LAMPIRAN
SURAT EDARAN DIREKTUR JENDERAL PAJAK
NOMOR : SE-15/PJ/2011
TENTANG : PEDOMAN PENCEGAHAN *MALWARE*

Pedoman Pencegahan *Malware*

Direktorat Jenderal Pajak

Kementerian Keuangan Republik Indonesia

VERSI 1.0

KLASIFIKASI : TERBATAS

Tanggal : 9 Februari 2011

LEMBAR PENGENDALIAN

NO	Penerima Dokumen	Format Dokumen
1	Direktur Jenderal Pajak	Cetakan
2	Direktur TTKI	Cetakan
3	Direktur TIP	Cetakan
4	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 Pencegahan Malware dibuat dengan tujuan untuk menjadi pedoman bagi seluruh pegawai Direktorat Jenderal Pajak (DJP) dan pihak ketiga dalam upaya pencegahan terhadap bahaya *malware* serta melindungi perangkat dan aset informasi milik DJP.

Pedoman ini mendefinisikan peraturan anti malware yang antara lain meliputi :

1. Ketentuan umum dalam pencegahan dan penanganan *malware;* 2.
4. Pemantauan dan laporan dalam pencegahan dan penanganan *malware*.

B. Acuan

1. Kebijakan dan Standar Sistem Manajemen Keamanan Informasi di Lingkungan Kementerian Keuangan.
2. Kebijakan Pengelolaan Keamanan Informasi Direktorat Jenderal Pajak.
3. ISO/IEC 27002 : 2005 : Sub-klausul 10.4 - *Protection against melicious and mobile code*. 2.

C. Dokumen Terkait

1. Pedoman Backup dan Restore Sistem/Data/Informasi
2. Pedoman Penggunaan *User Account/Password* dan Pengamanan *Log-on* ke dalam Fasilitas Teknologi Informasi, Penggunaan Fasilitas *e-Mail*, serta Penggunaan Akses Internet dan Intranet
3. Pedoman Tindakan Perbaikan dan Pencegahan serta Pengelolaan Gangguan Keamanan Informasi
4. Pedoman Audit Internal Tata Kelola TIK

D. Pedoman

1. Ketentuan Umum

1.1. Untuk mel

1.2. Pelanggara
Pegawai Direktorat Jenderal Pajak.

2. Pencegahan *Malware*

2.1. Strategi pe

2.1.1. Penetapan

2.1.2. Pelaksanaa

2.1.3. Penggunaa

2.2. Tanggung Jawab dan Larangan Terkait Pencegahan *Malware*.

2.2.1. Seluruh Pe

2.2.1.1. Melakukan
informasi dan jaringan komunikasi data milik DJP.

2.2.1.2. Menyimpa

2.2.1.3. Mengundu

2.2.1.4. Melakukan

2.2.1.5. Mematuhi
Internet dan Intranet.

2.2.1.6. Segera me

2.2.1.7. *Meng-upda*

2.2.1.8. Segera me

2.2.2. Seluruh Pegawai DJP dilarang untuk :

2.2.2.1. Mengirim a

2.2.2.2. Menyalin,

2.2.2.3. Mengunjur

2.2.2.4. Mengubah

2.2.2.5. Menonakti

2.2.2.6. Membuka

2.2.3. Seluruh Pihak Ketiga harus :

2.2.3.1. Mematuhi

2.2.3.2. Membawa

2.2.3.3. Mengaktifk

2.2.4. Subdirektorat Analisis dan Evaluasi Sistem Informasi (AESI), Direktorat Transformasi Teknologi Komunikasi dan Informasi (TTKI) menetapkan dan memperbarui standar atau *baseline configuration* untuk perangkat jaringan komunikasi data.

2.3. Pelaksanaan Pelatihan dan *Awareness Program*

2.3.1. Ketua Tim Keamanan Informasi secara berkala mengkoordinasikan kegiatan pelatihan dan peningkatan kesadaran (*awareness*) terkait pencegahan malware bagi pegawai DJP.

2.3.2. Ketua Tim Keamanan Informasi mengusulkan rencana pelatihan terkait pencegahan dan penanganan *malware* kepada Sekretaris Direktorat Jenderal Pajak setiap tahun sekali dan mengoordinasikannya dengan Direktorat Kepatuhan Internal dan Transformasi Sumber Daya Aparatur (KITSDA).

