LAMPIRAN
NOMOR : SE-16/PJ/2011
TENTANG : PEDOMAN PENGAMANAN PERANGKAT DAN FASILITAS PENGOLAHAN DATA DAN INFORMASI

Pedoman Pengaman Perangkat dan Fasilitas Pengolahan Data dan Informasi

Direktorat Jenderal Pajak
Kementerian Keuangan Republik Indonesia

versi 1.0

Klasifikasi : TERBATAS
Tanggal (Tanggal Terbit)

LEMBAR PENGENDALIAN

NO	Penerima Dokumen	Format Dokumen
1	Direktorat TTKI	Cetakan
2	Direktorat TIP	Cetakan
3	Direktorat KITSDA	Cetakan
4	Direktorat TPB	Cetakan
5	PPDDP	Cetakan
6	Pegawai DJP	Elektronik

Klasifikasi : TERBATAS

HALAMAN REVISI

Bab / Sub-Bab	Halaman	Revisi	Tanggal	Uraian Revisi
		Ver 1.0	Feb 2011	

Klasifikasi : TERBATAS

DAFTAR ISI

A Deskripsi

Pedoman Pengamanan Perangkat dan Fasilitas Pengolahan Data dan Informasi disusun dengan tujuan untuk memberikan panduan dan aturan dalam mengamankan perangkat komputer dan fasilitas pendukungnya milik DJP yang digunakan oleh seluruh unit kerja DJP, ruang *server* di KPP, Kanwil dan PPDDP, dan secara khusus mengamankan fasilitas fisik *Data Center* yang berada di unit kerja Teknologi Informasi dan Komunikasi (TIK) dari dampak lingkungan, bencana atau intervensi, serta penyalahgunaan akses oleh pihak yang berwenang maupun yang tidak berwenang. Pedoman ini berlaku bagi seluruh pegawai DJP, tamu, dan pihak ketiga lainnya.

Hal-hal yang diatur dalam Pedoman Pengamanan Perangkat dan Fasilitas Pengolahan Data dan Informasi adalah :

1. Pengamanan perangkat komputer di seluruh Unit Kerja DJP.
2. Pengamanan ruang server di KPP, Kanwil, dan PPDDP.
3. Pengamanan *Data Center*, yang meliputi :
   a. Lingkungan *Data Center* ,
   b. Konstruksi fisik *Data Center*,
   c. Pengamanan perangkat komputer *Data Center*,
   d. Fasilitas pendukung *Data Center*,
   e. Akses ke dalam *Data Center*,
   f. Pengamanan di dalam *Data Center*,
   g. Pengamanan koneksi perangkat ke *Data Center*, dan
   h. Pengendalian operasional dan layanan.
4. Pengamanan removable media.

B. Acuan

1. ISO/IEC 27001 : 2005 : Anex 9 - Keamanan Fisik.
2. ANSI/TIA - 942 : Telecommunications Infrastructure Standard for Data Center.

C. Dokumen Terkait

1. Kebijakan Pengelolaan Keamanan Informasi DJP.
2. Kebijakan Pengelolaan Layanan TIK DJP.

D. Pengamanan Perangkat Komputer di seluruh Unit Kerja DJP

1. Ketentuan Umum
   1.1. Perangkat komputer harus digunakan sebaik-baiknya sebagaimana fungsinya dan sesuai dengan petunjuk manualnya untuk alasan kebersihan, keamanan, serta untuk kepentingan penggunaan jangka panjang.
   1.2. Pengguna aset informasi dilarang membuka/membongkar perangkat komputer seperti CPU, *monitor, keyboard, mouse,* dan lain-lain.
   1.3. Perangkat komputer yang berisikan informasi rahasia dan sangat rahasia harus diberi *password* dengan mengacu pada Pedoman Penggunaan *User Account/Password*, Pengamanan *Log-On* Ke Dalam Fasilitas Teknologi Informasi, Penggunaan Fasilitas *E-Mail*, serta Akses *Internet* dan *intranet*.
   1.4. Pengguna aset informasi bertanggung jawab untuk menjaga kerahasiaan informasi yang dipercayakan kepadanya, mencegah terjadinya kerusakan pada perangkat komputer, dan mematuhi kebijakan dan prosedur pengelolaan keamanan informasi yang berlaku.
   1.5. Pemilik aset informasi bertanggung jawab menjaga keamanan informasi miliknya dan menjamin bahwa aset informasi serta sistem pengamanannya tersedia, terawat dan berfungsi dengan baik.
   1.6. Perangkat komputer harus dirawat, dipelihara, diperiksa dan diuji secara berkala, dilakukan hanya oleh petugas/pegawai yang berwenang, dan mempunyai kompetensi teknis yang sesuai untuk menjamin ketersediaan, keutuhan (integrity), dan fungsi perangkat komputer misalnya Administrator Sistem atau *Operator Console* (OC).
   1.7. Pimpinan unit kerja bertanggungjawab memastikan ketersediaan fasilitas pendukung perangkat komputer.
   1.8. Dalam hal ketersediaan perangkat komputer, permintaan dan perencanaan perangkat komputer mengacu pada Pedoman Pengembangan Aplikasi dan Infrastruktur Teknologi Informasi dan Komunikasi (TIK).

