III yang merupakan bagian tidak terpisahkan dari Peraturan Menteri ini.

BAB IV

APLIKASI

Pasal 7

(1) Aplikasi *e-Government* terdiri atas aplikasi umum dan aplikasi khusus.
(2) Aplikasi *e-Government* sebagaimana dimaksud pada ayat (1) harus dilengkapi dengan:
    a. kode program;
    b. basis data; dan
    c. dokumentasi.
(3) Dokumentasi sebagaimana dimaksud pada ayat (2) huruf c sekurang-kurangnya terdiri atas identifikasi kebutuhan, desain aplikasi, penjelasan kode program, prosedur standar manual, penjelasan basis data, hak akses, dan kebutuhan sumber daya informatika.

Pasal 8

(1) Aplikasi *e-Government* harus memenuhi standar pengembangan, interoperabilitas, dan standar keamanan informasi.
(2) Penyelenggara aplikasi pada unit organisasi Kementerian wajib berkoordinasi dengan Pusdatin dalam perencanaan dan pengembangan aplikasi.
(3) Hak cipta atas aplikasi dan kelengkapannya sebagaimana dimaksud dalam Pasal 7 ayat (1) yang dibangun oleh mitra kerja menjadi milik Kementerian.
(4) Aplikasi sebagaimana dimaksud pada ayat (1) yang berbasis *web* harus dipasang pada *data center* Kementerian.
(5) Ketentuan standar pengembangan aplikasi sebagaimana dimaksud pada ayat (1) tercantum dalam lampiran IV yang merupakan bagian tidak terpisahkan dari Peraturan Menteri ini.

Pasal 9

(1) Nama domain aplikasi umum sebagaimana dimaksud dalam Pasal 7 ayat (1) yang berbasis *web* menggunakan nama domain sebagaimana dimaksud dalam Pasal 6 ayat (1) diletakkan di depan nama domain Kementerian menjadi nama sub domain.
(2) Ketentuan nama domain aplikasi sebagaimana dimaksud pada ayat (1) mengikuti ketentuan dalam pasal 6 Peraturan Menteri ini.

BAB V

DATA DAN INFORMASI

Pasal 10

(1) Data dan informasi dalam penyelenggaraan *e-Government* wajib disediakan oleh masing-masing unit organisasi Kementerian.

(2) Data dan informasi sebagaimana dimaksud pada ayat (1) harus memenuhi kaidah struktur data, interoperabilitas, kebaruan, keakuratan, kerahasiaan, dan keamanan informasi.
(3) Data dan informasi sebagaimana dimaksud pada ayat (1) dikelola dan dikumpulkan oleh unit organisasi dan Pusdatin.
(4) Data dan informasi sebagaimana dimaksud pada ayat (1) dapat dimanfaatkan oleh seluruh unit organisasi.

Pasal 11

(1) Data dan informasi sebagaimana dimaksud dalam Pasal 10 ayat (1) merupakan hak cipta Kementerian.
(2) Data dan informasi sebagaimana dimaksud dalam Pasal 10 ayat (1) harus disimpan pada *data center* Kementerian.
(3) Pemanfaatan data dan informasi sebagaimana dimaksud dalam Pasal 10 ayat (1) harus berkoordinasi dengan Pusdatin.
(4) Pemanfaatan data dan informasi selain oleh unit organisasi sebagaimana dimaksud dalam Pasal 10 ayat (4) harus berkoordinasi dengan Pejabat Pengelola Informasi dan Dokumentasi (PPID) Kementerian.

BAB VI

PORTAL *WEB* KEMENTERIAN

Pasal 12

(1) Portal *web* resmi Kementerian dikelola oleh Pusdatin.
(2) Nama domain portal *web* resmi Kementerian adalah www.pu.go.id.
(3) Situs *web* unit organisasi dikelola oleh unit organisasi masing-masing.
(4) Nama domain situs *web* unit organisasi di Kementerian yang menggunakan nama domain sebagaimana dimaksud pada ayat (1) diletakkan di depan nama domain Kementerian menjadi nama sub domain.

(5) Ketentuan portal *web* sebagaimana dimaksud pada ayat (1) tercantum dalam lampiran V yang merupakan bagian tidak terpisahkan dari Peraturan Menteri ini.

(6) Ketentuan tata kelola portal *web* sebagaimana dimaksud pada ayat (1) tercantum dalam lampiran VI yang merupakan bagian tidak terpisahkan dari Peraturan Menteri ini.

Pasal 13

(1) Portal *web* Kementerian sebagaimana dimaksud dalam Pasal 12 ayat (1) dilaksanakan oleh masing-masing unit organisasi:
   a. Sekretariat Jenderal untuk informasi pengelolaan anggaran, peraturan perundang-undangan, kepegawaian, aset, berita, saran pengaduan, dan layanan informasi publik;
   b. Direktorat Jenderal Sumber Daya Air untuk informasi pengelolaan sumber daya air;
   c. Direktorat Jenderal Bina Marga untuk informasi jalan, jembatan, dan jalan tol;
   d. Direktorat Jenderal Cipta Karya untuk informasi pengembangan infrastruktur permukiman;
   e. Direktorat Jenderal Penyediaan Perumahan untuk informasi penyediaan perumahan;
   f. Direktorat Jenderal Bina Konstruksi untuk informasi jasa konstruksi;
   g. Direktorat Jenderal Pembiayaan Perumahan untuk informasi pembiayaan perumahan;
   h. Inspektorat Jenderal untuk informasi pengawasan;
   i. Badan Pengembangan Infrastruktur Wilayah untuk informasi pengembangan infrastruktur wilayah;
   j. Badan Penelitian dan Pengembangan untuk informasi penelitian dan pengembangan;
   k. Badan Pengembangan Sumber Daya Manusia untuk informasi pengembangan sumber daya manusia.

(2) Dalam mengembangkan situs *web*, unit organisasi harus berkoordinasi dengan Pusdatin.

BAB VII

SURAT ELEKTRONIK (*e-Mail*)

Pasal 14

(1) Alamat surat elektronik resmi Kementerian menggunakan nama domain mail.pu.go.id.
(2) Akun surat elektronik resmi Kementerian menggunakan alamat @pu.go.id.
(3) Surat elektronik Kementerian diperuntukkan bagi Aparatur Sipil Negara Kementerian dengan mengajukan permohonan secara resmi kepada Pusdatin.
(4) Surat elektronik Kementerian dikelola oleh Pusdatin.

BAB VIII

TATA KELOLA

Pasal 15

Tata kelola *e-Government* di Kementerian dilaksanakan pada tingkat Kementerian dan unit organisasi.

Pasal 16

(1) Tata kelola *e-Government* Kementerian dikoordinasikan oleh Pusdatin.
(2) Dalam tata kelola *e-Government* Kementerian, Pusdatin mempunyai tugas:
    a. menyusun cetak biru (*blue print*);
    b. menyusun standar manual peralatan, interoperabilitas, dan keamanan sistem informasi;
    c. memfasilitasi unit kerja dalam pembangunan dan pengembangan sistem informasi pekerjaan umum dan perumahan rakyat;
    d. membina sumber daya manusia di bidang teknologi informasi dan komunikasi;

e. menyediakan data dan informasi untuk keperluan internal dan eksternal sesuai dengan tugas dan fungsinya;
f. menyediakan infrastruktur teknologi informasi;
g. membangun, mengembangkan dan memelihara aplikasi umum berdasarkan masukan proses kerja unit organisasi di Kementerian;
h. membangun, mengembangkan dan memelihara aplikasi yang melibatkan lebih dari satu unit organisasi;
i. memfasilitasi dan mengelola nama sub domain Kementerian untuk situs *web* resmi unit organisasi;
j. menyediakan menu unit organisasi pada portal *web* Kementerian sebagai sarana pendukung penyelenggaraan *e-Government*;
k. melakukan evaluasi sistem informasi secara berkala.

(3) Cetak biru (*blue print*) sebagaimana dimaksud pada ayat (2) huruf a harus memuat:
a. Arsitektur infrastruktur teknologi informasi dan komunikasi;
b. Arsitektur sistem informasi;
c. Kebutuhan data dan informasi;
d. Tata kelola teknologi informasi dan komunikasi; dan
e. Rencana pengembangan teknologi informasi dan komunikasi (*road map*).

Pasal 17

(1) Tata kelola *e-Government* unit organisasi dilaksanakan oleh:
a. Pada Sekretariat Jenderal, dilaksanakan oleh Pusdatin;
b. Pada Direktorat Jenderal Sumber Daya Air, dilaksanakan oleh Direktorat Pengembangan Jaringan Sumber Daya Air;
c. Pada Direktorat Jenderal Bina Marga, dilaksanakan oleh Direktorat Pengembangan Jaringan Jalan;
d. Pada Direktorat Jenderal Cipta Karya, dilaksanakan oleh Direktorat Keterpaduan Infrastruktur Permukiman;

e. Pada Direktorat Jenderal Penyediaan Perumahan, dilaksanakan oleh Direktorat Perencanaan Penyediaan Perumahan;
f. Pada Direktorat Jenderal Bina Konstruksi, dilaksanakan oleh Sekretariat Direktorat Jenderal Bina Konstruksi;
g. Pada Direktorat Jenderal Pembiayaan Perumahan, dilaksanakan oleh Direktorat Perencanaan Pembiayaan Perumahan;
h. Pada Inspektorat Jenderal, dilaksanakan oleh Sekretariat Inspektorat Jenderal;
i. Pada Badan Pengembangan Infrastruktur Wilayah, dilaksanakan oleh Sekretariat Badan Pengembangan Infrastruktur Wilayah;
j. Pada Badan Penelitian dan Pengembangan, dilaksanakan oleh Sekretariat Badan Penelitian dan Pengembangan;
k. Pada Badan Pengembangan Sumber Daya Manusia, dilaksanakan oleh Sekretariat Badan Pengembangan Sumber Daya Manusia.

(2) Penyelenggara *e-Government* sebagaimana dimaksud pada ayat (1) sesuai kewenangannya mempunyai tugas:
a. melaporkan dan mengkoordinasikan penyelenggaraan *e-Government*;
b. menyusun rencana dan mengembangkan *e-Government* unit organisasi sesuai cetak biru (*blue print*) sebagaimana yang dimaksud dalam Pasal 16 ayat (2) huruf a;
c. membina sumber daya manusia di bidang teknologi informasi dan komunikasi;
d. menyediakan dan memutakhirkan data dan informasi;
e. menyediakan akses bagi sistem informasi lain;
f. menyediakan infrastruktur;
g. menyediakan aplikasi khusus;
h. mengelola situs *web* unit organisasi.

(3) Penyelenggara *e-Government* unit organisasi sebagaimana dimaksud pada ayat (1) berkoordinasi dengan Pusdatin.

Pasal 18

(1) Untuk memperlancar penyelenggaraan *e-Government* Kementerian, perlu dibentuk Tim Pengelola *e-Government* Kementerian yang ditetapkan dengan Keputusan Menteri.
(2) Penyelenggaraan *e-Government* sebagaimana dimaksud dalam Pasal 16 dan Pasal 17 dapat bekerja sama dengan instansi pemerintah Pusat, Daerah, Badan Usaha, dan masyarakat.

BAB IX
EVALUASI

Pasal 19

(1) Evaluasi *e-Government* di Kementerian dilakukan oleh Kepala Pusdatin secara periodik setiap 1 (satu) tahun sekali.
(2) Evaluasi *e-Government* sebagaimana dimaksud pada ayat (1), meliputi:
    a. infrastruktur teknologi informasi dan komunikasi;
    b. aplikasi;
    c. data dan informasi;
    d. portal *web* Kementerian;
    e. surat elektronik (*e-mail*) Kementerian; dan
    f. tata kelola.
(3) Evaluasi sebagaimana dimaksud pada ayat (2) hasilnya dilaporkan kepada Menteri.