2.3.3. Jenis pelatihan sebagaimana dimaksud pada angka 2.3.2 terdiri dari beberapa tingkat yaitu :

2.3.3.1. Pelatihan d

2.3.3.2. Pelatihan k
dan Administrator Sistem) sesuai dengan tugas dan tanggung jawab masing-masing.

2.3.4. Kegiatan peningkatan *awareness* bagi Pengguna yang berupa pelatihan sebagaimana dimaksud pada angka 2.3.3 dilaksanakan oleh Seksi Bimbingan Sistem, Direktorat Teknologi Informasi Perpajakan (TIP).

2.3.5. Seksi Bimbingan Sistem, Direktorat TIP berkoordinasi dengan Subdirektorat AESI, Direktorat TTKI mengonsolidasikan materi pelatihan dan peningkatan *awareness* terkait pencegahan dan penanganan *malware*.

2.3.6. Pelatihan khusus sebagaimana dimaksud pada angka 2.3.3.2 hendaknya dapat

menghasilkan keterampilan antara lain meliputi :

2.3.6.1. Teknik unt

2.3.6.2. Teknis unt

2.3.6.3. Teknik unt

2.3.6.4. Teknik unt

2.4. Penggunaan Perangkat/Fasilitas Anti Malware

2.4.1. Direktorat TTKI bertanggung jawab untuk melakukan kajian dan pengembangan TIK dalam penyediaan perangkat/fasilitas *anti malware* yang akan digunakan oleh seluruh Unit Kerja di DJP.

2.4.2. Direktorat TIP bertanggung jawab atas distribusi dan operasional dari perangkat/fasilitas *anti malware*, termasuk update dan perawatan infrastrukturnya.

2.4.3. Perangkat/fasilitas *anti malware* yang harus disediakan antara lain :

2.4.3.1. *Antivirus*;

2.4.3.2. *Spyware d*

2.4.4.3. *Spam filte*

2.4.4.4. *Web Conte*

2.4.4.5. *Intrusion D*

2.4.4. Kriteria yang harus dipertimbangkan dalam pengadaan *antivirus* adalah sebagai berikut :

2.4.4.1. *Antivirus* s

a. Mampu me

b. Mampu me

c. Memiliki ke

d. Mampu me

e. Mampu me

f. Mampu me

g. Dapat men

h. Memiliki ke

2.4.4.2. Mempunya

2.4.4.3. Telah mela

2.4.5. Hal-hal yang harus dipertimbangkan dalam pengadaan anti *spyware* seperti *spyware detection* dan *removal utilities* adalah sebagai berikut :

2.4.5.1. *Anti spywa*

a. Dapat men

b. dapat men

c. Dapat men

d. Dapat men

e. Dapat men

f. Dapat men

2.4.6. Ketentuan dalam operasional dan manajemen perangkat/fasilitas *anti malware* adalah sebagai berikut :

2.4.6.1. *Source* dar

2.4.6.2. Perangkat

2.4.6.3. Untuk pera

2.4.6.4. Untuk pera

2.4.6.5. Direktorat

2.4.6.6. Direktorat

2.4.6.7. Pegawai ya

3. Penanganan Gangguan/Insiden Keamanan Informasi Akibat *Malware*

3.1. Direktorat TIP menyediakan, mempublikasikan, dan mendistribusikan panduan dasar bagi Pengguna dalam penanganan gangguan/insiden akibat malware yang disesuaikan dengan perangkat/fasilitas *anti malware* milik DJP.

3.2. Hal-hal berikut merupakan beberapa indikasi umum terjadinya *malware* :

3.2.1. Adanya peringatan (*alert*) yang dihasilkan oleh perangkat/fasilitas *anti malware* tentang adanya komputer/*host* yang telah terinfeksi;

3.2.2. Adanya *file* dengan karakter atau format yang tidak lazim ;

3.2.3. Adanya perubahan konfigurasi yang tidak normal yang tercatat pada *log* komputer;

3.2.4. Perangkat komputer atau *server* yang mengalami *reboot* secara otomatis setiap kali Pengguna mencoba menjalankan program tertentu (misalnya *web browser*);

3.2.5. Administrator *e-mail* menemukan adanya mass e-mail yang umumnya berukuran besar yang berisi konten mencurigakan;

3.2.6. Kontrol keamanan yang berupa *firewall* maupun *anti malware* tidak aktif/dimatikan (*disabled*);

3.2.7. Administrator jaringan menemukan tanda-tanda yang tidak lazim berdasarkan *tools* pemantauan perangkat jaringan komunikasi data misalnya, dari *tools* pemantauan *traffic flows*.

