

LAMPIRAN
SURAT EDARAN DIREKTUR JENDERAL PAJAK
NOMOR : SE-61/PJ/2011
TENTANG : PEDOMAN *TELEWORKING*



Pedom an Telew orking

Direktorat Jenderal Pajak
Kementerian Keuangan Republik Indonesia

Klasifikasi : TERBATAS

Tanggal : 9 Agustus 2011

LEMBAR PENGENDALIAN

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

DAFTAR ISI

A.	Deskripsi	1
B.	Acuan	1
C.	Dokumen Terkait	1
D.	Pedoman <i>Teleworking</i>	1 E.
	Definisi	3
LAMPIRAN I		4
LAMPIRAN II		6
LAMPIRAN III		8

A. Deskripsi

Pedoman *Teleworking* disusun dengan tujuan untuk mengamankan proses kerja pengolahan informasi Direktorat Jenderal Pajak (DJP) yang melibatkan lokasi kerja di luar lokasi unit kerja DJP dan untuk mengamankan ketersediaan suatu perangkat komputer ke jaringan milik DJP dari jarak jauh. Kegiatan *teleworking* yang diatur dalam pedoman ini adalah kegiatan *teleworking* yang dilakukan melalui *Virtual Private Network* (VPN) sebagai media ketersediaan perangkat di luar lokasi resmi DJP ke dalam jaringan milik DJP. Semua proses kerja yang dilakukan di suatu lokasi di luar area resmi DJP dengan menggunakan perangkat/infrastruktur milik DJP atau perangkat milik pribadi yang terhubung dari jarak jauh ke fasilitas milik DJP harus mematuhi pedoman ini.

B. Acuan

1. Peraturan Direktur Jenderal Pajak Nomor PER-41/PJ/2010 tentang Kebijakan Pengelolaan Keamanan Informasi Direktorat Jenderal Pajak
2. ISO/IEC 27001:2009 *Annex.11.72 Teleworking*
3. ISO/IEC 27002:2008 *Code of Practice for Information Security Management*

C. Dokumen Terkait

1. Pedoman Penggunaan *User Account/Password*, Pengamanan *Log-On* ke dalam Fasilitas Teknologi Informasi, Penggunaan Fasilitas *E-Mail*, serta Akses Internet dan Intranet
2. Pedoman Enkripsi dan *Key Management*