BAB X
KETENTUAN PENUTUP

Pasal 20

Peraturan Menteri ini mulai berlaku pada tanggal diundangkan.

Agar setiap orang mengetahuinya, memerintahkan pengundangan Peraturan Menteri ini dengan penempatannya dalam Berita Negara Republik Indonesia.

Ditetapkan di Jakarta
pada tanggal 2 Mei 2016

MENTERI PEKERJAAN UMUM DAN
PERUMAHAN RAKYAT REPUBLIK INDONESIA,

ttd

M. BASUKI HADIMULJONO

Diundangkan di Jakarta
pada tanggal 2 Juni 2016

DIREKTUR JENDERAL
PERATURAN PERUNDANG-UNDANGAN
KEMENTERIAN HUKUM DAN HAK ASASI MANUSIA
REPUBLIK INDONESIA,

ttd

WIDODO EKATJAHJANA

BERITA NEGARA REPUBLIK INDONESIA TAHUN 2016 NOMOR 819

Salinan sesuai dengan aslinya
KEMENTERIAN PEKERJAAN UMUM DAN
PERUMAHAN RAKYAT
Kepala Biro Hukum,

Siti Martini
NIP. 195803311984122001

LAMPIRAN I
PERATURAN MENTERI PEKERJAAN UMUM
DAN PERUMAHAN RAKYAT REPUBLIK INDONESIA
NOMOR 17 /PRT/M/2016
TENTANG
PENYELENGGARAAN TEKNOLOGI INFORMASI DAN KOMUNIKASI DI KEMENTERIAN PEKERJAAN UMUM DAN PERUMAHAN RAKYAT

STANDAR KEAMANAN INFORMASI

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.

2. RUANG LINGKUP

2.1 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.

2.2 Aset informasi Kementerian adalah aset dalam bentuk:

2.2.1 Seluruh data/dokumen/informasi sebagaimana diatur dalam klasifikasi informasi yang berlaku;

2.2.2 Piranti lunak, meliputi aplikasi, sistem operasi, sistem basis data, dan alat bantu (*tools*) aplikasi;

2.2.3 Aset fisik, meliputi perangkat komputer, perangkat jaringan dan komunikasi, media penyimpanan (*storage*), media lepas

pasang (*removable media*), dan perangkat pendukung (*peripheral*); dan

2.2.4 Aset tak berwujud (*intangible*), meliputi pengetahuan, pengalaman, keahlian, citra, dan reputasi.

3. KEBIJAKAN

3.1 Setiap Pimpinan Unit Organisasi dan Unit Kerja bertanggung jawab mengatur penerapan Kebijakan dan Standar Keamanan Informasi yang ditetapkan dalam Peraturan Menteri ini di Unit masing-masing.

3.2 Unit Organisasi dan Unit Kerja harus menerapkan Kebijakan dan Standar Keamanan Informasi yang ditetapkan dalam Peraturan Menteri ini di Unit masing-masing.

3.3 Setiap Pimpinan Unit Organisasi dan Unit Kerja bertanggung jawab mengatur pelaksanaan pengamanan dan perlindungan aset informasi di Unit masing-masing dengan mengacu pada Kebijakan dan Standar Keamanan Informasi di Kementerian yang ditetapkan dalam Peraturan Menteri ini.

3.4 Pusdatin dan Unit Organisasi bertanggung jawab meningkatkan pengetahuan, keterampilan, dan kepedulian terhadap keamanan informasi pada seluruh pengguna di lingkungan Unit Organisasi masing-masing.

3.5 Pusdatin dan Unit Organisasi menerapkan dan mengembangkan manajemen risiko dalam rangka pelaksanaan pengamanan dan perlindungan aset informasi.

3.6 Pihak ketiga harus bertanggung jawab untuk melindungi kerahasiaan, keutuhan, dan/atau ketersediaan aset informasi Kementerian.

3.7 Pusdatin dan Unit Organisasi melakukan evaluasi terhadap pelaksanaan Keamanan Informasi secara berkala untuk menjamin efektivitas dan meningkatkan keamanan informasi.

3.8 Inspektorat Jenderal Kementerian 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.

3.9 Pusdatin dan Unit Organisasi menggunakan laporan audit internal Keamanan Informasi untuk meninjau efektivitas penerapan Keamanan Informasi dan melakukan tindak lanjut terhadap temuan auditor.

4. TANGGUNGJAWAB

4.1 Pihak-pihak yang terkait dalam keamanan informasi terdiri dari:
- 4.1.1 Pemilik aset informasi adalah Pimpinan Unit Organisasi yang memiliki kebutuhan akan keamanan informasi untuk mendukung tugas dan fungsinya;
- 4.1.2 Petugas keamanan informasi adalah pegawai Kementerian dan/atau Pihak Ketiga yang melaksanakan tanggung jawab terkait keamanan informasi;
- 4.1.3 Tim pengendali mutu keamanan informasi (*information security assurance*) adalah tim yang dibentuk untuk melaksanakan kegiatan penjaminan keamanan informasi;
- 4.1.4 Pengguna, adalah pegawai dan bukan pegawai Kementerian yang mengakses informasi Kementerian.

4.2 Pemilik aset informasi mempunyai tanggung jawab terhadap:
- 4.2.1 Menetapkan target keamanan informasi setiap tahunnya dan menyusun rencana kerja untuk Kementerian, masing-masing Unit Organisasi, maupun yang bersifat lintas unit;
- 4.2.2 Memastikan efektivitas dan konsistensi penerapan Kebijakan dan Standar Keamanan Informasi di Kementerian; dan
- 4.2.3 Melaporkan kinerja penerapan Kebijakan dan Standar Keamanan Informasi di Kementerian dan pencapaian target kepada tim pengendali mutu keamanan informasi (*information security assurance*).

4.3 Petugas keamanan informasi mempunyai tanggung jawab terhadap:
- 4.3.1 Melaksanakan dan mengawasi penerapan Kebijakan dan Standar Keamanan Informasi di Kementerian;
- 4.3.2 Memberi masukan peningkatan terhadap Kebijakan dan Standar Keamanan Informasi di Kementerian;
- 4.3.3 Mendefinisikan kebutuhan, merekomendasikan, dan mengupayakan penyelenggaraan pendidikan dan pelatihan keamanan informasi bagi pegawai;

4.3.4 Memantau, mencatat, dan menguraikan secara jelas gangguan keamanan informasi yang diketahui atau laporan yang diterima, dan menindaklanjuti laporan tersebut sesuai prosedur pelaporan gangguan keamanan informasi; dan

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

4.4 Tim pengendali mutu keamanan informasi (*information security assurance*) mempunyai tanggung jawab terhadap:

4.4.1 Pendampingan dan penjaminan keamanan informasi;

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

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

5. STANDAR

5.1 Standar Keamanan Informasi terdiri atas:

5.1.1 Standar Manajemen Keamanan Informasi;

5.1.2 Standar Pengendalian Pengelolaan Aset Informasi;

5.1.3 Standar Pengendalian Keamanan Sumber Daya Manusia;

5.1.4 Standar Pengendalian Keamanan Fisik dan Lingkungan;

5.1.5 Standar Pengendalian Pengelolaan Komunikasi dan Operasional;

5.1.6 Standar Pengendalian Akses;

5.1.7 Standar Pengendalian Keamanan Informasi dalam Pengadaan, Pengembangan, dan Pemeliharaan Sistem informasi;

5.1.8 Standar Pengendalian Pengelolaan Gangguan Keamanan Informasi;

5.1.9 Standar Pengendalian Keamanan Informasi dalam Pengelolaan Kelangsungan Kegiatan; dan

5.1.10 Standar Pengendalian Kepatuhan.

5.2 Standar Manajemen Keamanan Informasi

5.2.1 Catatan Penerapan Kebijakan dan Standar Keamanan Informasi di Kementerian

1) Pusdatin dan Unit Organisasi 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.

5.2.2 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.

5.2.3 Pengendalian Dokumen

1) Pusdatin dan Unit Organisasi 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) Pusdatin dan Unit Organisasi harus menempatkan dokumen keamanan informasi Kementerian di semua area operasional sehingga mudah diakses oleh pengguna di unit kerja masing-masing sesuai peruntukannya.

5.3 Standar Pengendalian Pengelolaan Aset Informasi

5.3.1 Pemilik Aset Informasi menetapkan dan mengkaji secara berkala klasifikasi aset informasi dan jenis perlindungan keamanannya.

5.3.2 Pemilik Aset Informasi menetapkan pihak yang berwenang untuk mengakses aset informasi.

5.3.3 Dalam pengelolaan aset informasi Kementerian, aset informasi diklasifikasikan mengacu kepada peraturan perundang-undangan yang berlaku.

5.4 Standar Pengendalian Keamanan Sumber Daya Manusia

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

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

5.4.3 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.

5.4.4 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.

5.5 Standar Pengendalian Keamanan Fisik dan Lingkungan

5.5.1 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.

5.5.2 Pengamanan Area

1) Seluruh pegawai, pihak ketiga, dan tamu yang memasuki lingkungan Kementerian harus mematuhi aturan yang berlaku di Kementerian.
2) Pusdatin dan Unit Organisasi 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, *data center*, dan area kerja yang berisikan aset informasi yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA harus dibatasi dan hanya diberikan kepada pegawai yang berwenang;

4) Pihak ketiga yang memasuki ruang server, pusat data (*data center*), dan area kerja yang berisikan aset informasi yang memiliki klasifikasi SANGAT RAHASIA dan RAHASIA harus didampingi pegawai Pusdatin dan/atau Unit Organisasi 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.

5.5.3 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.

5.5.4 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.

5.6 Standar Pengendalian Pengelolaan Komunikasi dan Operasional

5.6.1 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.

5.6.2 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.

5.6.3 Pemantauan dan Pengkajian Layanan Pihak Ketiga Pemantauan dan pengkajian layanan dari pihak ketiga, serta laporan dan catatan dari pihak ketiga mencakup proses sebagai berikut:

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.

5.6.4 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 (*miss-routing*), 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 perIu 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.

5.7 Standar Pengendalian Akses

5.7.1 Persyaratan untuk Pengendalian Akses

Unit Organisasi 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.

5.7.2 Pengelolaan Akses Pengguna

Pusdatin dan Unit Organisasi 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.

5.7.3 Pengelolaan Hak Akses Khusus (*privilege management*)

Pusdatin dan Unit Organisasi 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*).

5.7.4 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.

5.7.5 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.

5.7.6 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.

5.7.7 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.

5.8 Standar Pengendalian Keamanan Informasi dalam Pengadaan, Pengembangan, dan Pemeliharaan Sistem Informasi

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

5.8.2 Pengolahan Data pada Aplikasi

1) Pemeriksaan data masukan harus mempertimbangkan:
   a. Penerapan masukan rangkap (*dual input*) atau mekanisme pengecekan masukan Iainnya 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 seIuruh 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.

5.8.3 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.

5.8.4 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. Pengelola TIK tidak boleh memiliki akses yang tidak terbatas ke 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.

5.8.5 Keamanan dalam proses pengembangan dan pendukung (*support proceses*)

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. Perjanjian *escrow*;
   c. Hak untuk melakukan audit terhadap kualitas dan akurasi pekerjaan;
   d. Persyaratan kontrak mengenai kualitas dan fungsi keamanan aplikasi;
   e. 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.

5.9 Standar Pengendalian Pengelolaan Gangguan Keamanan Informasi

5.9.1 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 Pusdatin dan Unit Organisasi 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.