3.3. Penanganan gangguan/insiden keamanan informasi akibat *malware* pada perangkat TIK di DC/DRC :

3.3.1. Pegawai atau administrator sistem yang mendeteksi adanya malware pada perangkat TIK di DC/DRC harus segera melaporkan kepada Pejabat Keamanan Informasi Kantor Pusat untuk ditindaklanjuti.

3.3.2. Pejabat Keamanan Informasi Kantor Pusat melakukan tindak lanjut dengan mengacu kepada Pedoman Tindakan Perbaikan dan Pencegahan serta Pengelolaan Gangguan Keamanan Informasi.

3.4. Penanganan ganguan/insiden keamanan informasi akibat malware pada perangkat TIK selain DC/DRC :

3.4.1. Apabila Pegawai DJP mendeteksi adanya malware, maka pegawai tersebut harus melakukan mekanisne yang tercantum dalam panduan dasar sebagaimana dimaksud pada angka 3.1 sebelum melapor kepada Petugas Keamanan Informasi;

3.4.2. Dalam hal setelah mengikuti panduan dasar Pengguna tetap tidak dapat menyelesaikan gangguan tersebut, maka Pengguna melaporkannya kepada *Operator Console* atau Pegawai yang ditunjuk oleh Pimpinan Unit Kerja;

3.4.3. Tindak lanjut penanganan gangguan mengacu kepada Pedoman Tindakan Perbaikan dan Pencegahan serta Pengelolaan Gangguan Keamanan Informasi.

3.5. Pada saat melakukan penanganan gangguan keamanan informasi akibat adanya *malware*, Petugas Keamanan Informasi Kantor Pusat berkoordinasi dengan seksi lain yang terkait di lingkungan Unit Kerja TIK. Sarana yang harus tersedia dalam rangka penanganan *malware* antara lain :

3.5.1. *Packet sniffer* dan *protocol analyzer* ;

3.5.2. Daftar *port*, baik *port* yang digunakan dalam kegiatan operasional maupun *port* yang biasa dipakai oleh *malware*;

3.5.3. Perangkat/fasilitas anti *malware*;

3.5.4. *Network diagram* dan daftar perangkat TIK yang bersifat kritikal;

3.5.5. *Update security patch* untuk sistem operasi dan aplikasi lainnya; dan

3.5.6. media lain seperti *operating system media, boot disk/CD, backup data,* atau *installer* perangkat lunak lainnya.

4. Pemantauan dan Laporan dalam Pencegahan dan Penanganan *Malware*

4.1. Petugas Keamanan Informasi Kantor Pusat mengkoordinasikan pemantauan dan kajian berkala terhadap sistem/data/aplikasi DJP sebagai tindakan proaktif untuk menemukan kelemahan (*vulnerabillity*)-nya terhadap *malware* dan menyampaikan laporan setiap 6 (enam) bulan sekali kepada Pejabat Keamanan Informasi Kantor Pusat DJP dan Subdirektorat Analisis dan Evaluasi Sistem Informasi, Direktorat TTKI.

4.2. Format laporan pemantauan dan kajian sebagaimanan dimaksud pada angka 4.1 terdapat pada Lampiran I Pedoman ini.

4.3. Petugas Keamanan Informasi di seluruh Indonesia melakukan reviu secara berkala terhadap *server* yang berada di wilayah penugasannya dengan ketentuan sebagai berikut :

4.3.1. Pemantauan dilakukan setiap tiga bulan sekali;

4.3.2. Pemantauan dilakukan dengan mengambil data konfigurasi perangkat di lapangan dan membandingkannya dengan hasil pemantauan periode sebelumnya;

4.3.3. Direktorat TIP menyediakan tools standar untuk membantu proses pemantauan;

4.3.4. Dalam hal terdapat file atau program yang mencurigakan/tidak wajar atau terjadi perubahan secara tidak sah (*unauthorized amendments*) pada konfigurasi perangkat, Petugas Keamanan Informasi segera mencari penyebabnya dan melakukan langkah-langkah untuk melindungi perangkat lunak dan data tersebut.

4.4. Petugas Keamanan Informasi harus menyusun laporan terkait gangguan *malware* yang terjadi di wilayah penugasannya, kemudian menyampaikannya kepada Pejabat Keamanan Informasi Kantor Pusat DJP setiap 3 (tiga) bulan sekali.