2. Di Dalam Lokasi Kantor DJP
   2.1. Posisi layar (*monitor*) komputer harus diatur penempatannya dan dibatasi arah sudut pandangnya sehingga mengurangi risiko informasi dilihat secara langsung oleh pihak yang tidak berkepentingan.
   2.2. Layar (*monitor*) PC dan *Notebook* harus menggunakan *screensaver* dan tidak boleh ditinggalkan dalam keadaan tidak terkunci (*ter-password*).
   2.3. Perangkat komputer harus ditempatkan di titik/lokasi yang aman, diposisikan sedemikian rupa, mudah diawasi untuk mengurangi risiko aset informasi dapat diakses oleh pihak yang tidak berwenang dan terhindar dari dampak lingkungan seperti panas/sinar matahari, air, kelembaban, debu, sampah, dan lain-lain yang berpotensi merusak perangkat komputer tersebut.
   2.4. Perangkat pengolah informasi termasuk mesin faksimili, *printer* atau komputer yang digunakan untuk memproses informasi rahasia dan sangat rahasia harus ditempatkan di lokasi yang aman dan tidak dilewati/dilalui oleh tamu atau pihak ketiga lainnya yang tidak berwenang, untuk mencegah kebocoran informasi tersebut ke pihak yang tidak berwenang.
   2.5. Semua perangkat pengolah informasi yang menyimpan informasi penting dan rawan yang

dikelola DJP harus ditempatkan di lokasi yang terpisah dari area publik untuk mencegah akses pihak yang tidak berwenang, seperti ruang arsip atau ruang *server* dan lain-lain.

2.6. Semua perangkat dan fasilitas pengolahan data dan informasi harus mendapatkan pasokan daya yang sesuai dengan spesifikasi yang disyaratkan oleh pabrikan perangkat. Untuk setiap lokasi kerja termasuk ruang *server* dan *Data Center* harus tersedia pasokan listrik yang cukup untuk beban maksimal seluruh perangkat, termasuk fasilitas atau perangkat pendukung yang ada di lokasi tersebut.

2.7. Kantor, ruangan, dan fasilitas yang berisikan informasi rahasia dan sangat rahasia harus memiliki pengamanan fisik yang memadai. Sebagai contoh, pintu dan jendelanya harus dikunci jika ditinggalkan.

2.8. Akses keluar masuk ruangan yang berisikan aset informasi yang bersifat rahasia dan sangat rahasia harus dibatasi dan hanya diberikan kepada pegawai yang berwenang mengelola aset informasi tersebut.

3. Di Luar Lokasi Kantor DJP

3.1. Perangkat komputer tidak boleh digunakan untuk kepentingan pribadi pada saat di luar lokasi kantor DJP.

3.2. Pada saat kegiatan-kegiatan *rapat/seminar/workshop/training* ataupun pada saat bermalam di fasilitas penginapan/hotel, perangkat komputer harus dalam kondisi terjaga/di bawah pengawasan pengguna aset informasi. Apabila dimungkinkan, perangkat komputer harus disimpan dalam lemari besi atau lemari terkunci.

3.3. Selama dalam perjalanan, perangkat komputer harus selalu dalam kondisi terjaga/di bawah pengawasan dan tidak boleh ditinggalkan di dalam transportasi umum atau kendaraan lainnya ataupun di tempat/area publik/umum lainnya.

3.4. Apabila perangkat komputer akan dibawa keluar lokasi kantor DJP untuk keperluan perbaikan/perawatan dan/atau keperluan lainnya yang menunjang kedinasan DJP, tehadap data yang bersifat kritikal atau sangat rahasia dan rahasia yang tersimpan dalam perangkat tersebut harus dipindahkan terlebih dahulu dan diamankan sehingga tidak dapat diakses oleh pihak yang tidak berwenang.

3.5. Aktivitas yang dilakukan oleh pegawai untuk melakukan pekerjaan dari suatu tempat di luar lokasi kantor DJP dengan menggunakan teknologi komunikasi, misalnya internet, sehingga mendapatkan tingkatan akses yang sama dengan pada saat bekerja di lokasi kantor (melalui *intranet*) harus dilakukan dengan mengacu pada Pedoman *Teleworking*.

3.6. Pengguna aset informasi dapat membawa perangkat komputer ke luar lokasi kantor DJP dalam hal mendapatkan perintah untuk bertugas di luar lokasi kantor DJP, memiliki kebutuhan pemakaian perangkat komputer, dan telah mendapatkan persetujuan dari pejabat terkait. Tata cara pengendalian penggunaan perangkat komputer ke luar lokasi kantor DJP harus dilakukan dengan mengacu pada Pedoman Pengelolaan Aset Informasi.

E. Pengamanan Ruang *Server* di KPP, Kanwil, dan PPDDP

1. Lingkungan Ruang *Server*

1.1. Lokasi ruang *server* harus berada dalam lingkungan yang aksesnya terbatas untuk publik (*restricted area*), mudah diawasi, aman dari bahaya genangan air/banjir dan tidak boleh berada di bawah kamar mandi atau tempat penampungan air.

1.2. Lokasi ruang *server* tidak boleh dicantumkan pada papan nama atau papan petunjuk.

1.3. Ruangan *server* harus tertutup dan dinding ruangan harus terbuat dari material yang tidak dapat dilihat dari luar, misal dari kaca.