5.9.2 Pengelolaan Gangguan Keamanan Informasi dan Perbaikannya

1) Pusdatin dan Unit Organisasi 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 *denial of service*;
      - 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

Pusdatin dan Unit Organisasi harus mengumpulkan, menyimpan, dan menyajikan bukti pelanggaran terhadap Kebijakan dan Standar Keamanan Informasi di Kementerian.

5.10 Standar Pengendalian Keamanan Informasi dalam Pengelolaan Kelangsungan Kegiatan

5.10.1 Unit Organisasi harus mengelola proses kelangsungan kegiatan pada saat keadaan darurat di Unit Organisasi

masing-masing.

5.10.2 Unit Organisasi harus mengidentifikasi risiko, dan menganalisis dampak yang diakibatkan pada saat terjadi keadaan darurat untuk menjamin kelangsungan kegiatan.

5.10.3 Unit Organisasi harus menyusun dan menerapkan Rencana Kelangsungan Kegiatan untuk menjaga dan mengembalikan kegiatan operasional dalam jangka waktu yang disepakati dan level yang dibutuhkan.

5.10.4 Unit Organisasi harus memelihara dan memastikan rencana-rencana yang termuat dalam Rencana Kelangsungan Kegiatan masih sesuai, dan mengidentifikasi prioritas untuk kegiatan uji coba.

5.10.5 Unit Organisasi harus melakukan uji coba Rencana Kelangsungan Kegiatan secara berkala untuk memastikan Rencana Kelangsungan Kegiatan dapat dilaksanakan secara efektif.

5.10.6 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.

5.10.7 Proses identifikasi risiko mengikuti ketentuan mengenai

Penerapan Manajemen Risiko di Kementerian.

5.10.8 Proses analisis dampak kegiatan harus melibatkan pemilik proses bisnis dan dievaluasi secara berkala.

5.10.9 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*).

5.10.10 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 Petugas 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.

5.11 Standar Pengendalian Kepatuhan

5.11.1 Kepatuhan terhadap Peraturan Perundangan yang terkait Keamanan Informasi

1) Seluruh pegawai dan pihak ketiga harus menaati peraturan perundangan yang terkait dengan keamanan informasi.
2) Pusdatin dan Unit Organisasi harus mengidentifikasi, mendokumentasikan, dan memelihara kemutakhiran semua peraturan perundangan yang terkait dengan sistem keamanan informasi.
3) Hak Atas Kekayaan Intelektual
   Piranti lunak yang dikelola Pusdatin dan Unit Organisasi 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
   Pusdatin dan Unit Organisasi melindungi kepemilikan dan kerahasiaan data. Data hanya digunakan untuk kepentingan yang dibenarkan oleh peraturan perundangan dan kesepakatan.

5.11.2 Kepatuhan Teknis

Pusdatin dan Unit Organisasi harus melakukan pemeriksaan kepatuhan teknis secara berkala untuk menjamin efektivitas standar dan prosedur keamanan informasi yang ada di area operasional.

5.11.3 Audit Sistem Informasi

1) Pengendalian audit sistem informasi

   Pusdatin dan Unit Organisasi bersama dengan Inspektorat Jenderal harus membuat perencanaan persyaratan, ruang lingkup, dan kegiatan audit yang melibatkan pemeriksaan sistem operasional untuk mengurangi kemungkinan risiko gangguan yang bisa terjadi terhadap kegiatan Kementerian selama proses audit.

2) Perlindungan terhadap alat bantu (*tools*) audit sistem informasi

   Penggunaan alat bantu (baik piranti lunak maupun perangkat keras) untuk mengetahui kelemahan keamanan, memindai (*scanning*) kata sandi, atau untuk melemahkan dan menerobos sistem keamanan inforrnasi tidak diizinkan kecuali atas persetujuan Pimpinan Pusdatin dan Unit Organisasi.

3) Proses audit sistem informasi harus memperhatikan hal berikut:

   a. Persyaratan audit harus disetujui oleh Pimpinan Unit Organisasi;
   b. Ruang lingkup pemeriksaan/audit harus disetujui dan dikendalikan oleh pihak berwenang;
   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.

5.11.4 Kepatuhan terhadap Hak Kekayaan Intelektual

Hal yang perIu 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.

5.11.5 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.

5.11.6 Kepatuhan Teknis

Sistem informasi harus diperiksa secara berkala untuk memastikan pengendalian perangkat keras dan piranti lunak

telah diimplementasikan secara benar. Kepatuhan teknis juga mencakup pengujian penetrasi (*penetrating testing*) untuk mendeteksi kerentanan dalam sistem, dan memeriksa pengendalian akses untuk mencegah kerentanan tersebut telah diterapkan.

6. ISTILAH YANG DIGUNAKAN

6.1 Akun adalah identifikasi pengguna yang diberikan oleh unit Pengelola TIK, bersifat unik dan digunakan bersamaan dengan kata sandi ketika akan memasuki sistem TIK.

6.2 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).

6.3 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.

6.4 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.

6.5 *Conduit* adalah sebuah tabung atau saluran untuk melindungi kabel yang biasanya terbuat dari baja.

6.6 Data adalah catatan atas kumpulan fakta yang mempunyai arti baik secara kualitatif maupun kuantitatif.

6.7 *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.

6.8 Direktori adalah hirarki atau *tree structure.*

6.9 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.

6.10 *Fallback* adalah suatu tindakan pembalikan/menarik diri dari posisi awal.

6.11 Fasilitas adalah sarana untuk melancarkan pelaksanaan fungsi atau mempermudah sesuatu.

6.12 Fasilitas utama adalah sarana utama gedung atau bangunan, seperti pusat control listrik, CCTV.

6.13 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.

6.14 *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.

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

6.16 Kata sandi adalah serangkaian kode yang dibuat pengguna, bersifat rahasia dan pribadi yang digunakan bersamaan dengan Akun Pengguna.

6.17 Keamanan informasi adalah perlindungan aset informasi dari berbagai bentuk ancaman untuk memastikan kelangsungan kegiatan, menjamin kerahasiaan, keutuhan, dan ketersediaan aset informasi.

6.18 Koneksi eksternal (*remote access*) adalah suatu akses jaringan komunikasi dari luar organisasi ke dalam organisasi.

6.19 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.

6.20 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.

6.21 Cakram utama (*master disk*) adalah media yang digunakan

sebagai sumber dalam melakukan instalasi piranti lunak.

6.22 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.

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

6.24 Perangkat jaringan adalah peralatan jaringan komunikasi data seperti *modem, hub, switch, router,* dan lain-lain.

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

6.26 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.

6.27 Perangkat pengolah informasi adalah setiap sistem pengolah informasi, layanan atau infrastruktur. Contoh perangkat pengolah informasi adalah komputer, faksimili, telepon, mesin *fotocopy.*

6.28 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).*

6.29 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.

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

6.31 Pihak ketiga adalah semua unsur di Iuar 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.

6.32 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.

6.33 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.

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

6.35 *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.

6.36 Sanitasi adalah proses penghilangan informasi yang disimpan secara permanen dengan menggunakan medan magnet besar atau perusakan fisik.

6.37 Manajemen Keamanan Informasi adalah sistem manajemen yang meliputi kebijakan, organisasi, perencanaan, penangung jawab, proses, dan sumber daya yang mengacu pada pendekatan risiko bisnis untuk menetapkan, mengimplementasikan, mengoperasikan, memantau, mengevaluasi, mengelola, dan meningkatkan keamanan informasi.

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

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

6.40 Sistem TIK adalah sistem operasi, sistem surat elektronik, sistem aplikasi, sistem basis data, sistem jaringan intranet/internet, dan sebagainya.

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

6.42 Perangkat jarak jauh (*teleworking*) adalah penggunaan teknologi telekomunikasi untuk memungkinkan pegawai bekerja di suatu lokasi yang berada di luar kantor untuk mengakses jaringan internal

kantor.

MENTERI PEKERJAAN UMUM DAN
PERUMAHAN RAKYAT REPUBLIK INDONESIA,

ttd

M. BASUKI HADIMULJONO

Salinan sesuai dengan aslinya
KEMENTERIAN PEKERJAAN UMUM DAN
PERUMAHAN RAKYAT
Kepala Biro Hukum,

Siti Martini
NIP. 195803311984122001

LAMPIRAN II
PERATURAN MENTERI PEKERJAAN UMUM
DAN PERUMAHAN RAKYAT REPUBLIK INDONESIA
NOMOR 17/PRT/M/2016
TENTANG
PENYELENGGARAAN TEKNOLOGI INFORMASI DAN KOMUNIKASI DI KEMENTERIAN PEKERJAAN UMUM DAN PERUMAHAN RAKYAT

PUSAT DATA (*DATA CENTER*)

1. TUJUAN

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

2. RUANG LINGKUP

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

3. KEBIJAKAN

3.1 Kementerian menyediakan fasilitas berupa pusat data (*data center*) untuk pengelolaan *e-Government.*
3.2 Penyelenggara pusat data (*data center*) Kementerian dilakukan secara terpusat oleh Pusdatin.
3.3 Pusdatin menyediakan layanan penempatan (*hosting*) portal *web* (*website)* dan aplikasi berbasis *web* kepada setiap Unit Organisasi.
3.4 Pusdatin menyediakan layanan pencadangan sistem (*system backup*) untuk aplikasi yang bersifat umum dan aplikasi khusus untuk Unit Organisasi.
3.5 Pusdatin menyediakan seluruh fasilitas, infrastruktur teknologi informasi (*server*, sistem operasi, penyimpanan (*storage*), cadangan (*backup*), perangkat jaringan) dan sistem keamanan pusat data *(data*

center) untuk memfasilitasi layanan penempatan (*hosting*) pada butir 3.3.

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

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

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

3.9 Seluruh peralatan, baik perangkat keras maupun piranti lunak termasuk di dalamnya data dan aplikasi, yang berada di dalam pusat data *(data center)* menjadi milik Kementerian dan tidak boleh digunakan di luar Kementerian tanpa izin dari Kepala Pusdatin.

4. TANGGUNG JAWAB

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

4.1.1 Pemilik aplikasi adalah Pimpinan Unit Organisasi atau Pejabat di Kementerian yang membutuhkan aplikasi untuk mendukung tugas dan fungsinya;

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

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

4.1.4 Pengguna, adalah pegawai Kementerian.

4.2 Pemilik aplikasi mempunyai tanggung jawab terhadap:

4.2.1 Pemberian persetujuan:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

5. STANDAR

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

5.1.1 Persyaratan Disain Teknis dan Implementasi;

5.1.2 Persyaratan Operasi;

5.1.3 Persyaratan Keberlangsungan Kegiatan.

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

5.2.1 Lokasi

1) Bangunan harus berada pada lokasi yang aman berdasarkan kajian indeks rawan bencana Indonesia.
2) Bangunan harus mempunyai akses jalan yang cukup dan fasilitas parkir.
3) Lokasi sebaiknya berada di kawasan yang memiliki temperatur rendah serta tingkat kelembaban yang rendah.

5.2.2 Persyaratan Bangunan dan Arsitektur

1) Tidak berada di bawah area perpipaan (*plumbing*) seperti kamar mandi, toilet, dapur, laboratorium dan ruang mekanik kecuali jika sistem pengendalian air disiapkan.
2) Tiap jendela yang menghadap ke sinar matahari harus ditutup untuk mencegah paparan panas.
3) Memiliki area bongkar muat yang memadai untuk menangani kegiatan bongkar/muat barang/peralatan.