D. Pedoman *Teleworking*

1. Jenis kegiatan yang dapat dilakukan secara *teleworking* yaitu :
 - 1.2. Kegiatan yang bersifat insidental/bukan kegiatan rutin sehari-hari; dan
 - 1.3. Kegiatan yang memerlukan akses ke intranet DJP dalam jangka waktu tertentu;
2. Kegiatan yang dimaksud pada angka 1 misalnya sosialisasi, rapat, konsinyering, *visiting*, *benchmarking*, dan *workshop* di luar unit kerja DJP.
3. Setiap pegawai Direktorat Jenderal Pajak (DJP) yang akan melakukan kegiatan *teleworking* harus mendapatkan persetujuan dari atasan langsungnya dan Pejabat Keamanan Informasi pada unit kerja terkait yang didapatkan dengan cara mengisi Formulir Permohonan Melaksanakan Kegiatan *Teleworking* sebagaimana terdapat pada lampiran I pedoman ini.
4. Pejabat Keamanan Informasi melakukan kajian risiko keamanan informasi sebelum memberikan persetujuan terhadap permohonan pegawai yang akan melaksanakan kegiatan *teleworking* yang dituangkan ke dalam Formulir Hasil Kajian Risiko sebagaimana pada Lampiran II Pedoman ini.
5. Dalam hal unit kerja pegawai yang akan melaksanakan kegiatan *teleworking* bukan termasuk unit kerja Kantor Pusat DJP maka Formulir Permohonan Melaksanakan Kegiatan *Teleworking* dan Formulir Hasil Kajian Risiko yang telah disetujui oleh Pejabat Keamanan Informasi terkait dikirimkan ke Direktorat Teknologi Informasi Perpajakan (TIP) untuk disetujui oleh Pejabat Keamanan Informasi Kantor Pusat DJP.
6. Seksi Pemantauan Keamanan Sistem dan Jaringan Komunikasi Data, Direktorat TIP bertugas untuk :
 - 6.1. Memberikan *user account* VPN kepada pegawai yang akan melakukan kegiatan *teleworking*;
 - 6.2. Memantau penggunaan *user account* VPN. Dalam hal jangka waktu kegiatan *teleworking* sebagaimana tercantum dalam permohonan telah berakhir, maka *user account* tersebut harus segera dihapus atau dinonaktifkan;
 - 6.3. Memantau sistem jaringan yang digunakan untuk kegiatan *teleworking* untuk memastikan bahwa tidak ada akses yang tidak sah ke dalam sistem atau jaringan tersebut; dan
 - 6.4. Meneliti log kegiatan akses jaringan yang dilakukan oleh pengguna untuk memastikan bahwa pengguna menggunakan haknya sesuai dengan permohonan yang diajukan.
7. Sebelum memberikan *user account* VPN kepada pegawai yang akan melakukan kegiatan *teleworking*, Seksi Pemantauan Keamanan Sistem dan Jaringan Komunikasi Data, Direktorat TIP bertanggung jawab untuk menjelaskan penggunaan *user account* dan memberikan penjelasan mengenai pengamanan informasi pada saat bekerja di luar lokasi kantor sehingga dapat memahami risiko, ancaman, dan kelemahan keamanan informasi yang ada. Petunjuk, pelatihan, atau *briefing* dapat diberikan secara langsung atau melalui petunjuk/manual yang dikirimkan melalui *e-mail* DJP kepada pegawai yang akan melaksanakan *teleworking*.
8. Setiap pegawai yang melaksanakan kegiatan *teleworking* harus memahami dan mematuhi Kebijakan Keamanan Informasi DJP dan bertanggung jawab terhadap keamanan aset informasi milik DJP.
9. Setiap pegawai yang akan melaksanakan kegiatan *teleworking* harus memastikan bahwa aset informasi milik DJP dapat terjaga keamanannya di setiap lokasi kegiatan *teleworking*.
10. Tata cara pemberian izin melaksanakan kegiatan *teleworking* sebagaimana pada lampiran II pedoman ini.
11. Segala pelanggaran terhadap Pedoman *Teleworking* ini akan ditindaklanjuti dengan pengenaan hukuman disiplin sesuai dengan Peraturan Pemerintah tentang Disiplin Pegawai Negeri Sipil dan Peraturan Menteri Keuangan tentang Kode Etik Pegawai Direktorat Jenderal Pajak.

E. Definisi

1. **E-mail** atau **Electronic Mail** adalah fasilitas surat menyurat melalui jalur komunikasi elektronik baik internet maupun intranet. Setiap pengguna yang memiliki alamat *e-mail* dapat saling berkirim surat layaknya menggunakan kertas melalui kantor pos.
2. **Internet** adalah suatu jaringan komputer yang saling terhubung di seluruh dunia yang dapat saling bertukar data dengan menggunakan protokol standar TCP/IP. Internet terdiri dari berjuta-juta jaringan baik yang bersifat privat/pribadi maupun yang bersifat publik/terbuka yang dapat merupakan

- jaringan akademis, pemerintahan, bisnis, atau lainnya.
3. **Intranet** adalah sebuah jaringan privat yang menggunakan protokol TCP/IP seperti halnya internet yang digunakan untuk berbagi informasi secara aman di internal DJP. Dalam operasionalnya intranet dapat memanfaatkan internet untuk menyambungkan bagian-bagian antar lokasi kerja di DJP.
 4. **Pejabat Keamanan Informasi** adalah pejabat setingkat Eselon III yang ditunjuk oleh Direktur Jenderal Pajak untuk mengoordinasikan dan mengarahkan kegiatan penerapan kebijakan, pedoman, dan prosedur keamanan informasi di lingkungan unit eselon II dimana pejabat tersebut ditugaskan.
 5. **Petugas Keamanan Informasi** adalah pejabat setingkat Eselon IV yang ditunjuk oleh Direktur Jenderal Pajak untuk melaksanakan kegiatan penerapan kebijakan dan prosedur keamanan informasi di unit Eselon II dimana pejabat tersebut ditugaskan dan bekerja di bawah pengawasan dan pengarahan Pejabat Keamanan Informasi.
 6. **Teleworking** adalah suatu aktifitas yang dilakukan oleh pegawai untuk melakukan pekerjaan dari suatu tempat di luar lokasi unit kerja DJP dan tidak tersambung ke jaringan internal (intranet) DJP dengan menggunakan teknologi komunikasi sehingga mendapatkan tingkatan akses yang sama dengan pada saat bekerja di lokasi kantor (melalui intranet).
 7. **User Account** adalah identifikasi pengguna yang bersifat unik dan digunakan bersamaan dengan *password* ketika akan memasuki fasilitas teknologi informasi.
 8. **Virtual Private Network (VPN)** adalah jaringan komputer yang menggunakan infrastruktur telekomunikasi publik, misalnya internet, untuk menyediakan fasilitas akses yang aman kepada pengguna ke dalam jaringan komputer internal organisasi pengguna tersebut seperti layaknya pengguna berada dalam jaringan lokal organisasi tersebut.