1.4. Lokasi di sekitar ruangan server harus diberikan penerangan yang memadai, dan alat penerangan darurat yang dapat mencangkup seluruh area ruang *server*.

1.5. Pada lokasi ruang *server* harus tersedia alarm api dan asap, alat pengukur suhu dan kelembaban, serta perangkat pengawasan video/gambar.

1.6. Pemadam api berbasis air yang digunakan di gedung tidak boleh digunakan di lingkunagan ruangan *server*.

1.7. Pegawai dan pihak ketiga tidak diizinkan makan, minum, merokok, dan membawa bahan-bahan material berbahaya seperti bahan radioaktif, bahan yang mudah terbakar, perangkat *electro-magnetic* yang dapat berinterferensi dengan komputer dan perangkat telekomunikasi, serta bahan-bahan material berbahaya lainnya ke dalam ruang *server*.

1.8. Akses keluar masuk ruang *server* harus dibatasi dan hanya diberikan kepada petugas yang berwenang mengelola *server* tersebut seperti *Administrator Sistem* atau *Operator Console* (OC).

1.9. Setiap orang selain petugas *server* yang berwenang, yang memerlukan akses ke ruang *server* harus didampingi oleh petugas *server* yang berwenang dan diwajibkan mengisi buku *log* (daftar pengunjung ruang *server*).

1.10. Ruang server tidak boleh digunakan untuk ruang kerja.

1.11. Ruang *server* tidak boleh digunakan sebagai tempat penyimpanan berkas, perangkat rusak/*idle*, serta barang-barang tidak terpakai yang tidak semestinya berada di ruang *server*.

1.12 Untuk menjamin kelayakan sirkulasi udara, tinggi ruang yang tersedia untuk penempatan rak komputer minimal 2,5 (dua koma lima) meter.

2. Pengamanan Perangkat Komputer Ruang *Server*

2.1. Seluruh perangkat dan fasilitas pengolahan data dan informasi seperti perangkat *server, storage, printer, routers, switches,* jaringan kabel, dan sebagainya yang ada dalam ruang *server*, harus ditempatkan di area yang hanya bisa diakses oleh petugas yang berwenang.

2.2. Komputer di ruang *server* tidak boleh digunakan sebagai sarana untuk *log-on* pegawai lain tanpa izin khusus dari Kepala Seksi Pengolahan Data dan Informasi di KPP, Kepala Bidang Dukungan Teknis dan Konsultasi di Kanwil, atau Kepala Bidang Pemindaian Dokumen dan Perekaman Data di PPDDP.

2.3. Setiap kabel jaringan harus diberi label yang sesuai dan jelas dan diatur untuk memudahkan penanganan kesalahan.

2.4. Jaringan kabel data harus dipisahkan dari jaringan kabel listrik dengan jarak minimal 3 (tiga)

meter untuk menghindari dampak radiasi (elektromagnet). Dalam hal ruang *server* terdapat *raised floor*, maka jaringan kabel data harus berada di dalam jalur khusus yang menggantung di atas plafon ruang *server* dan dipisahkan dari jaringan kabel listrik yang harus berada di bawah *raised floor*.

2.5. Pimpinan unit kerja bertanggung jawab untuk memastikan ketersediaan perangkat komputer di ruang *server* beserta perawatan, pemeliharaan, pemeriksaan dan penggujian secara berkala untuk menjamin ketersediaan, keutuhan (*integrity*), dan fungsi seluruh perangkat dan fasilitas pengolahan data dan informasi di ruang *server* dibuktikan dengan bukti rekaman kegiatan beserta *checklist*.

2.6. Perawatan, pemeliharaan, pemeriksaan, dan pengujian secara berkala seluruh perangkat dan fasilitas pengolahan data dan informasi di ruang *server* dilakukan hanya oleh petugas/pegawai yang berwenang, dan mempunyai kompetensi teknis yang sesuai misalnya Administrator Sistem atau *Operator Console* (OC).

3. Fasilitas Pendukung Ruang *Server*

3.1. Pada lokasi ruang server harus tersedia fasilitas *Uninterruptible Power Supply (UPS)* yang mempunyai kapasitas yang cukup untuk memberikan pasokan listrik selama minimal 15 (lima belas) menit kepada semua perangkat komputer yang ada dalam ruang *server* pada saat sumber listrik ke ruang *server* mengalami gangguan.

3.2. Selain perangkat dan fasilitas pengolahan data dan informasi tidak boleh dihubungkan ke perangkat *Uninterruptible Power Supply (UPS)*.

3.3. Pada lokasi ruang server harus tersedia generator listrik dengan fungsi pengaturan pasokan daya otomatis dengan kapasitas yang cukup untuk keseluruhan perangkat komputer dan fasilitas pendukungnya, seperti *server, router, printer, Air Conditioning System* , dan lainnya yang ada di ruang *server*.

3.4. Fasilitas *Air Conditioning System* yang ada harus mempunyai kapasitas yang sesuai dengan volume ruang *server*, termasuk beban panas yang dihasilkan perangkat komputer maupun jaringan, dengan aliran udara yang baik dan tetap dapat beroperasi ketika aliran listrik utama padam. Suhu udara di ruang server diatur dalam batas 20^0 - 25^0 C dengan kelembaban relatif antara 40 - 55%.