5.2.3 Persyaratan Kontrol Akses dan Keamanan

1) Setiap pintu dan jendela yang memungkinkan akses langsung ke pusat data *(data center)*, diberi pengaman fisik.
2) Pusat data *(data center)* harus diamankan selama 24 jam dengan paling sedikit 1 (satu) orang petugas per siklus kerja (*shift*).
3) Perangkat sistem pemantau visual (seperti CCTV) harus dipasang untuk memantau dan merekam setiap aktivitas pada ruang *server*, ruang mekanik dan kelistrikan, ruang telekomunikasi, dan kawasan kantor.
4) Akses ke dalam ruang *server* menggunakan perangkat yang dikendalikan dengan mekanisme otentikasi (seperti pin, kartu gesek, kartu nirkontak atau akses biometrik). Tamu/pengunjung harus dilengkapi dengan tanda masuk dan tanda pengenal untuk dapat masuk ke ruang *server*, ruang mekanikal dan kelistrikan, ruang telekomunikasi dan kawasan kantor. Setiap orang yang masuk ke dalam ruangan sebagaimana dimaksud di atas harus memiliki izin dan didampingi oleh pemilik aplikasi dan Pusdatin.

5.2.4 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 *pre-action*.

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

5.2.5 Penyediaan Catu Daya

1) Kabel daya masuk ke dalam bangunan pusat data *(data center)* diterminasi di ruang kendali penyambungan listrik yang handal.
2) Daya listrik utama paling sedikit 20% lebih besar dari proyeksi beban puncak di mana pusat data *(data center)* berada.
3) Tersedianya catu daya listrik alternatif (seperti generator *standby*) dengan kapasitas yang memadai untuk operasional minimal 3 jam selama kejadian gangguan listrik utama.
4) Perangkat TIK (Teknologi Informasi dan Komunikasi) harus diproteksi dengan *Uninterruptible Power Supply* (UPS) atau catu daya cadangan lainnya.
5) UPS atau catu daya cadangan lainnya harus memiliki kapasitas memadai untuk memasok beban TIK sampai catu daya alternatif mampu memikul beban perangkat TIK (*steady-state*).
6) Kapasitas UPS harus lebih besar dari proyeksi beban puncak perangkat TIK. Kapasitas beban rata-rata tidak lebih besar dari 80% kapasitas UPS.
7) UPS memiliki sistem pelaporan, pemantauan kinerja, dan sistem peringatan.
8) UPS yang digunakan telah memiliki jaminan dari pabrikan untuk dapat berfungsi sesuai spesifikasinya.
9) Bangunan harus dilengkapi dengan sistem proteksi petir.
10) Kabel komunikasi tembaga dari luar gedung diproteksi dengan peredam tegangan lebih (*surge suppressor*) sebelum ke ruang pusat data *(data center)* .
11) Ruang pusat data *(data center)* memiliki terminal pembumian (*grounding*) tembaga yang menjadi titik acuan pembumian ruangan tersebut.

5.2.6 Penyediaan Sistem Pendingin dan Kelembaban

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

5.2.7 Penyediaan Sistem Pengkabelan dan Manajemen Kabel

1) Sistem pengkabelan yang digunakan untuk konektivitas ke setiap rak sesuai dengan standar nasional/internasional.
2) Seluruh pengkabelan interior adalah kabel dalam ruangan dengan tipe tidak mudah terbakar (*low flammability*).
3) Setiap rak memiliki akses ke sistem saluran kabel, di atas atau di bawahnya, yang memungkinkan kabel-kabel dapat ditata secara baik antar rak.
4) Kabel daya satu fase dan kabel data tembaga harus dipisahkan paling sedikit 20 cm.
5) Kabel daya tiga fase dan kabel data tembaga harus dipisahkan paling sedikit 60 cm.
6) Kabel yang melewati dinding dilindungi terhadap bahaya api sesuai ketentuan peraturan perundang-undangan.
7) Kabel tidak boleh diletakkan di pintu, lantai, atau digantung antar rak.
8) Setiap kabel memiliki label identifikasi yang unik pada kedua ujung awal dan akhir, dengan data pemilik (jika diperlukan).
9) Setiap rak peralatan memiliki label identifikasi data pemilik (jika diperlukan).
10) Kabel input telekomunikasi eksternal dihubungkan di area atau ruang telekomunikasi tersendiri.
11) Jika area telekomunikasi terpisah dari ruang pusat data *(data center)* maka harus memiliki sistem pengatur temperatur, proteksi kebakaran, kelistrikan yang sama dengan standar ruang pusat data *(data center)* .
12) Seluruh item perangkat logam berisi kabel harus dibumikan (*grounded*).

5.2.8 Sistem Manajemen Bangunan dan Pemantauan

1) Ruang pusat data *(data center)* memiliki paling sedikit satu sensor temperatur ruang dan satu sensor kelembaban ruang.
2) Ruang telekomunikasi dan ruang mekanikal dan kelistrikan memiliki sebuah sensor temperatur dan sensor kelembaban ruang.

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

5.3.1 Tata Kerja dalam Bangunan

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

5.3.2 Dokumentasi Manajemen Operasi

1) Manual operasi umum diperlukan dan harus mencakup seluruh persyaratan operasi pusat data *(data center)*.
2) Seluruh perangkat utama seperti pengkondisi udara, UPS, generator, dan lain sebagainya harus terdapat dalam pencatatan aset:
   a. Lokasi
   b. Nomor seri
   c. Data pengadaan
   d. Kontak rinci pabrikan
   e. Tanggal kalibrasi jika diperlukan
3) Konfigurasi dan prosedur operasi harus didokumentasikan termasuk di dalamnya:
   a. Perubahan konfigurasi
   b. *Set-point default*
4) Informasi dokumentasi lokasi meliputi:
   a. Bangunan dan lantai
   b. Lokasi rak dan item utama dari perangkat
   c. Denah rak
   d. Koneksi fisik dan logik antar 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)*.

5.3.3 Prosedur Pemeliharaan

1) Setiap staf pusat data *(data center)* dan/atau kontraktor yang bertugas dalam pemeliharaan harus memiliki kompetensi dalam pemeliharaan pusat data *(data center)*.
2) Setiap peralatan yang membutuhkan pemeliharaan harus memiliki catatan pemeliharaan yang berisi peralatan, tanggal pemeliharaan, hasil, dan kontak rinci.

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

5.4.1 Manajemen Risiko

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

5.4.2 Penanganan Insiden

1) Setiap gangguan kritis dan berhentinya layanan harus diinformasikan kepada pengguna pusat data *(data center) secepatnya*.
2) Setiap gangguan dan berhentinya layanan dapat disampaikan kepada Pusdatin 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 (*start-up*) generator dapat beroperasi dengan baik.
6) Pada setiap siklus kerja (*shift*) harus diidentifikasi oleh petugas yang bertanggung jawab untuk memberikan tanggapan terhadap setiap insiden/bencana.

5.4.3 Pusat Pemulihan Bencana (*Disaster Recovery Center*)

1) Penyelenggara pusat data *(data center)* harus memiliki fasilitas sistem cadangan (*backup system*).
2) Penempatan fasilitas Pusat Pemulihan Bencana harus mempertimbangkan:
   a. jarak terhadap lokasi pusat data *(data center)* yang meminimalkan risiko;
   b. biaya yang layak; dan
   c. memenuhi Perjanjian Tingkat Layanan (*Service Level Agreement* (SLA)) yang disyaratkan.

6. ISTILAH YANG DIGUNAKAN

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

6.2 Pusat pemulihan bencana *(disaster recovery center)* adalah fasilitas sistem cadangan (*backup system*) pusat data (*data center*) yang terdiri dari

perangkat keras dan piranti lunak untuk mendukung kegiatan operasional Kementerian secara berkesinambungan ketika pusat data *(data center)* mati/rusak karena bencana .

MENTERI PEKERJAAN UMUM DAN
PERUMAHAN RAKYAT REPUBLIK INDONESIA,

ttd

M. BASUKI HADIMULJONO

Salinan sesuai dengan aslinya
KEMENTERIAN PEKERJAAN UMUM DAN
PERUMAHAN RAKYAT
Kepala Biro Hukum,

Siti Martini
NIP. 195803311984122001

LAMPIRAN III
PERATURAN MENTERI PEKERJAAN UMUM
DAN PERUMAHAN RAKYAT REPUBLIK INDONESIA
NOMOR 17/PRT/M/2016
TENTANG
PENYELENGGARAAN TEKNOLOGI INFORMASI DAN KOMUNIKASI DI KEMENTERIAN PEKERJAAN UMUM DAN PERUMAHAN RAKYAT

NAMA DOMAIN DAN SUBDOMAIN

1. UMUM

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. 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 Pusdatin disertai dengan data penanggung jawab portal *web* (*website*), aplikasi berbasis *web* serta pemilik kegiatan.

3. KEBIJAKAN

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

3.2 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.

3.3 Domain dan subdomain yang sudah dibuat menjadi milik Kementerian dan tidak boleh digunakan di luar Kementerian tanpa izin dari pejabat yang berwenang.

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

4.1 Pengertian DNS

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

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

Contoh : yahoo.com → 68.142.197.64

4.2 Struktur DNS

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

4.2.1 Domain Tingkat Pertama (*Root Domain*)

1) Domain Level Global (*Generic/Global Top Level Domain* (gTLD))

Contoh: .com, .net, .org, .ac, .*web*, .go

2) Domain Level Negara (*Country Code Top Level Domain* (ccTLD))

Contoh: .sg, .au, .id

4.2.2 Domain Tingkat Kedua (*Second Level Domain*)

Contoh: pu.go.id

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

Contoh: binamarga.pu.go.id, lpse.pu.go.id

5. PENGELOLAAN PENAMAAN DOMAIN

5.1 Pengelolaan Penamaan Domain meliputi:

a) Pendaftaran,

b) Penggunaan,

c) Penonaktifan,

d) Perpanjangan,

e) Penunjukan pejabat,

f) Perubahan nama domain,

g) *Server* nama domain.

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

5.3 Seluruh situs *web* (*website*) Unit Organisasi dan Unit Kerja serta aplikasi berbasis *web* pada Kementerian harus menjadi subdomain dari nama domain Kementerian.

6. SUBDOMAIN DI KEMENTERIAN

6.1 Yang berhak mendapatkan nama subdomain:

1) Unit Organisasi dan Unit Kerja di Kementerian.
2) Pelayanan publik di Kementerian.
3) Kegiatan Kementerian.
4) Aplikasi berbasis *web*.

6.2 Permohonan mendapatkan nama subdomain.

Mengajukan permohonan melalui Pusdatin dengan mencantumkan dan melampirkan:

1) Surat permohonan nama subdomain layanan publik/domain khusus.
2) Peraturan perundang-undangan yang menjadi dasar penyelenggaraan pelayanan publik/penyelenggaraan kegiatan Kementerian.
3) Surat keterangan mengenai pelayanan publik/kegiatan berskala nasional atau internasional.
4) Penunjukan pejabat nama subdomain.
   a. Surat penunjukan pejabat nama subdomain.
   b. Kartu PNS atau kartu identitas pegawai tetap.