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PAJAK



Gedung B Lantai 4 Telepon :
021-52904830
Jalan Gatot Subroto Kav. 40-42
021-5272723
Jakarta 12190

Faksimile :

Website : <http://www.pajak.go.id>

Formulir Permohonan Melaksanakan Kegiatan Teleworking
No : (1)

Nama : (2)
NIP : (3)
Unit Kerja : (4)
Jabatan : (5)
No Telepon (Kantor/HP) :/..... (6)
Alamat E-mail : (7)

Lokasi Kerja : (8)
Jenis Kegiatan : (9)
Aplikasi yang diakses : SIDJP Portal DJP Aplikasi lain di Portal DJP (sebutkan) : (10)
Jangka Waktu Akses : (.....) Jam /Hari* (11)
Dari s.d. (12)

Pernyataan :
Dengan menandatangani formulir ini,
1. Saya telah memahami dan akan mematuhi Kebijakan Pengelolaan Keamanan Informasi yang berlaku dalam penggunaan akses dan aset informasi yang diberikan oleh DJP.
2. Apabila dalam penggunaan akses/aset informasi ini saya melakukan tindakan yang melanggar kebijakan atau peraturan yang berlaku, saya bertanggung jawab sepenuhnya dan bersedia untuk menanggung segala kerugian yang timbul atau konsekuensi lainnya.

....., (14) Mengetahui,
Pemohon, (17),
(.....) (15) (.....) (18)
NIP (16) NIP (19)

Menyetujui,
..... (20)* (23)
(.....) (21)* (.....) (24)
NIP (22)* NIP (25)

Petunjuk Pengisian
Formulir Permohonan Melaksanakan Kegiatan *Te le w o r k i n g*

Data Pemohon

- (1) Diisi dengan nomor urut permohonan.
- (2) Diisi dengan nama lengkap pemohon.
- (3) Diisi dengan Nomor Induk Pegawai (NIP) pemohon.
- (4) Diisi dengan unit kerja pegawai pemohon, yaitu diisi dengan Unit Eselon III dan Unit Eselon II. Contoh : KPP Madya Tangerang, Kanwil DJP Banten.
- (5) Diisi dengan jabatan pegawai pemohon.
- (6) Diisi dengan nomor telepon kantor atau nomor *handphone* dari pegawai pemohon.
- (7) Diisi dengan alamat *e-mail* DJP pegawai pemohon.

Data Kegiatan

- (8) Diisi dengan nama tempat dan alamat lengkap lokasi kegiatan *teleworking* akan dilaksanakan.
- (9) Diisi dengan jenis kegiatan yang akan dilakukan, misalnya : sosialisasi, demo program, dan sebagainya.
- (10) Dipilih/diisi dengan nama aplikasi yang diakses.
- (11) Diisi dengan jumlah jam atau jumlah hari pelaksanaan kegiatan.
- (12) Diisi dengan tanggal pelaksanaan kegiatan.
- (13) Bila diperlukan, bagian ini dapat diisi dengan keterangan tambahan terkait permohonan kegiatan *teleworking*.