3.5. Fasilitas pemadam api yang tersedia harus mampu memadamkan api dalam waktu kurang dari 2 (dua) menit.

3.6. Fasilitas pemadam api harus menggunakan gas yang tidak merusak perangkat ataupun membahayakan manusia.

3.7. Pimpinan unit kerja bertanggung jawab untuk memastikan ketersediaan fasilitas pendukung di ruang *server* beserta perawatan, pemeliharaan, pemeriksaan dan pengujian secara berkala untuk ketersediaan, keutuhan (*integrity*), dan fungsi seluruh perangkat dan fasilitas pengolahan data dan informasi di ruang *server* yang dapat dibuktikan dengan rekaman kegiatan beserta *cheklist.*

F. Pengamanan *Data Center* di Unit Kerja TIK

1. Lingkungan *Data Center*

1.1. Lokasi *Data Center* harus berada dalam lingkungan yang aksesnya terbatas untuk publik (*restricted area*) serta mudah diawasi keamanan dan kebersihannya.

1.2. Lokasi *Data Center* tidak boleh dicantumkan pada papan nama atau papan petunjuk yang ada di lokasi DJP tersebut.

1.3. Untuk masuk ke dalam bangunan *Data Center* diperlukan kode akses masuk tertentu, misalnya dengan menggunakan *biometric scanner* atau *access card*.

1.4. Lokasi *Data Center* tidak boleh di lantai dasar dan tidak boleh berada di bawah kamar mandi atau tempat penampungan air.

1.5. Lokasi di sekitar *Data Center* harus diberikan penerangan yang memadai, dan alat penerangan darurat yang dapat mencakup seluruh area *Data Center*.

1.6. Pemadam api berbasis air yang digunakan di gedung tidak boleh digunakan di lingkungan *Data Center.*

1.7. *Data Center* harus memiliki alat/sistem komunikasi yang baik, minimal terdapat satu pesawat telepon untuk masing-masing area di lingkungan *Data Center.*

2. Konstruksi Fisik Data Center

2.1. Ruangan *Data Center* memiliki area sesuai aktivitas yang dapat dilakukan dalam area tersebut. Setiap area memiliki identitas dan tingkat kewenangan/otorisasi yang diperlukan bagi pengguna aset informasi yang akan mengakses *Data Center* sebagai berikut :

2.1.1. Area *staging* : area untuk membuka kemasan hardware dan pre-installed software sebelum dipindahkan ke area *server*;

2.1.2. Area *operator* : area yang dilengkapi *console* untuk akses *server* secara *remote* tanpa harus memasuki area *server*;

2.1.3. Area *Server* : area *Data Center* utama dan hanya petugas yang berwenang saja yang dapat mengakses area ini;

2.1.4. Area *library* : area untuk menyimpan media *backup*; dan

2.1.5. Area *network* : area untuk menyimpan perangkat-perangkat utama jaringan.

2.2. Keseluruhan konstruksi fisik *Data Center*, termasuk penggunaan *raised floor* harus sesuai dengan penggunaan beban struktural yang ada, termasuk beban keseluruhan fasilitas pendukung.

2.3. *Raised floor* harus menggunakan bahan yang tahan api.

2.4. Untuk menjamin kelayakan sirkulasi udara, tinggi ruang minimal yang tersedia untuk penempatan rak komputer, di luar tinggi *raised floor* dan langit-langit, adalah 2,5 (dua koma lima) meter.

2.5. Konstruksi dinding dan pintu *Data Center* harus tahan terhadap upaya perusakan fisik tanpa bantuan peralatan berat, dan konstruksi bangunan harus tahan gempa.

2.6. Dinding dan pintu *Data Center* harus menggunakan material atau rancangan konstruksi yang mampu menahan dampak api selama 2 (dua) jam.

2.7. Dinding *Data Center* tidak boleh terbuat dari kaca, untuk alasan keamanan dan untuk mengurangi dampak panas matahari yang dapat mempengaruhi suhu ruangan.

2.8. Keseluruhan area *server* harus dalam kondisi kedap udara dan memiliki katup pengaman yang digunakan untuk mengeluarkan gas pemadam api, setelah proses pemadaman selesai, jika terjadi kebakaran.

2.9. Penerapan fasilitas perlindungan petir harus dipasang untuk semua jalur komunikasi dan listrik.

3. Pengamanan Perangkat komputer *Data Center*

3.1. Seluruh perangkat dan fasilitas pengolahan data dan informasi di *Data Center* seperti perangkat *sever, storage, patch panel, core routers, core switches*, jaringan kabel, *firewall*, dan sebagainya yang ada dalam ruang *Data Center*, harus ditempatkan di area yang hanya bisa diakses oleh petugas yang berwenang.

3.2. Penempatan seluruh perangkat dan fasilitas pengolahan data dan informasi di lokasi *Data Center* harus terlindungi dari dampak lingkungan/polusi, dan memiliki aliran udara (ventilasi), suhu, serta kelembaban yang sesuai dengan batas minimum dan batas maksimum operasional perangkat yang disyaratkan oleh pabrikan.