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

6.4 Penataan subdomain untuk Unit Organisasi dan Unit Kerja di bawahnya:

1) Unit Organisasi : *eselonI*.pu.go.id
2) Unit Kerja : *eselonI*.pu.go.id/*eselonII*

3) Unit Eselon III : *eselonI*.pu.go.id/*eselonII*/*produk*

6.5 Penataan subdomain untuk kegiatan Kementerian:

1) Kegiatan Skala Nasional/Internasional:
   kegiatan.pu.go.id
2) Kegiatan Internal Kementerian Tingkat Unit Organisasi:
   eselonI.pu.go.id/*kegiatan*
3) Kegiatan Internal Kementerian Tingkat Unit Kerja:
   eselonI.pu.go.id/*eselonII*/*kegiatan*

6.6 Penataan subdomain untuk aplikasi berbasis web:

1) Digunakan oleh publik:
   aplikasi.pu.go.id
2) Digunakan di lingkungan Kementerian:
   aplikasi.pu.go.id
3) Digunakan di lingkungan Unit Organisasi/Unit Kerja/khusus:
   aplikasi.eselonI.pu.go.id

6.7 Nama subdomain Unit Organisasi di Kementerian:

1) Sekretariat Jenderal : setjen.pu.go.id
2) Ditjen Sumber Daya Air : sda.pu.go.id
3) Ditjen Bina Marga : binamarga.pu.go.id
4) Ditjen Cipta Karya : ciptakarya.pu.go.id
5) Ditjen Penyediaan Perumahan : perumahan.pu.go.id
6) Ditjen Bina Konstruksi : binakonstruksi.pu.go.id
7) Ditjen Pembiayaan Perumahan : pembiayaan.pu.go.id
8) Inspektorat Jenderal : itjen.pu.go.id
9) Badan Pengembangan Infrastruktur Wilayah : bpiw.pu.go.id
10) Badan Penelitian Dan Pengembangan : litbang.pu.go.id
11) Badan Pengembangan SDM : bpsdm.pu.go.id

6.8 Ketentuan lain yang harus diikuti bagi seluruh unit organisasi di Kementerian:

1) Seluruh basis data (*database*) dan portal *web* (*website*)/aplikasi berbasis *web* harus disimpan pada server yang berada di pusat data (*data center*) Kementerian.
2) Unit Organisasi wajib melakukan pembinaan dan pengawasan terhadap unit kerja di bawahnya.
3) Jika terjadi gangguan jaringan komunikasi dan keamanan menjadi tanggung jawab Pusdatin untuk melakukan perbaikan.

4) Jika terjadi gangguan terkait data dan informasi menjadi tanggung jawab unit organisasi pemilik data dan informasi tersebut dan akan dibantu oleh Pusdatin dalam melakukan perbaikan.

MENTERI PEKERJAAN UMUM DAN
PERUMAHAN RAKYAT REPUBLIK INDONESIA,

ttd

M. BASUKI HADIMULJONO

Salinan sesuai dengan aslinya
KEMENTERIAN PEKERJAAN UMUM DAN
PERUMAHAN RAKYAT
Kepala Biro Hukum,

Siti Martini
NIP. 195803311984122001

LAMPIRAN IV
PERATURAN MENTERI PEKERJAAN UMUM
DAN PERUMAHAN RAKYAT REPUBLIK INDONESIA
NOMOR 17/PRT/M/2016
TENTANG
PENYELENGGARAAN TEKNOLOGI INFORMASI DAN KOMUNIKASI DI KEMENTERIAN PEKERJAAN UMUM DAN PERUMAHAN RAKYAT

STANDAR PENGEMBANGAN APLIKASI

1. TUJUAN

standar ini digunakan sebagai pedoman dalam pengembangan aplikasi di Kementerian agar pelaksanaan pengembangan aplikasi efektif dan efisien.

2. RUANG LINGKUP

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

3. KEBIJAKAN

3.1 Aplikasi harus dikembangkan oleh pemilik proses bisnis sesuai dengan tugas dan fungsinya;
3.2 Pemilik proses bisnis bertanggung jawab atas aplikasi yang dikembangkan;
3.3 Penyelenggara pengembangan aplikasi adalah pihak yang ditunjuk oleh pemilik proses bisnis untuk mengembangkan aplikasi mulai dari perencanaan hingga implementasinya;
3.4 Setiap Pimpinan Unit Organisasi bertanggung jawab dalam penerapan Kebijakan dan Standar Pengembangan Aplikasi di Unit Organisasi masing-masing;
3.5 Unit Organisasi harus menerapkan Kebijakan dan Standar Pengembangan Aplikasi di Unit Organisasi masing-masing;

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

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

3.8 Unit Organisasi harus berkoordinasi dengan Pusdatin selama proses pengembangan aplikasi sampai dengan operasionalisasi aplikasi;

3.9 Pusdatin sebagai pengatur, pembina dan pengawas TIK di Kementerian memiliki kewenangan untuk memastikan bahwa proses pengembangan telah sesuai dengan kebijakan dan standar pengembangan aplikasi;

3.10 Aplikasi yang telah dikembangkan untuk kepentingan Kementerian dan Unit Organisasi harus ditempatkan di pusat data (*data center*) Kementerian yang dikelola oleh Pusdatin;

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

4. TANGGUNG JAWAB

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

4.1.1 Pemilik proses bisnis adalah Pimpinan Unit Organisasi atau Pejabat di Kementerian yang memiliki kebutuhan akan adanya aplikasi untuk mendukung berjalannya tugas dan fungsi;

4.1.2 Pengembang aplikasi adalah pegawai pada Unit Organisasi di Kementerian dan/atau Pihak Ketiga yang melaksanakan pengembangan aplikasi;

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

4.1.4 Pengguna aplikasi;

4.1.5 Pusdatin.

4.2 Pemilik proses bisnis mempunyai tanggung jawab terhadap:

4.2.1 Pemberian persetujuan:

a. Dokumen analisis dan spesifikasi kebutuhan aplikasi serta perubahannya;

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

c. Dokumentasi pengembangan aplikasi; dan

d. Dokumen rencana dan skenario pengujian.

4.2.2 Pelaksanaan *User Acceptance Test* (UAT);

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

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

4.2.5 Pemeriksaan dan penandatanganan berita acara anaIisis hasil pengujian dan juga berita acara hasil tinjauan pasca implementasi aplikasi; dan

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

4.2.7 Melakukan evaluasi pasca implementasi dan melaporkan hasilnya ke Pusdatin.

4.3 Pengembang aplikasi mempunyai tanggung jawab terhadap:

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

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

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

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

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

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

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

4.4.1 Pendampingan dan pengendalian mutu dalam pengembangan aplikasi;

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

4.4.3 Pelaksanaan User Acceptance Test (UAT).

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

4.6 Pusdatin mempunyai tanggung jawab terhadap:

4.6.1 Pendampingan dalam pelaksanaan pengendalian mutu dalam pengembangan aplikasi;

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

4.6.3 Pengaturan, pembinaan, dan pengawasan pelaksanaan pengembangan aplikasi di Kementerian ;

4.6.4 Memastikan bahwa pengembangan aplikasi baik proses maupun produk yang dihasilkan sesuai dengan standar aplikasi yang berlaku di Kementerian yang ditetapkan oleh Pusdatin;

4.6.5 Terlibat dalam proses pengujian aplikasi;

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

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

5. STANDAR

5.1 Siklus pengembangan aplikasi terdiri atas:

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

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

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

5.1.4 Proses pengujian aplikasi, merupakan proses yang dilaksanakan untuk menguji aplikasi yang telah dikembangkan;

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

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

5.2 Proses analisis kebutuhan aplikasi

5.2.1 Proses analisis kebutuhan aplikasi meliputi kegiatan:

1) Pengumpulan, analisis, penyusunan, dan pendokumentasian spesifikasi kebutuhan bisnis dan aplikasi yang 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 pengembangan aplikasi;
   e) Konsep dasar operasional aplikasi;
   f) Rencana kapasitas (*capacity planning);*
   g) Infrastruktur pendukung.
2) Pendokumentasian perubahan analisis dan spesifikasi kebutuhan aplikasi yang terjadi dalam proses ini.

5.2.2 Proses analisis kebutuhan aplikasi menghasilkan keluaran:

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

5.3 Proses Perancangan Aplikasi

5.3.1 Sistem aplikasi dan basis data, meliputi kegiatan:

1) Penyusunan dan pendokumentasian rancangan tingkat tinggi dengan mengacu pada dokumen sebagaimana dimaksud pada butir 5.2.2) yang mencakup:
   a) Kebutuhan informasi dan struktur informasi;
   b) Pemetaan hak akses atas informasi oleh peran-peran yang terlibat; dan
   c) Infrastruktur pendukung yang mencakup jaringan komunikasi, *server, workstation,* perangkat pendukung, piranti lunak, dan media penyimpanan data.
2) Penyusunan dan pendokumentasian rancangan rinci yang mencakup:
   a) Rancangan kebutuhan sistem aplikasi dan basis data serta infrastruktur pendukung dengan mengacu pada rancangan tingkat tinggi;
   b) Rancangan antarmuka pengguna (*user interface*)/ rancangan tampilan memasukkan data (*data entry screen design*), pencarian (*inquiry*), menu bantuan, dan navigasi dari layar ke layar sesuai dengan tingkatan pengguna dan pemisahan fungsi tugas (*segregation of duties*);
   c) Rancangan proses waktu nyata (*real-time processing*) dan/atau proses bertahap (*batch processing*);
   d) Rancangan laporan dan dokumen keluaran;
   e) Formulir pracetak (*pre-printed form*) (jika dibutuhkan) serta distribusinya sesuai dengan tingkatan pengguna dan pemisahan fungsi tugas;
   f) Rancangan antarmuka (*interface*) untuk integrasi dengan aplikasi yang lain (jika dibutuhkan);
   g) Rancangan konversi dan/ atau migrasi data (jika dibutuhkan);
   h) Rancangan kendali internal (*internal control*) yang diperlukan dalam kegiatan antara lain validasi, otorisasi dan, jejak audit (*audit trail*); dan
   i) Rancangan keamanan logika (*logic*).

5.3.2 Sistem jaringan pendukung aplikasi, meliputi kegiatan:

1) Penyusunan dan pendokumentasian rancangan tingkat tinggi dengan mengacu pada dokumen sebagaimana dimaksud pada butir 5.2.2.2) yang mencakup:
   a) Gambaran secara garis besar mengenai penempatan aplikasi sistem jaringan yang ada dan rencana penempatan aplikasi dalam sistem jaringan; dan
   b) Gambaran integrasi antara aplikasi dengan sistem jaringan.
2) Penyusunan dan pendokumentasian rancangan rinci yang mencakup:
   a) Rancangan kebutuhan sistem jaringan dengan mengacu pada rancangan tingkat tinggi pengembangan aplikasi;
   b) Rancangan kapasitas mengacu pada rencana kapasitas (*capacity planning*) dan/atau kebutuhan dukungan sistem jaringan terhadap aplikasi;
   c) Rancangan integrasi aplikasi dengan sistem jaringan yang sudah ada;
   d) Rancangan keamanan aplikasi dalam sistem jaringan yang meliputi keamanan fisik maupun logika (*logic*); dan
   e) Rancangan penempatan dan pemasangan sesuai dengan Kebijakan dan Standar Keamanan Aplikasi di Kementerian.
3) Menghasilkan keluaran:
   a) Dokumen rancangan tingkat tinggi; dan
   b) Dokumen rancangan rinci.

5.4 Proses Pengkodean (*coding*) Aplikasi

5.4.1 Sistem aplikasi dan basis data, meliputi kegiatan:

1) Pelaksanaan Pengkodean (*coding*) aplikasi dan basis data sesuai dengan rancangan rinci yang telah disetujui;
2) Pengelolaan perubahan dalam pengkodean (*coding*) aplikasi dan basis data;
3) Penyusunan dokumentasi pengkodean (*coding*) aplikasi dan basis data yang terdiri atas :
   a) Formulir perubahan dan rencana dan laporan hasil pengembangan;
   b) Kode program (*source code*) disertai dengan penjelasannya.

4) Pengendalian terhadap kode program (*source code*) yang sesuai dengan Kebijakan dan Standar Keamanan Aplikasi di Kementerian.