Surat Pernyataan

- (14) Diisi dengan tempat, dan tanggal permohonan.
- (15) Diisi dengan nama lengkap pemohon.
- (16) Diisi dengan NIP pemohon.
- (17) Diisi dengan jabatan dari atasan langsung pemohon.
- (18) Diisi dengan nama lengkap atasan langsung pemohon.
- (19) Diisi dengan NIP atasan langsung pemohon.

Persetujuan

- (20) Diisi dengan nama jabatan pejabat yang menyetujui permintaan akses yaitu Pejabat Keamanan Informasi setempat, contoh : Pejabat Keamanan Informasi Kanwil DJP Banten.
- (21) Diisi dengan nama lengkap Pejabat Keamanan Informasi setempat.
- (22) Diisi dengan NIP Pejabat Keamanan Informasi setempat.
- *) Keterangan : Poin no. 20 - 22 tidak perlu dicantumkan dalam hal unit kerja pemohon merupakan unit kerja Kantor Pusat DJP
- (23) Diisi dengan nama jabatan pejabat yang menyetujui permintaan akses di Kantor Pusat, yaitu Pejabat Keamanan Informasi Kantor Pusat DJP.
- (24) Diisi dengan nama lengkap Pejabat Keamanan Informasi Kantor Pusat DJP.
- (25) Diisi dengan NIP Pejabat Keamanan Informasi Kantor Pusat DJP.

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PAJAK



Gedung B Lantai 4 Telepon :
021-52904830
Jalan Gatot Subroto Kav. 40-42 Faksimile :
021-5272723
Jakarta 12190
Website : <http://www.pajak.go.id>

Hasil Kajian Risiko untuk Permintaan *Teleworking*
Atas Permintaan No : (1) Tgl : (2)

Aplikasi yang diakses : <input type="checkbox"/> SIDJP <input type="checkbox"/> Portal DJP <input type="checkbox"/> Aplikasi lain di Portal DJP sebutkan (3)	
Jenis Kegiatan : (4)	Lokasi Kegiatan : (5)
Jangka Waktu Akses : jam/hari*), tanggal : s.d. (6)	
Dampak yang terjadi apabila akses yang diperlukan untuk <i>teleworking</i> tidak tersedia : (7)	
Potensi risiko yang terjadi apabila akses untuk <i>teleworking</i> tersedia : (8)	
a. Terhadap keamanan data :	
b. Terhadap integritas data :	
c. Terhadap beban operasional :	
Dari kajian risiko di atas, kami merekomendasikan hal-hal berikut ini dalam pemberian akses untuk kegiatan <i>teleworking</i> : (9)	
....., (10)	
Menyetujui, (11),	Pembuat Kajian, (14),
(.....) (12) NIP (13)	(.....) (15) NIP (16)

Petunjuk Pengisian
Hasil Kajian Risiko untuk Permintaan *Teleworking*

- (1) Diisi dengan nomor Formulir Permohonan Melaksanakan Kegiatan *Teleworking* yang akan dibuatkan kajian risikonya oleh Administrator Sistem / Operator Console.
- (2) Diisi dengan tanggal permohonan dalam Formulir yang akan dibuat kajian risikonya oleh Administrator Sistem / Operator Console.

Aset

- (3) Diisi dengan nama aplikasi yang akan diakses atau dengan memberi tanda "v".

Pelaksanaan Kajian Risiko

- (4) Diisi dengan jenis kegiatan yang dilakukan pemohon.
- (5) Diisi dengan lokasi kegiatan yang dilaksanakan pemohon.
- (6) Diisi dengan jangka waktu akses yang dibutuhkan oleh pemohon.
- (7) Diisi dengan hasil kajian berupa dampak yang terjadi apabila akses tidak tersedia.
- (8) Diisi dengan potensi risiko yang terjadi apabila akses yang diperlukan untuk *teleworking* tersedia dari segi keamanan, integritas dan beban operasional.

Rekomendasi dan Persetujuan

- (9) Diisi dengan hal-hal yang bisa direkomendasikan berdasarkan kesimpulan hasil kajian risiko.
- (10) Diisi dengan tempat dan tanggal dimana kajian risiko dibuat.
- (11) Diisi dengan nama jabatan pejabat yang menyetujui hasil kajian risiko.
- (12) Diisi dengan nama lengkap pejabat yang menyetujui hasil kajian risiko.
- (13) Diisi dengan NIP pejabat yang menyetujui hasil kajian risiko.
- (14) Diisi dengan nama jabatan pembuat kajian risiko, contoh : *Operator Console*.
- (15) Diisi dengan nama lengkap pembuat kajian risiko.
- (16) Diisi dengan NIP pembuat kajian risiko.