3.3. Lemari/*rack server* harus memiliki ventilasi yang cukup untuk mengeluarkan suhu panas yang dihasilkan dari perangkat dan fasilitas pengolahan data dan informasi yang berada di dalam lemari/*rack server* tersebut.

3.4. Posisi dan penempatan lemari/*rack server* harus diatur sebaik mungkin, sisi depannya berhadapan satu sama lain, dan antar lemari/*rack server* diberi jarak yang cukup, sehingga suhu panas yang dihasilkan tidak saling mengganggu antar perangkat dan fasilitas pengolahan data dan informasi yang ada di lemari/*rack* lainnya.

3.5. Pada lokasi *Data Center* harus memiliki *Data Center Monitoring System* yang mampu melakukan pemantauan dan memberikan notifikasi apabila terjadi sesuatu di *Data Center*. *Data Center Monitoring System* memiliki 3 (tiga) bagian utama :

a) *Environmental Monitoring System* : perangkat ini akan memonitor terhadap lingkungan *Data Center* yang mungkin menjadi ancaman, mulai dari abnormal suhu dan kelembaban ruangan, genangan air, asap, masalah listrik utama, masalah pendingin udara, akses kontrol, dan lain-lain;

b) *Network Monitoring System* : perangkat ini akan memonitor pada hampir seluruh perangkat dan fasilitas pengolahan data dan informasi di *Data Center*, seperti *server, router, storage device*, akses kontrol, dan lain-lain;

c) *Message Center* : perangkat ini akan mengirim notifikasi terhadap gangguan sistem kepada petugas *Data Center*.

3.6. Setiap kabel jaringan harus diberi label yang sesuai dan jelas untuk memudahkan penanganan kesalahan.

3.7. Jaringan kabel data harus berada di dalam jalur khusus yang menggantung di atas plafon ruang data center dan dipisahkan dari jaringan kabel listrik yang harus berada di bawah *raised floor* dengan jarak yang cukup untuk menghindari dampak radiasi (elektromagnet).

4. Fasilitas Pendukung Data Center

4.1. Pada lokasi *Data Center* harus tersedia alarm api dan asap, alat pengukur suhu dan kelembaban, perangkat pengawasan video/gambar, dan alat penerangan darurat yang dapat mencakup seluruh area.

4.2. Pasokan listrik bagi seluruh perangkat komputer, jaringan, dan sistem pendukungnya harus tersedia dari sumber yang memadai, dengan tegangan dan daya yang sesuai/cukup untuk beban maksimum penggunaan *Data Center*.

4.3. Pasokan listrik yang digunakan *Data Center* harus berasal dari sumber yang berbeda atau menggunakan jalur yang berbeda dari yang digunakan gedung.

4.4. Pada lokasi Data Center harus tersedia generator listrik dengan fungsi pengaturan pasokan daya otomatis dengan kapasitas yang cukup untuk keseluruhan perangkat komputer dan fasilitas pendukungnya dalam *Data Center*.

4.5. Fasilitas *Uninterruptible Power Supply (UPS)* harus mempunyai kapasitas yang cukup untuk memberikan pasokan listrik selama minimal 15 (lima belas) menit kepada semua perangkat komputer yang ada dalam area *server*.

4.6. Fasilitas pengatur suhu dan kelembaban serta pemadam api harus menggunakan jalur dan instalasi kabel listrik yang berbeda dari yang digunakan perangkat komputer.

4.7. Fasilitas pengatur suhu dan kelembaban *(Air Conditioning System)* yang ada harus mempunyai kapasitas yang sesuai dengan volume ruang *Data Center*, termasuk beban panas yang dihasilkan perangkat komputer maupun jaringan, dan dengan aliran udara yang baik. Suhu udara di dalam lokasi Data Center diatur dalam batas 18^0 - 20^0 C dengan kelembaban relatif antara 40 - 55%.

4.8. Fasilitas pemadam api yang tersedia harus mampu memadamkan api dalam waktu kurang dari 2 (dua) menit.

4.9. Fasilitas pemadam api harus menggunakan gas yang tidak merusak perangkat ataupun membahayakan manusia.

4.10. Pada lokasi *Data Center* harus tersedia perangkat sensor kebocoran air (*Water leak detector*) yang dapat mendeteksi dan memberikan peringatan ketika ada kebocoran air di lokasi *Data Center*.

5. Akses ke dalam *Data Center*

5.1. Pintu masuk ke *Data Center* harus dipasangi kunci elektronik.

5.2. Petugas *Data Center* yang memasuki lokasi *Data Center* harus memastikan bahwa setiap pintu tertutup/terkunci dengan benar setelah masuk/keluar ruang *Data Center*.

5.3. Setiap orang selain petugas *Data Center* yang memerlukan akses ke *Data Center* harus didampingi sepanjang waktu oleh petugas *Data Center* yang berwenang dan diwajibkan mengisi buku *log* (daftar pengunjung *Data Center*).

5.4. Setiap orang yang masuk ke *Data Center* harus melepas sepatu atau menggunakan selimut sepatu yang telah disediakan serta menyimpan semua barang-barang bawaannya di lemari

penitipan.