5.4.2 Sistem jaringan pendukung aplikasi, meliputi kegiatan:

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

5.5 Proses Pengujian Aplikasi

5.5.1 Proses pengujian aplikasi meliputi kegiatan:

1) Penyusunan rencana dan skenario untuk setiap jenis pengujian yang mencakup:
   a) Tujuan dan sasaran:
   b) Strategi dan metode, termasuk langkah-Iangkah alternatif apabila aplikasi gagal dalam pengujian;
   c) Ruang lingkup;
   d) Asumsi dan batasan;
   e) Jadwal:

f) Pihak pelaksana dan kompetensi yang dibutuhkan;
g) Alat bantu;
h) Skenario dengan mempertimbangkan risiko teknologi yang telah diidentifikasi;
i) Kriteria penerimaan (*acceptance criteria*); dan
j) Sumber daya yang diperlukan, termasuk penyiapan lingkungan pengujian yang mencerminkan lingkungan operasional.

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

3) Pelaksanaan analisis hasil pengujian.

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

5.6 Proses Implementasi Aplikasi

5.6.1 Proses implementasi aplikasi meliputi kegiatan:
1) Penyusunan rencana implementasi aplikasi di lingkungan operasional yang mencakup sekurang-kurangnya:
a) Kebutuhan sumber daya;
b) Urutan langkah implementasi dari komponen aplikasi;
c) Pemindahan perangkat lunak dari/atau perangkat keras dari lingkungan pengujian ke lingkungan operasional;
d) *Fall-backplan* dan/atau *backup plan* untuk mengantisipasi kegagalan dalam implementasi aplikasi; dan
e) Jadwal pelatihan dan pengajar.

2) Implementasi aplikasi dilakukan sesuai rencana implementasi dengan memperhatikan kebijakan dan standar manajemen rilis yang akan ditetapkan dalam ketentuan tersendiri;

3) Pelaksanaan pelatihan dan transfer pengetahuan;

4) Pendampingan dalam pengoperasian aplikasi dalam kurun waktu tertentu; dan
5) Serah terima aplikasi berikut dokumentasinya kepada pemilik proses bisnis.

5.6.2 Proses implementasi aplikasi menghasilkan keluaran:
1) Dokumen rencana implernentasi aplikasi;
2) Dokumen implementasi/rilis aplikasi;
3) Laporan pelaksanaan pelatihan;
4) Berita acara serah terima aplikasi;
5) Petunjuk instalasi sistem aplikasi dan basis data;
6) Petunjuk instalasi dan pengoperasian perangkat pendukung (jika dibutuhkan);
7) Payung hukum beserta petunjuk teknis yang selaras dengan proses bisnis; dan
8) Materi pelatihan.

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

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

5.7 Pengendalian Mutu

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

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

5.7.3 Menghasilkan keluaran berupa laporan pengendalian mutu.

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

6. ISTILAH YANG DIGUNAKAN

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

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

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

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

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

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

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

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

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

6.10 Pengujian sistem (*system testing*) adalah pengujian perangkat keras/lunak yang baru terhadap aplikasi yang sudah terpasang. Pengujian ini bertujuan untuk melihat apakah perangkat keras/lunak

yang baru dapat berintegrasi dengan baik dengan aplikasi yang sudah ada.

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

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

MENTERI PEKERJAAN UMUM DAN
PERUMAHAN RAKYAT REPUBLIK INDONESIA,

ttd

M. BASUKI HADIMULJONO

Salinan sesuai dengan aslinya
KEMENTERIAN PEKERJAAN UMUM DAN
PERUMAHAN RAKYAT
Kepala Biro Hukum,

Siti Martini
NIP. 195803311984122001

LAMPIRAN V
PERATURAN MENTERI PEKERJAAN UMUM
DAN PERUMAHAN RAKYAT REPUBLIK INDONESIA
NOMOR 17/PRT/M/2016
TENTANG
PENYELENGGARAAN TEKNOLOGI INFORMASI DAN KOMUNIKASI DI KEMENTERIAN PEKERJAAN UMUM DAN PERUMAHAN RAKYAT

PORTAL *WEB*

1. UMUM

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

standar ini berlaku bagi seluruh pembuatan dan pengembangan portal *web* (*website*) yang dilaksanakan oleh seluruh unit organisasi di Kementerian.

2. RUANG LINGKUP

Ruang lingkup dari penataan portal *web* (*website*) meliputi struktur menu, konten serta tata letak (*layout*) portal *web* (*website*) Unit Organisasi dan Unit Kerja yang harus berkoordinasi dengan Pusdatin .

3. KEBIJAKAN

3.1 Setiap Pimpinan Unit Organisasi bertanggung jawab dalam memantau dan mengawasi pembuatan dan pengembangan portal *web* (*website*) di Unit Organisasi masing-masing.

3.2 Setiap Pimpinan Unit Organisasi bertanggung jawab dan mengetahui terhadap penambahan dan perubahan portal *web* (*website*) di Unit

Organisasi masing-masing, dalam hal ini meliputi penambahan, perubahan, dan penghapusan portal *web* (*website*).

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

4. TANGGUNG JAWAB

Pihak-pihak yang terkait dalam pembuatan dan pengembangan portal *web* (*website*) terdiri dari:

4.1. Penanggung jawab portal *web* (*website*) adalah Unit Organisasi di Kementerian yang mengajukan dan menggunakan portal *web* (*website*).

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

4.3. Pengguna adalah publik baik eksternal maupun internal Kementerian.

5. PLATFORM PORTAL *WEB* (*WEBSITE*)

	Penetapan		Penjelasan
	Berlisensi terbuka (*open source*)	Berlisensi berbayar (*licensed*)	
Web Server	▪ Apache	IIS	Mengacu pada kondisi di Pusdatin
Basis Data (*Database*)	▪ MySQL ▪ Postgre	▪ MS SQL ▪ MySQL	
Pengkodean (*Coding*)	▪ PHP ▪ Java	▪ ASP ▪ ASP.NET	

Sistem Informasi Geografis (SIG)	▪ Quantum GIS ▪ Global Mapper	▪ ArcGIS Desktop/ Server ▪ ErMapper, Envi	
Aplikasi yang dikembangkan	• Memiliki Web Server API (Response JSON/XML) • *Single Sign On* • Harus dapat diakses pada semua browser yang bisa digunakan oleh masyarakat luas, antara lain Internet Explorer, Mozilla Firefox, Chrome, Opera, Safari , dll • Dapat diakses pada perangkat (*gadget*) yang umum digunakan, antara lain komputer tablet, *smartphone*, dll		
• Pada *server* tersedia FTP (*File Transfer Protocol*), GD2 (*Graphics Draw*), FFMPEG (*Video*) • Pusdatin menyediakan pusat data (*data center*) untuk penempatan (*hosting*) *website* internal Kementerian dan aplikasinya • Pusdatin akan melakukan pengujian terhadap portal *web* (*website*) yang dikembangkan oleh masing-masing Unit Organisasi			

6. PENATAAN KONTEN

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

Mengacu pada Undang Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik dan Keputusan Menteri Pekerjaan Umum Nomor 391/KPTS/M/2011 tentang Penetapan Klasifikasi Informasi, konten yang wajib tersedia di portal *web* (*website*) Kementerian dan Unit Organisasi lainnya adalah sebagai berikut:

6.1 Profil Kementerian atau Unit Organisasi, dengan sub konten sebagai berikut :

6.1.1 Sejarah

6.1.2 Tugas dan Fungsi

6.1.3 Struktur Organisasi (bagan)

6.1.4 Info Pejabat

6.1.5 Lokasi Kantor

6.2 Organisasi, berisikan tautan ke unit-unit di bawahnya, baik Struktural maupun Fungsional.

6.3 Produk, menjelaskan produk dari masing-masing Unit Organisasi dan Unit Kerja seperti :

6.3.1 Renstra,

6.3.2 Kebijakan/Strategi,

6.3.3 Rencana program,

6.3.4 Pengelolaan anggaran (DIPA, RKAKL, ringkasan laporan keuangan, lakip, dll),

6.3.5 Peraturan perundang-undangan,

6.3.6 Info kepegawaian (SDM),

6.3.7 SNI/Pedoman,

6.3.8 NSPK/SPM,

6.3.9 Data statistik,

6.3.10 Pemetaan/GIS,

6.3.11 Kamus/istilah (*Glossary*),

6.3.12 Katalog,

6.3.13 Aplikasi,

6.3.14 Teknologi Terapan,

6.3.15 Jasa layanan,

6.3.16 Iklan layanan masyarakat,

6.3.17 Spesifikasi,

6.3.18 Ilmu pengetahuan dan teknologi, dan lain-lain.

6.4 Publikasi, merupakan sarana dalam penyampaian informasi seperti :

6.4.1 Majalah,

6.4.2 Buletin,

6.4.3 Jurnal,

6.4.4 Artikel/guntingan berita,

6.4.5 Buku ilmiah, dan lain-lain

6.5 Berita, merupakan sarana penayangan berita kegiatan seperti Berita Terkini, Berita Terkait, dan Berita Terpopuler.

6.6 Galeri, merupakan media untuk menayangkan Foto dan Video.

6.7 Layanan Informasi Publik, merupakan wadah bagi saran dan pengaduan serta layanan informasi publik yang dikoordinasi oleh Pejabat Pengelola Informasi dan Dokumentasi (PPID).

6.8 Layanan Pengadaan Secara Elektronik (LPSE) Kementerian, merupakan layanan pengadaan barang dan jasa.

6.9 Agenda kegiatan, merupakan kegiatan rutin yang dilaksanakan setiap tahun atau peristiwa (*event*) besar lainnya seperti Seminar, Kolokium, dll.

6.10 Fasilitas/dukungan, merupakan sarana untuk menayangkan pelayanan jasa seperti laboratorium, perpustakaan, sumber daya manusia, dukungan teknis.

6.11 Selain konten yang tersebut di atas, hal lain yang perlu disiapkan pada portal *web* (*website*) yang dibangun oleh masing-masing Unit Organisasi adalah sebagai berikut :

6.11.1 Navigasi kembali ke portal *web* (*website*) Kementerian dan ke portal *web* (*website*) Unit Organisasi;

6.11.2 Peta situs (*Site Map*);

6.11.3 Fasilitas pencari;

6.11.4 Kontak berupa alamat, nomor telepon, dan surat elektronik;

6.11.5 Catatan kaki (*footer*);

6.11.6 Hak Cipta;

6.11.7 Fasilitas dua Bahasa (Bahasa Indonesia dan Bahasa Inggris).

7. PENENTUAN TATA LETAK (*LAYOUT*)

7.1 Menentukan tata letak (*layout*) secara proporsional sesuai dengan kaidah estetika pada penempatan elemen-elemennya;

7.2 Menyesuaikan dengan resolusi layar yang biasa digunakan oleh pengguna (minimal resolusi 1024 x 768 piksel);

7.3 Menyertakan kontras bentuk, ukuran, posisi, warna dan huruf;

7.4 Menggunakan tekstur yang halus dan tidak kompleks untuk latar belakang;

7.5 Secara umum tata letak (*layout*) untuk portal *web* (*website*) Kementerian terdiri dari beberapa bagian utama, yaitu :