4.5. Format laporan sebagaimana dimaksud pada angka 4.4 terdapat dalam Lampiran II Pedoman ini.

4.6. Pejabat Keamanan Informasi Kantor Pusat DJP melakukan kompilasi atas laporan tersebut dan menyampaikannya kepada Kepala Subdirektorat AESI.

4.7. Hasil dari laporan rutin tersebut digunakan oleh Subdirektorat AESI sebagai bahan evaluasi rutin untuk melakukan perbaikan berupa :

4.7.1. Perbaikan kebijakan atau pedoman terkait pencegahan dan penanganan *malware*;

4.7.2. Perbaikan materi pelatihan dan/atau program *awareness* bagi Pengguna;

4.7.3. Perbaikan konfigurasi terhadap sistem yang terbukti kelemahan (*vulnerabillity*)-nya; dan

4.7.4. Perbaikan terhadap perangkat/fasilitas *anti malware* yang dimiliki DJP.

4.8. Untuk memastikan kepatuhan (*compliance*) dari semua pihak terhadap pelaksanan Pedoman Pencegahan *Malware* ini, Direktur TIP dapat mengusulkan pelaksanaan pencegahan dan penanganan *malware* sebagai salah satu objek audit internal kepada DIrektur KITSDA, pelaksanaannya mengacu kepada Pedoman Audit Internal Tata Kelola TIK.

E. Definisi

1. ***Active content*** adalah isi (*content*) dalam *website* yang bersifat interaktif, misalnya : gambar animasi, aplikasi javascript, *streaming video,* aplikasi ActiveX, dan sebagainya.
2. **Administrator Sistem** adalah pegawai DJP yang ditunjuk untuk mengelola, melakukan pemeliharaan, dan pengawasan terhadap sistem TIK serta bertanggung jawab terhadap integritas data, efisiensi, dan kinerja dari sistem TIK.
3. **Advertising-supported softwar**e atau disingkat ***adware*** adalah paket perangkat lunak yang secara otomatis menampilkan atau mengunduh iklan ke perangkat komputer.
4. ***Baseline security configuration*** adalah konfiguration suatu sistem yang disusun untuk memaksimalkan pengamanan melalui penentuan sejumlah parameter teknis yang ada, yang penerapannya harus dilakukan sebelum sistem tersebut digunakan secara operasional, di mana penetapannya dapat menggunakan referensi yang diterbitkan oleh pabrikan teknologi tersebut atau oleh organisasi yang secara khusus mengeluarkan standar untuk kepentingan publik.
5. ***Firewall*** adalah bagian dari sistem komputer atau jaringan yang dirancang untuk menyaring akses berdasarkan sejumlah aturan dan kriteria. Firewall memblokir akses yang tidak sah.
6. ***Intrusion Detection and Prevention System (IDPS)*** adalah perangkat keamanan yang berfungsi untuk memantau jaringan dan/atau sistem dari aktivitas-aktivitas yang membahayakan. Fungsi utama dari IDPS adalah untuk mengidentifikasi, mencatat, memblokir/menghentikan, dan melaporkan aktivitas berbahaya tersebut.
7. ***Mail server*** adalah perangkat komputer dan aplikasi yang bertindak sebagai kantor pos elektronik pada lalu lintas *e-mail*. Pengiriman *e-mail* lintas jaringan dilakukan dengan melewati *mail server*.
8. ***Malicous Software*** atau ***Malware*** adalah perangkat lunak yang dirancang untuk menyusup ke dalam sistem komputer dan memiliki kemampuan untuk mengganggu kinerja, merusak perangkat lunak dan sistem komputer, serta membahayakan kerahasiaan, keutuhan, maupun ketersediaan data, aplikasi, atau sistem operasi. Yang termasuk *malware* diantaranya adalah : *virus, trojan, worm , spyware*, dan *adware*.