5.5. Setiap orang selain petugas *Data Center* yang akan mengakses *server Data Center* harus mendapatkan izin dari petugas *Data Center* dan diwajibkan menggunakan peralatan yang telah disediakan oleh *Data Center*, kecuali di *Data Center* tidak tersedia peralatan tersebut, dan harus atas seizin petugas *Data Center*.

5.6. Akses pengguna aset informasi ke *Data Center* harus direviu secara periodik, paling sedikit setiap 6 (enam) bulan sekali oleh Pejabat Keamanan Informasi DJP.

5.7. Hasil reviu akses pengguna akses informasi harus didokumentasikan dan apabila ditemukan pelanggaran atau ketidakpatuhan terhadap Kebijakan Pengelolaan Keamanan Informasi DJP harus ditindaklanjuti dengan ketentuan yang berlaku.

6. Pengamanan di dalam *Data Center*

6.1. Selama berada di ruang *Data Center*, siapapun dilarang membawa bahan-bahan atau material yang dapat membahayakan keamanan dan mengganggu kenyamanan lingkungan *Data Center*. Yang termasuk ke dalam bahan-bahan atau material tersebut antara lain :

6.1.1. makanan atau minuman;

6.1.2. rokok atau tembakau;

6.1.3. senjata api dan senjata tajam ;

6.1.4. bahan yang mudah terbakar;

6.1.5. bahan radioaktif;

6.1.6. perangkat electro-magnetic yang dapat berinterferensi dengan komputer dan perangkat telekomunikasi; atau

6.1.7. kamera atau perekam video dan audio.

6.2. Setiap lemari/rack yang ada dalam *Data Center* harus dalam keadaan terkunci. Penyimpanan kunci harus dikelola oleh *Petugas Data Center.*

6.3. Perangkat yang dipasang dalam *Data Center* harus memenuhi standar infrastruktur yang ditetapkan pabrik atau telah menjadi *best-practice*.

6.4. Jika terdapat perangkat yang memerlukan konfigurasi sebelum instalasi maka proses ini harus dilakukan di area *staging* yang berada di luar area *server.*

7. Pengamanan Koneksi Perangkat ke *Data Center*

7.1. Koneksi setiap perangkat ke infrastruktur *Data Center* hanya boleh dilakukan dengan menggunakan IP *address* dan *hostname* yang dialokasikan oleh petugas *Data Center*.

7.2. Kepala Subdirektorat Pemantauan Sistem dan Infrastruktur harus memastikan bahwa penggunaan perangkat yang dikoneksikan ke infrastruktur *Data Center* telah mematuhi Kebijakan Pengelolaan Keamanan Informasi DJP.

7.3. Kepala Subdirektorat Pemantauan Sistem dan Infrastruktur berhak menghentikan atau memutus akses fisik atau lojik dari perangkat yang dikoneksikan ke infrastruktur *Data Center* tanpa pemberitahuan terlebih dahulu bila terdapat akses yang tidak terotorisasi atau ditemukan indikasi pelanggaran kebijakan yang berlaku.

7.4. Akses dengan tingkat administrator ke *server* dan perangkat jaringan utama (*core network*) tidak boleh dilakukan secara *remote* dari dalam maupun dari luar *Data Center* dan hanya boleh dilakukan dari area *operator* di *Data Center*.

7.5. Komputer di area operator tidak boleh digunakan sebagai sarana untuk *log-on* pegawai yang tidak berwenang kecuali dengan izin khusus dari Pejabat Keamanan Informasi KPDJP.

8. Pengendalian Operasional dan Layanan

8.1. Perawatan (*Maintenance*) Perawatan

8.1.1. Lingkungan fisik di sekitar *Data Center* untuk melindungi dari bahaya kebakaran, kebocoran air hujan, atau pengaruh lingkungan lainnya;

8.1.2. Instalasi kabel listrik *Data Center* berikut pengatur distribusinya dan *Circuit Breaker* untuk memastikan kondisi kelayakan dan deteksi kerusakan;

8.1.3. Instalasi perangkat penangkal petir dan *grounding* termasuk pengukuran untuk memastikan kelayakannya;

8.1.4. *Uninterruptible power supply (UPS)* termasuk cadangan batere untuk melindungi sistem dari fluktuasi sumber daya listrik PLN dan generator listrik;

8.1.5. Perangkat generator listrik berikut persediaan bahan bakar dan instalasi kabel yang tersambung ke jalur distribusi *Data Center* dan *Circuit Breaker*;

8.1.6. Fasilitas pemadam api utama *Data Center* mencakup ketersediaan dan tekanan gas, kebersihan katup, dan kondisi kelayakan perangkat elektronik terkait;

8.1.7. Perangkat pemadam api jinjing (APAR-Alat Pemadam Api Ringan);

8.1.8. Alarm deteksi api dan asap, termasuk kebersihan dan pemeriksaan batere (apabila digunakan);

8.1.9. Kondisi *Raised Floor* dan kebersihan ruang/rongga di bawah untuk penempatan jalur kabel komunikasi, kabel sumber daya listrik, dan/atau jalur saluran lainnya dalam *Data Center;*

8.1.10. Fasilitas pengatur lingkungan (*Environmental Control System atau Air Conditioning System*);

8.1.11. Perangkat sensor kebocoran air (*Water leak detector*);

8.1.12. Kondisi suhu, kelembaban, dan penerangan;

8.1.13. Kunci pintu *Data Center* dan alarm yang digunakan untuk memonitor kondisi terkuncinya/tertutupnya pintu; dan

8.1.14. kamera gambar/video.