7.5.1 Navigasi untuk kembali ke halaman utama portal *web* (*website*) Kementerian;

7.5.2 Tajuk (*header*) utama sebagai identitas unit organisasi;

7.5.3 Navigasi utama yang telah dikelompokkan;

7.5.4 Berita utama kelembagaan (20-30% dari seluruh konten portal *web* (*website*));

7.5.5 Menu pendukung lainnya;

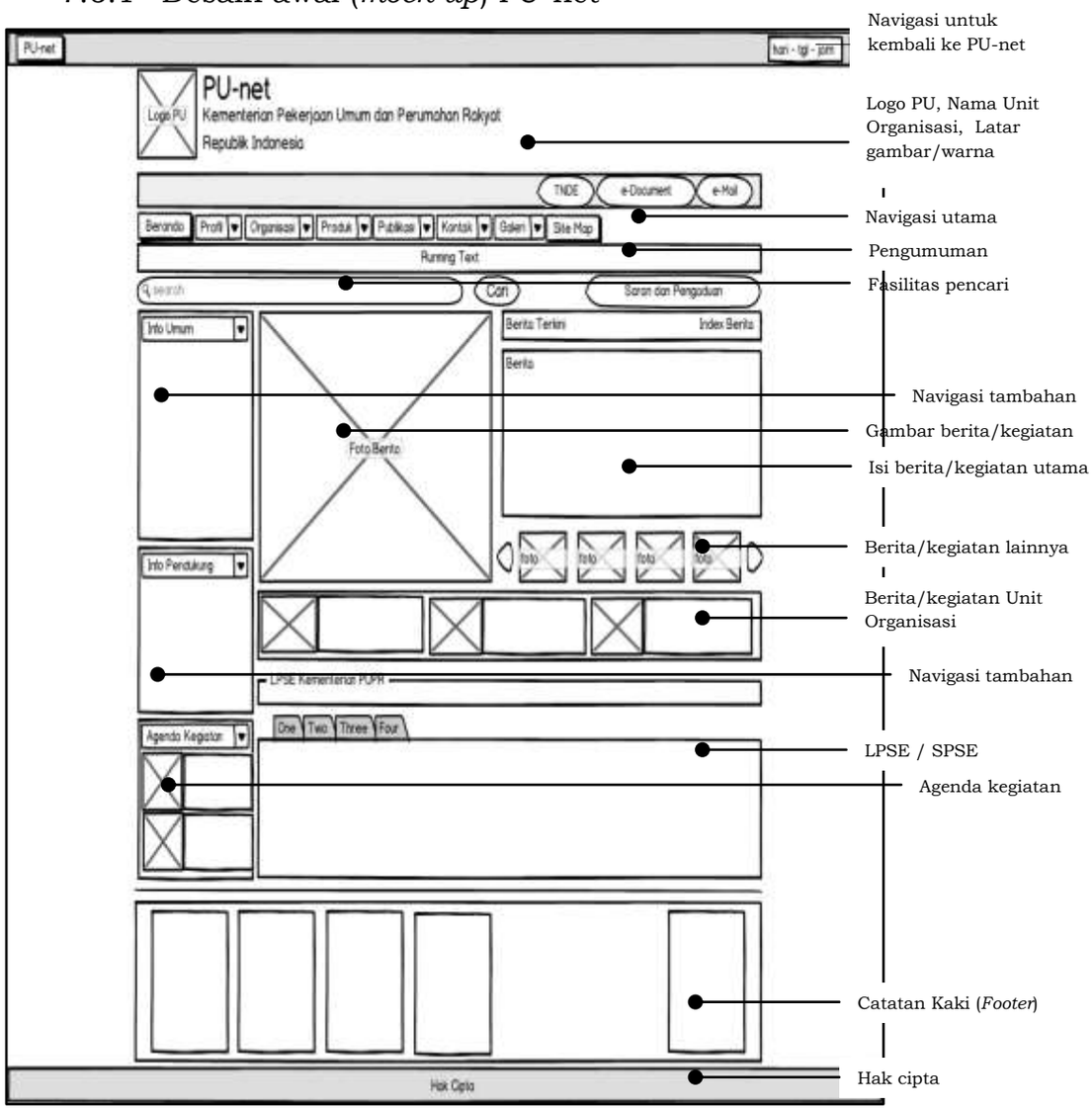
7.5.6 Catatan kaki (*footer*);

7.5.7 Hak cipta;

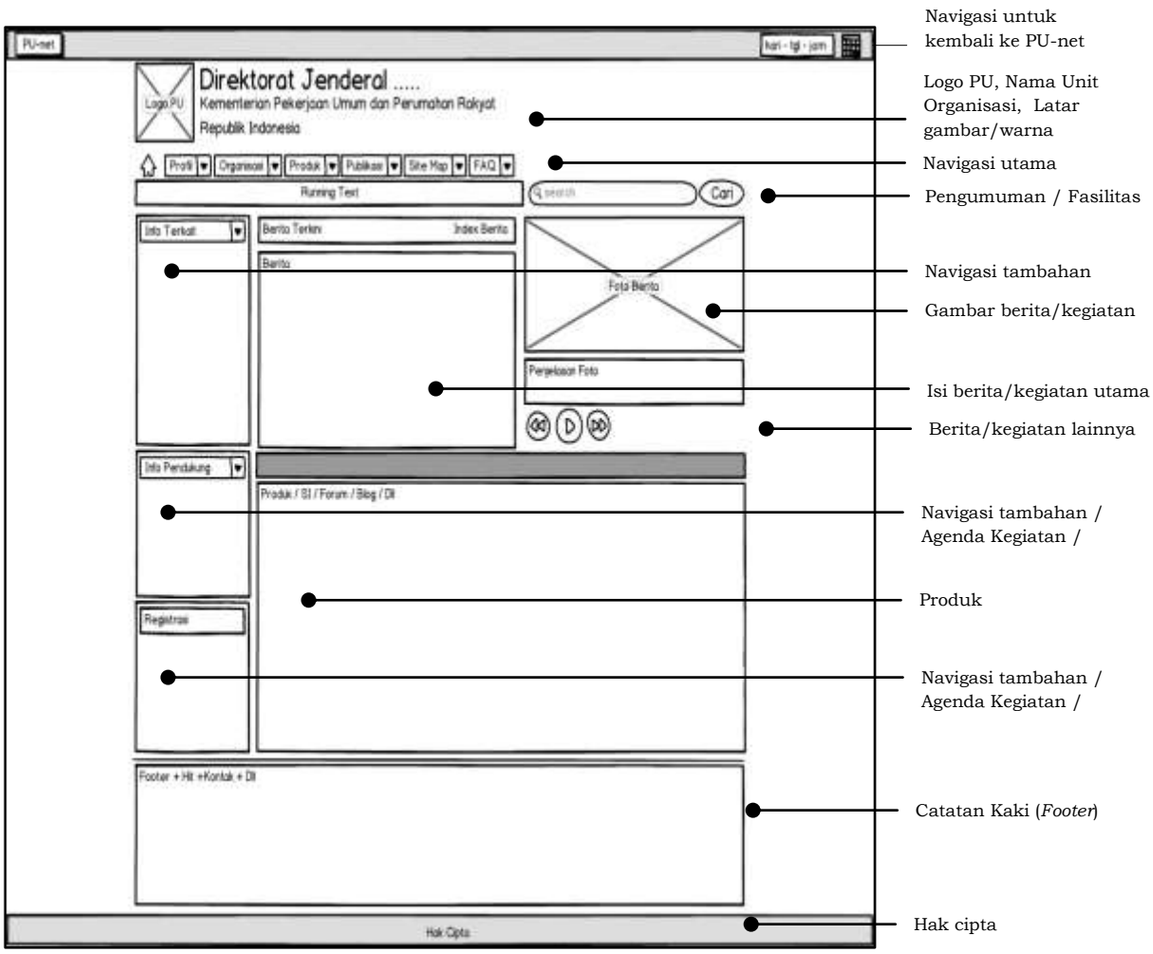
7.5.8 Fasilitas dua Bahasa (Bahasa Indonesia dan Bahasa Inggris).

7.6 Desain awal (*mock-up*) yang dibuat untuk lebih jelasnya dapat dilihat sebagai berikut :

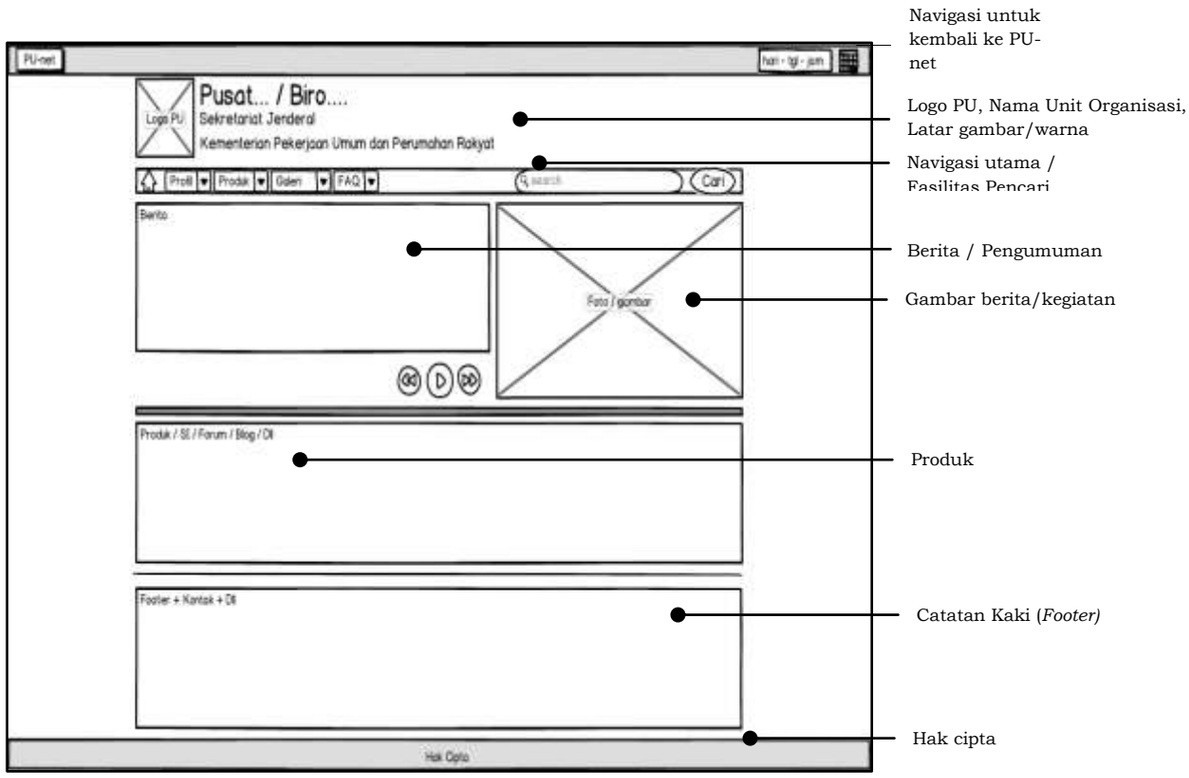
7.6.1 Desain awal (*mock-up*) PU-net



7.6.2 Desain awal (*mock-up*) Portal *Web* (*Website*) Unit Organisasi



7.6.3 Desain Awal (*Mock-up*) Portal *Web* (*Website*) Unit Kerja



8. PENATAAN TAYANGAN

Standardisasi tayangan dalam pembuatan dan pengembangan portal *web* (*website*) Kementerian diharapkan dapat menjadi acuan bagi seluruh portal *web* (*website*) Unit Organisasi dan Unit Kerja di Kementerian.

8.1 Penentuan warna

8.1.1 Menentukan warna dengan kombinasi yang serasi dan sesuai dengan identitas Kementerian.

8.1.2 Tidak menggunakan kombinasi warna yang menyebabkan tulisan sulit terbaca.

8.1.3 Menggunakan maksimum 4 warna dasar yang mendukung, jika membutuhkan warna lainnya, menggunakan turunan warna dari warna-warna yang telah dipilih.

8.2 Penggunaan huruf

8.2.1 Tidak menggunakan huruf yang harus diunduh dulu, gunakan huruf standar yang terdapat pada semua peramban (*browser*).