9. ***Mass e-mail*** atau ***bulk e-mail*** adalah *e-mail* serupa yang dikirimkan ke sejumlah besar penerima. *Mass e-mail* umumnya berupa selebaran, kelompok diskusi, dan iklan.
10. ***Mobile code*** adalah perangkat lunak yang berpindah tempat antar sistem dan dapat dijalankan pada sistem lokal tanpa diinstalasi atau dijalankan dengan sepengetahuan Pengguna.
11. ***Moble computing*** adalah Penggunaan perangkat komputer jinjing (*portabel*) seperti *notebook* dan *personal data assistant* (PDA) untuk melakukan akses, pengolahan, dan penyimpanan data.
12. ***Packet sniffer*** atau ***protocol analyzer*** program komputer atau perangkat keras yang dapat menangkap dan mencatat lalu lintas jaringan. *Sniffer* menangkap setiap paket data yang melintasi jaringan dan apabila diperlukan, dapat men-*decode* dan menganalisis isinya.
13. **Pejabat Keamanan Informasi** adalah pejabat setingkat Eselon III yang ditunjuk oleh Direktur Jenderal Pajak untuk mengoordinasikan dan mengarahkan kegiatan penerapan kebijakan dan prosedur keamanan informasi di lingkungan unit Eselon II di mana pejabat tersebut ditugaskan. Yang termasuk Pejabat Keamanan Informasi adalah :
    a. Kepala Subdit Pemantauan Sistem dan Infrastruktur, Dit. TIP;
    b. Kepala Bidang Pemindaian Dokumen dan Perekaman Data, PPDDP;
    c. Seluruh Kepala Bidang Dukungan Teknis dan Konsultasi, Kanwil DJP.
14. **Perangkat/fasilitas *anti malware*** adalah perangkat lunak, perangkat keras, dan/atau *tools* yang digunakan untuk menemukan dan menghapus *malware*.
15. **Pengendali Catatan Penerapan Tata Kelola TIK** adalah Seksi Perancangan Prosedur Operasional, Direktorat Transformasi Teknologi Komunikasi dan Informasi.
16. **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 di mana pejabat tersebut ditugaskan dan bekerja di bawah pengawasan dan pengarahan Pejabat Keamanan Informasi. Yang termasuk Petugas Keamanan Informasi adalah :
    a. Kepala Seksi Pemantauan Keamanan Sistem dan Jaringan Komunikasi Data, Dit. TIP
    b. Kepala Seksi Perekaman dan Transfer Data, PPDDP
    c. Seluruh Kepala Seksi Dukungan Teknis Komputer, Kanwil DJP
17. **Pihak ketiga** adalah pihak selain pegawai Direktorat Jenderal Pajak yang melakukan pekerjaan di DJP dan menggunakan layanan milik DJP, misalnya dari lembaga pemerintah di luar DJP, mitra kerja seperti auditor, konsultan, penyedia jasa komunikasi, pemasok, dan pemelihara perangkat pengolah informasi, pegawai magang, dan sebagainya.
18. ***Pop up windows*** adalah *window* yang muncul ketika Pengguna memilih suatu tombol atau *link*. *Pop up wondows* biasanya berisi menu atau perintah yang tetap muncul di layar hingga Pengguna memilih salah satu opsi yang disediakan.
19. ***Proxy server*** adalah *server* (sistem komputer atau program aplikasi) yang bertindak sebagai perantara bagi *client* dalam melakukan *request* untuk mengakses *server* lain.
20. ***Removable media*** adalah media penyimpan data elektronik yang dapat dipindahkan dan tidak terpasang secara permanen pada komputer, misal *compact discs, DVD disc, memory stick, USB drive, floppy disk*, dan sebagainya.
21. ***Spam*** adalah penyalahgunaan dalam pengiriman berita elektronik untuk menampilkan berita iklan dan keperluan lainnya yang mengakibatkan ketidaknyamanan bagi Pengguna. Bentuk spam yang umum dikenal meliputi : *spam e-mail, instant message spam, usenet newsgroup spam, spam* mesin pencari *web* (*web search engine spam*), *spam blog, spam* berita pada telepon genggam, spam forum internet, dan lain-lain.
22. ***Spyware*** adalah jenis *malware* yang dirancang untuk melanggar privasi dari Pengguna, misalnya mengumpulkan informasi pribadi Pengguna perangkat komputer tersebut seperti *website* yang sering dikunjungi, maupun mengubah *setting* perangkat komputer sehingga mengganggu fungsinya.
23. ***Trojan horse*** atau ***trojan*** adalah suatu program yang membahayakan yang menyamar dalam program lain yang seolah-olah tidak membahayakan. *Trojan* tidak mereplikasi dirinya sendiri. *Trojan* dapat menimbulkan gangguan antara lain kerusakan sistem komputer lain yang terinfeksi atau pengendalian komputer yang terinfeksi dari komputer lain.
24. **Unit kerja TIK** adalah Direktorat Transformasi Teknologi Komunikasi dan Informasi serta Direktorat Teknologi Informasi Perpajakan.
25. ***Update security patch*** adalah perbaikan pada suatu program yang dapat mengatasi kelemahan yang berpotensi dapat dieksploitasi.
26. ***Virus*** adalah suatu segmen kode yang dapat membuat salinan terhadap dirinya sendiri melalui program yang berjalan tanpa sepengetahuan Pengguna komputer.
27. ***Virus definitions*** adalah definisi teknis dari suatu *virus* sehingga dapat diidentifikasi.
28. ***Windows shell*** adalah program antar muka grafis (*graphical user interface*) utama yang menampilkan desktop pada sistem operasi.
29. ***Worm*** adalah program yang menggandakan dirinya sendiri (*self replicating*) dalam memori dan menyebarkan dirinya melalui jaringan, sehingga menimbulkan gangguan pada jaringan.