8.2. Inventarisasi Aset Informasi *Data Center*

8.2.1. Inventarisasi aset *Data Center* dilakukan oleh Subdit Pemantauan Sistem dan Infrastruktur, dengan parameter inventarisasi sesuai dengan definisi *Configuration Management Database* (*CMDB*) dan mengacu pada Kebijakan Pengelolaan Layanan TIK DJP.

8.2.2. Setiap catatan perubahan terhadap aset *Data Center* harus dilakukan dengan

mengacu pada Pedoman Pengelolaan Aset dan Konfigurasi Layanan TIK.

8.3. Kesiapan Personil

8.3.1. Setiap pegawai DJP dan mitra atau pihak ketiga yang ditugaskan untuk mengelola dan merawat *Data Center* harus diberikan pemahaman mengenai Kebijakan pengelolaan Keamanan Informasi DJP.

8.3.2. Setiap pegawai DJP dan mitra yang ditugaskan untuk mengelola dan merawat *Data Center* harus mendapatkan pelatihan yang cukup untuk mengoperasikan peralatan pendukung di dalam *Data Center* khususnya alat pemadam api, pengatur suhu/kelembaban, dan perangkat kode akses pada pintu *Data Center*.

G. Pengamanan *Removable Media*

1. Proteksi Data

1.1. Transfer data dari dan ke dalam perangkat dan fasilitas pengolahan data dan informasi DJP dengan menggunakan *removable media* hanya boleh digunakan oleh pegawai DJP.

1.2. Data atau informasi dengan klasifikasi SANGAT RAHASIA atau RAHASIA yang tersimpan di *removable media* harus segera dihapus setelah tidak diperlukan.

1.3. *File* yang tidak dikenal asal-usulnya yang berasal dari *removable media* tidak boleh di buka sebelum di-*scan* dengan *antivirus*.

2. Penanganan *Removable Media* di *Data Center*

2.1. Petugas *Data Center* secara default menonaktifkan konfigurasi port *USB* untuk penggunaan *removable media* pada semua perangkat *server*.

2.2. Otorisasi pengaktifan konfigurasi port *USB* untuk pemakaian *removable media* di *Data Center* diberikan oleh Pejabat Keamanan Informasi DJP. Otorisasi ini bersifat sementara dan harus berdasarkan atas keperluan yang bersifat sangat penting.

H. Daftar Istilah

1. **Administrator Sistem** adalah pegawai DJP yang ditunjuk untuk mengelola, melakukan pemeliharaan, dan pengawasan tehadap sistem TIK serta bertanggung jawab terhadap integritas data, efisiensi, dan kinerja dari sistem TIK.
2. **Aset Informasi** adalah segala seuatu yang memmpunyai nilai bagi DJP.
3. **Circuit breaker** adalah suatu peralatan pemutus rangkaian listrik pada suatu sistem tenaga listrik, yang mampu untuk membuka dan menutup rangkaian listrik pada semua kondisi, termasuk arus hubungan singkat, sesuai dengan ratingnya. Juga pada kondisi tegangan yang normal ataupun tidak normal.
4. **Configuration Management Database (CMDB)** adalah logical data repository yang menyimpan informasi mengenai aset TIK, hubungan antar aset TIK, dan seluruh informasi yang diperlukan serta menunjang proses pengelolaan seluruh Layanan TIK.
5. **Data Center** adalah sarana fisik yang digunakan untuk menempatkan perangkat-perangkat layanan TIK secara terpusat.
6. **Data Center Monitoring System** adalah *tools* untuk menjaga ketersediaan fungsi TIK secara keseluruhan. Tools ini akan mencatat dan menginformasikan dengan akurat insiden atau kejadian sekecil apapun yang terjadi di *Data Center*.
7. **Fasilitas pendukung** adalah sarana dan fasilitas pendukung berupa perangkat teknologi informasi atau elektronik untuk melancarkan fungsi perangkat pengolah informasi, seperti *Uninterruptible Power Supply* (*UPS*), generator listrik, perangkat pengawasan video/gambar, alat penerangan darurat, pengatur suhu dan kelembaban (*Air Conditioning System*), fasilitas pemadam api, alarm api dan asap, perangkat sensor kebocoran air (*Water leak detector*), dan lain-lain.
8. **Log Book** adalah sebuah catatan data atau kegiatan untuk merekam kejadian berdasarkan urutan waktu sebagai bahan pendukung pengambilan keputusan.
9. **Log-on** adalah proses untuk mendapatkan hak akses menggunakan sumber daya sistem (komputer/jaringan/aplikasi), dengan memasukkan identitas dari pengguna dan kata sandi (*password*).
10. **Lokasi kantor DJP** adalah gedung/kantor DJP tempat aset informasi milik DJP dialokasikan.
11. **Operator Console (CO)** adalah pegawai DJP yang bertanggung jawab sebagai administrator sistem/aplikasi perpajakan di Kantor Wilayah atau Kantor Pelayanan Pajak di lingkungan DJP.
12. **Password** adalah kata rahasia atau rangkaian karakter yang digunakan dalam proses autentikasi untuk membuktikan identitas pengguna atau untuk mendapatkan hak akses terhadap fasilitas teknologi informasi.
13. **Pejabat keamanan informasi** adalah pejabat Eselon II yang ditunjuk untuk setiap Direktorat, Kantor Wilayah dan Pusat Pengolahan Data dan Dokumen Perpajakan oleh Direktur Jenderal Pajak dalam rangka mengkoordinasikan dan mengarahkan kegiatan penerapan kebijakan dan prosedur pengelolaan keamanan informasi di lingkungan tempat dia ditugaskan.
14. **Petugas Data Center** adalah pegawai Subdit Pemantauan Sistem dan Infrastruktur Direktorat TIP yang diberikan tanggung jawab untuk melakukan pengelolaan infrastruktur dan operasional *Data Center.*
15. **Pemilik aset informasi** adalah pimpinan unit kerja DJP di mana data atau informasi perpajakan dibuat, atau pihak yang secara hukum ditunjuk sebagai penanggung jawab aset informasi atau proses kerja di DJP.
16. **Pengguna aset informasi** adalah pegawai DJP atau pihak ketiga yang menggunakan perangkat dan fasilitas pengolahan data dan informasi milik DJP.
17. **Perangkat dan fasilitas pengolahan data dan informasi** adalah seluruh perangkat komputer atau sistem komunikasi elektronik lainnya milik DJP yang digunakan oleh pegawai DJP untuk mendukung pekerjaan beserta fasilitas pendukungnya, seperti perangkat komputer/*server, router, storage device*, *switch*, jaringan kabel, sistem operasi, *Data Center Monitoring System*, UPS, dan lain-lain yang terdapat di seluruh unit kerja DJP termasuk *Data Center* dan ruang *server.*
18. **Perangkat Komputer** adalah perangkat TIK dan elektronik yang digunakan oleh pegawai DJP atau pihak ketiga milik DJP untuk mendukung pekerjaan, yang terdiri dari perangkat keras TIK dan perangkat lunak TIK, seperti CPU, *monitor, keyboard, mouse,* PC, *notebook, printer*, sistem operasi,