8.2.2 Tidak menggunakan jenis huruf terlalu banyak, pilih jenis huruf yang mudah dibaca.

8.2.3 Tidak menggunakan huruf kapital terlalu banyak.

8.2.4 Tidak memberi garis bawah tulisan.

8.2.5 Mengatur jarak spasi antar baris dan jarak spasi antar huruf.

8.2.6 Membuat kombinasi kontras yang jelas antara huruf dan latar belakang atau antara huruf dan gambar.

8.2.7 Penggunaan huruf yang tidak standar harus dalam bentuk grafis agar bisa ditampilkan seragam di semua peramban (*browser*).

8.3 Penggunaan gambar, suara, dan video

8.3.1 Menggunakan gambar tipe GIF, JPG, dan PNG.

8.3.2 Menggunakan suara tipe MP3 dan WAV.

8.3.3 Menggunakan video tipe FLV, AVI, MPEG, dan MP4.

8.3.4 Gambar harus sesuai dengan artikel yang ditayangkan.

8.3.5 Peletakan gambar, suara, dan video harus proporsional dengan ketajaman yang cukup dan dimensi tidak terlalu besar.

8.3.6 Ukuran file gambar, suara, dan video dikoordinasikan dengan Pusdatin.

8.3.7 Menggunakan atribut “alt” dalam tag “img src” agar muncul keterangan dari gambar yang tidak bisa tayang

8.4 Penggunaan bahasa

8.4.1 Menggunakan bahasa dan istilah yang mudah dimengerti.

8.4.2 Menggunakan simbol sebagai pengganti bahasa.

8.4.3 Tidak membuat narasi yang terlalu panjang.

8.5 Ketentuan lain

8.5.1 Merancang menu navigasi utama yang mudah ditemukan.

8.5.2 Meletakkan alamat kontak dengan jelas.

8.5.3 Mencantumkan peta situs (*site map*) di halaman depan.

8.5.4 Menyiapkan tautan sesuai dengan informasi yang ada.

MENTERI PEKERJAAN UMUM DAN
PERUMAHAN RAKYAT REPUBLIK INDONESIA,

ttd

M. BASUKI HADIMULJONO

Salinan sesuai dengan aslinya
KEMENTERIAN PEKERJAAN UMUM DAN
PERUMAHAN RAKYAT
Kepala Biro Hukum,

Siti Martini
NIP. 195803311984122001

LAMPIRAN VI
PERATURAN MENTERI PEKERJAAN UMUM
DAN PERUMAHAN RAKYAT REPUBLIK INDONESIA
NOMOR 17/PRT/M/2016
TENTANG
PENYELENGGARAAN TEKNOLOGI INFORMASI DAN KOMUNIKASI DI KEMENTERIAN PEKERJAAN UMUM DAN PERUMAHAN RAKYAT

TATA KELOLA PORTAL *WEB*

1. UMUM

Tata kelola portal *web* merupakan kebijakan terkait dalam penyelenggaraan portal *web* (*website*) khususnya pengelolaan portal *web* (*website*) di Kementerian baik Unit Organisasi atau Unit Kerja. Tata kelola ini untuk dijadikan sebagai pedoman bagi pengelola portal *web* (*website*) di Kementerian agar mudah dalam melakukan koordinasi dan komunikasi.

Standar ini berlaku bagi seluruh pengelola portal *web* (*website*) yang dilaksanakan oleh seluruh unit organisasi di Kementerian.

2. RUANG LINGKUP

Ruang lingkup dari tata kelola portal *web* (*website*) meliputi penetapan penanggung jawab pengelola portal *web* (*website*) dan konten pada Unit Organisasi dan Unit Kerja di Kementerian.

3. KEBIJAKAN

3.1 Setiap Pimpinan Unit Organisasi bertanggung jawab dalam memantau dan mengawasi pembuatan dan pengembangan portal *web* (*website*) di Unit Organisasi masing-masing.

3.2 Setiap Pimpinan Unit Organisasi bertanggung jawab dan mengetahui terhadap penambahan dan perubahan portal *web* (*website*) di Unit

Organisasi masing-masing, dalam hal ini meliputi penambahan, perubahan dan penghapusan portal *web* (*website*).

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

4. TANGGUNG JAWAB

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

4.1 Penanggung jawab portal *web* (*website*) adalah Unit Organisasi di lingkungan Kementerian.

4.2 Penanggung jawab portal *web* (*website*) harus melakukan pemutakhiran konten portal *web* (*website*) secara rutin atau setiap ada perubahan pada kontennya.

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

4.4 Pengguna adalah publik baik eksternal maupun internal Kementerian.

5. PLATFORM *WEBSITE*

5.1 Penyelenggara *website*

Pemeliharaan infrastruktur portal *web* (*website*) Kementerian dilakukan secara berkelanjutan dan melibatkan seluruh unit organisasi di Kementerian dan lebih diperkuat melalui "Kerabat *Website*".

Penyediaan jaringan teknologi informasi dan komunikasi di Kementerian disiapkan dan dikelola oleh Pusdatin dengan didukung oleh seluruh Unit Organisasi dan Unit Kerja. Pemanfaatan jaringan teknologi informasi dan komunikasi ini dilaksanakan di seluruh Unit Organisasi Kementerian yang tersebar di seluruh wilayah Indonesia.

Secara umum pengelolaan infrastruktur jaringan teknologi informasi dan komunikasi dan portal *web* (*website*) Kementerian melibatkan antara lain:

5.1.1 Pusdatin

1) Penanggungjawab jaringan teknologi informasi dan komunikasi portal *web* (*website*) Kementerian dan Unit Organisasi
2) Penanggung jawab sistem portal *web* (*website*) Kementerian (PU-net)
3) Penanggung jawab sistem portal *web* (*website*) Setjen Kementerian
4) Pengelola tayangan:
   a) Pengumuman
   b) Agenda kegiatan Kementerian
   c) Tayangan informasi Kementerian di luar berita dan publikasi
   d) Kontributor konten portal *web* (*website*) Kementerian

5.1.2 Biro Komunikasi Publik

1) Penanggungjawab konten portal *web* (*website*) Kementerian (PU-net):
   a) Berita utama Kementerian
   b) Galeri foto dan video Kementerian
   c) Saran dan Pengaduan
   d) Layanan Informasi Publik
   e) Pelayanan Publik
2) Penanggungjawab konten portal *web* (*website*) Setjen:
   a) Berita Setjen Kementerian
   b) Galeri foto dan video Setjen Kementerian
   c) Kontributor konten lainnya

5.1.3 Unit Organisasi

1) Penanggung jawab sistem portal *web* (*website*) Unit Organisasi
2) Penanggung jawab berita dan konten portal *web* (*website*) Unit Organisasi
3) Kontributor konten portal *web* (*website*) Kementerian

5.1.4 Unit Kerja

1) Penanggung jawab sistem portal *web* (*website*) Unit Kerja
2) Penanggung jawab berita dan konten portal *web* (*website*) Unit Kerja
3) Kontributor konten portal *web* (*website*) Kementerian

5.1.5 Unit Pelaksana Teknis Setingkat Eselon III

1) Kontributor konten portal *web* (*website*) Unit Kerja

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

5.2 Matriks tugas dan tanggung jawab pemeliharaan portal *web* (*website*) Kementerian

		Tugas	Pelaksana
Top Level Management and *Policy maker* / Pembuat kebijakan			
1.	Pengelola *web* utama (*Webmaster*)	Menentukan kebijakan, mengelola dan menjaga portal *web* (*website*)	Pusdatin
2.	Administrator *web* (*Web Administrator*)	Proses manajemen	Pusdatin, Penanggung jawab portal *web* (*website*) Unit Organisasi, dan Unit Kerja
3	Administrator Konten (*Content Administrator*)	Penentuan kebijakan konten	Biro Komunikasi Publik
Content Management / Pengelola konten *web*			
4.	Penulis (*Author*)	Membangun konten portal *web* (*website*)	Pusdatin, Biro Komunikasi Publik, Penanggungjawab portal

			web (*website*) Unit Organisasi, dan Unit Kerja
5.	Penyunting (*Editor*)	Merawat konten portal *web* (*website*)	Biro Komunikasi Publik Penanggungjawab portal *web* (*website*) Unit Organisasi dan Unit Kerja
Web Development / Pengembang *website*			
6	Pengembang *web* (*Web Developer*)	Membangun portal *web* (*website*)	
a.	Arsitek *web* (*Web Architect*)	Desain portal *web* (*website*)	Pusdatin, Biro Komunikasi Publik, Penanggungjawab portal *web* (*website*) Unit Organisasi, dan Unit Kerja
b.	Pemogram *web* (*Web Programmer*)	Membuat aplikasi	Pusdatin, Penanggungjawab portal *web* (*website*) Unit Organisasi, dan Unit Kerja
c.	Administrator Basis Data (*Database Administrator*)	Merancang basis data (*database*) aplikasi	Pusdatin, Penanggungjawab portal *web* (*website*) Unit Organisasi, dan Unit Kerja
d.	Desainer grafis/ Desainer multimedia (*Graphic Designer/ Multimedia Designer*)	Membuat grafis, gambar, tipografi, animasi, dan multimedia	Pusdatin, Biro Komunikasi Publik, Penanggungjawab portal *web* (*website*) Unit Organisasi, dan Unit Kerja

5.2.1 Pengelola *web* utama (*webmaster*)

Pengelola *web* utama (w*ebmaster*) bertanggung jawab sebagai berikut:

1. Merencanakan, mengembangkan, mengelola, dan mengevaluasi portal *web* (*website*) secara berkelanjutan.
2. Menyusun Prosedur Operasional Standar Pengelolaan portal *web* (*website*),
3. Menetapkan persyaratan teknis portal *web* (*website*),
4. Menentukan situs terkait,
5. Memberikan pelayanan dan perawatan yang berkaitan dengan portal *web* (*website*),

5.2.2 Administrator *web* (*web Administrator*)

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

1. Membantu *webmaster* dalam merencanakan, mengembangkan, mengelola, dan mengevaluasi portal *web* (*website*) secara berkelanjutan serta menyusun Prosedur Operasional Standar,
2. Mengelola hak akses pengguna ke portal *web* (*website*),
3. Melakukan koordinasi dengan Unit Organisasi dan Unit Kerja terkait dalam pengelolaan portal *web* (*website*),
4. Melakukan cadangan (*back up*) sistem dan data.

5.2.3 Administrator konten (*content administrator*)

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

1. Membuat, menyiapkan, dan mengelola konten baru untuk setiap unit organisasi dan unit kerja,
2. Menyusun Prosedur Operasional Standar penyusunan konten portal *web* (*website*).

5.2.4 Penulis (*author*)

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

5.2.5 Penyunting (*editor*)

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

5.2.6 Pengembang *web* (*web developer*)

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

1. Merencanakan dan membangun dalam pengembangan portal *web* (*website*).
2. Membuat Petunjuk Teknis Penggunaan portal *web* (*website*).

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

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

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

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

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

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

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

5.2.6.c Administrator basis data (*database administrator*)

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

5.2.6.dDesainer Grafis/Desainer Multimedia (*Graphic Designer/Multimedia Designer*)

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

5.3 Pengelola Portal *Web* (*Website*) Kementerian

Susunan dan tugas pokok serta fungsi pengelola portal *web* (*website*) Kementerian ditetapkan oleh Menteri.

MENTERI PEKERJAAN UMUM DAN
PERUMAHAN RAKYAT REPUBLIK INDONESIA,

ttd

M. BASUKI HADIMULJONO

Salinan sesuai dengan aslinya
KEMENTERIAN PEKERJAAN UMUM DAN
PERUMAHAN RAKYAT
Kepala Biro Hukum,

Siti Martini
NIP. 195803311984122001