TATA CARA PEMBERIAN IZIN MELAKSANAKAN KEGIATAN TELEWORKING

A. Pihak yang Terkait

1. Kepala Subdit Pemantauan Sistem dan Infrastruktur, Dit. TIP
2. Kepala Seksi Pemantauan Keamanan Sistem dan Jaringan Komunikasi Data, Dit. TIP
3. Pelaksana Seksi Pemantauan Keamanan Sistem dan Jaringan Komunikasi Data, Dit. TIP
4. Kasubdit/Kabid yang ditunjuk sebagai Pejabat Keamanan Informasi
5. Kasi yang ditunjuk sebagai Petugas Keamanan Informasi
6. OC/Adm inistrato r setem pat atau Pelaksana Dit. TIP
7. Pegawai DJP sebagai pemohon dan atasan langsungnya

B. Prosedur Kerja

1. Pegawai DJP yang akan melaksanakan kegiatan *teleworking* (pemohon) mengisi Formulir Permohonan Melaksanakan Kegiatan *Teleworking* dan menyampaikannya kepada atasan langsungnya.
2. Atasan langsung pemohon meneliti dan menandatangani Formulir Permohonan Melaksanakan Kegiatan *Teleworking* dan menyampaikannya kepada Pejabat Keamanan Informasi terkait.
3. Pejabat Keamanan Informasi menerima Formulir Permohonan Akses untuk Kegiatan *Teleworking* dan menugaskan kepada Petugas Keamanan Informasi untuk melakukan kajian risiko atas permohonan tersebut.
4. Petugas Keamanan Informasi menugaskan *Operator Console* (OC)/Administrator Sistem/Pelaksana Dit. TIP terkait untuk melakukan kajian risiko.
5. OC/Adm inistrato r Sistem/Pelaksana Dit. TIP terkait melakukan kajian risiko paling lama 1 hari kerja dan melaporkan hasilnya kepada Petugas Keamanan Informasi.
6. Petugas Keamanan Informasi melaporkan hasil kajian risiko kepada Pejabat Keamanan Informasi.
7. Dalam hal tidak terdapat risiko keamanan informasi atas pemberian fasilitas *teleworking*, Pejabat Keamanan Informasi menyetujui dan menandatangani Formulir Permohonan Melaksanakan Kegiatan *Teleworking* dan menyampaikannya kepada Pejabat Keamanan Informasi Kantor Pusat (KP) DJP dalam hal unit kerja pemohon bukan merupakan unit kerja KP DJP.
8. Pejabat Keamanan Informasi KP DJP menerima dan menandatangani Formulir Permohonan Melaksanakan Kegiatan *Teleworking*.
9. Pejabat Keamanan informasi KP DJP menugaskan Kepala Seksi Pemantauan Keamanan Sistem dan Jaringan Komunikasi Data untuk memberikan *user account* VPN beserta petunjuk penggunaan dan penjelasan pengamanan informasi kepada pemohon.
10. Kepala Seksi Pemantauan Sistem dan Jaringan Komunikasi Data menugaskan Pelaksana Seksi Pemantauan Keamanan Sistem dan Jaringan Komunikasi Data untuk menindaklanjuti.
11. Pelaksana Seksi Pemantauan Keamanan Sistem dan Jaringan Komunikasi Data melaksanakan tugas yaitu memberikan *user account* VPN beserta petunjuk penggunaan dan penjelasan pengamanan informasi kepada pemohon melalui email DJP dalam jangka waktu 1 hari kerja dan melaporkan kepada Kepala Seksi Pemantauan Keamanan Sistem dan Jaringan Komunikasi Data.
12. Salinan Formulir Permohonan Melaksanakan Kegiatan *Teleworking* dikirimkan kepada pemohon dan aslinya diarsipkan.
13. Proses selesai.

C. Bagan Arus (Flow chart)