dan lain-lain

19. **Pihak ketiga** adalah pihak penyedia barang/jasa yang menjadi mitra DJP, kementerian/instansi lain terkait, dan pihak ketiga lainnya.
20. ***Port USB (Universal Serial Bus)*** adalah port berkecepatan tinggi yang memiliki interkoneksi yang universal yang memungkinkan kita untuk menghubungkan alat eksternal (*peripheral*) seperti *removable media* ke dalam komputer secara *plug and play* sehingga tidak perlu melakukan *booting* ulang komputer.
21. ***Raised floor*** adalah satu area lantai yang ditinggikan 10-50 cm dari lantai dasar, umumnya dibuat dari lembar baja, dengan materi konstruksi terisi semen padat kelas ringan yang kuat, dan dapat distruktur ulang. Dia antara lorong *raised floor* dapat digunakan untuk penempatan berbagai kabel, meliputi kabel elektrik, data, telekomunikasi/suara, pengaturan sirkulasi kontrol suhu ruang, serta dapat menghilangkan arus listrik liar di berbagai peralatan elektronik.
22. ***Remote*** adalah cara untuk mengakses suatu sistem tanpa bersinggungan secara langsung dengan sistem tersebut.
23. ***Removable media*** adalah media penyimpan data elektronik yang dapat dipindahkan dan tidak terpasang secara permanen pada komputer, misal *compact disc, DVD, memory stick,USB drive, floopy disk*, dan sebagainya.
24. ***Router*** adalah sebuah alat jaringan komputer yang mengirimkan paket data melalui sebuah jaringan atau internet menuju tujuannya melalui proses *routing* dan berfungsi sebagai penghubung antar dua atau lebih jaringan untuk meneruskan data dari satu jaringan ke jaringan lainnya.
25. **Ruang *Server*** adalah sarana fisik yang digunakan untuk menempatkan perangkat-perangkat *server, router, switch*, dan UPS yang berada di KPP, Kanwil, PPDDP, atau di lingkungan Kantor Pusat DJP.
26. ***Screensaver*** adalah gambar bergerak atau pola gambar tertentu yang muncul di layar monitor ketika mouse atau keyboard komputer tidak digunakan dalam beberapa waktu yang ditentukan.
27. ***Teleworking*** adalah suatu aktifitas yang dilakukan oleh pegawai untuk melakukan pekerjaan dari suatu tempat di luar lokasi kantor resmi dengan menggunakan teknologi komunikasi, misalnya internet, sehingga mendapatkan tingkatan akses yang sama dengan pada saat bekerja di lokasi kantor (melaui intranet).
28. **Unit Kerja TIK** adalah Direktorat Teknologi Informasi Perpajakan (TIP) dan Direktorat Transformasi Teknologi Informasi dan Komunikasi (TTKI).
29. ***Uninterruptible Power Supply (UPS)*** adalah perangkat untuk menyuplai tenaga listrik temporer yang langsung memberi pasokan tenaga listrik ketika sumber tenaga listrik utama (contoh dari PLN) terhenti atau padam.