

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 perundang-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