LAMPIRAN I

PEDOMAN

KEMENTERIAN KEUANGAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PAJAK
Gedung B Lantai 4 Telepon 021 52904830
Jalan Gatot Subroto Kav. 40-42 Faksimile 021-5272723
Website : http://www.pajak.go.id

Laporan Pemantauan dan Kajian
dalam Pencegahan Malicous *Software* (*Software*)
Periode ..... (1) **s.d** ..... (2) **tahun** ..... (3)

No.	Objek/Data/Sistem yang dipantau	Kelemahan yang Ditemukan	Tanggal Pemantauan	
			Mulai	Selesai
1.	(4)	(5)	(6)	(7)
2.				
3.				
Dst				

Petugas Ke

(
NIP .....

Petunjuk pengisian :

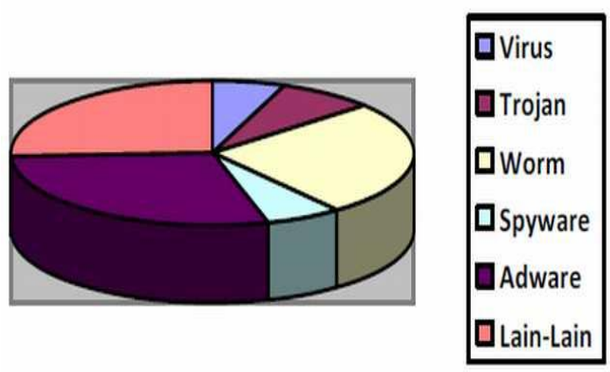
(1) Diisi dengan bulan awal periode pemantauan
(2) Diisi dengan bulan akhir periode pemantauan
(3) Diisi dengan tahun periode pemantauan
(4) Diisi dengan nama perangkat lunak atau data yang dipantau
(5) Diisi dengan kelemahan data atau sistem terhadap gangguan *malware*
(6) Diisi dengan tanggal awal pemantauan terhadap data/sistem yang dimaksud pada angka 4
(7) Diisi dengan tanggal akhir pemantauan terhadap data/sistem yang dimaksud pada angka 4
(8) Diisi dengan lokasi dan tanggal penyusunan laporan
(9) Diisi dengan nama lengkap Petugas Keamanan Informasi
(10) Diisi dengan NIP Petugas Keamanan Informasi

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

Laporan Gangguan *Malicious Software* (*Software*)

Perode : _____ (1) **s.d** _____ (2) **tahun** : _____ (3)

Wilayah : _____ (4)

Total Gangguan Malware yang terjadi (5) (*beri tanda 'V' pada pilihan yang sesuai*)	**DIAGRAM** (6)
☐ Virus : ..... kejadian ☐ Trojan : ..... kejadian ☐ Worm : ..... kejadian ☐ Spyware : ..... kejadian ☐ Adware : ..... kejadian ☐ Lain-lain : ..... kejadian	

Kerusakan Yang Dialami
(*uraikan*)

..... (7)

Langkah-Langkah Penanggulangan yang Dilakukan
(*uraikan*)

..... (8)

Mengetahui,
Pejabat Keamanan Informasi, Petugas Keamanan Informasi,

..... , ... (9)

( ) (10)

( ) (11)

NIP ..... (12)

( )

NIP ..... (13)

Petunjuk Pengisian Laporan Gangguan *Malicious Software (Malware)*

(1) Diisi dengan bulan awal periode pemantauan
(2) Diisi dengan bulan akhir periode pemantauan
(3) Diisi dengan tahun periode pemantauan
(4) Diisi dengan wilayah penugasan Pejabat dan Petugas Keamanan Informasi
(5) Diisi dengan memberikan tanda 'V' dan menuliskan jumlah kejadian gangguan *malware* sesuai dengan jenisnya
(6) Diisi dengan diagram kejadian gangguan malware sesuai dengan jumlah kejadian pada angka (5)
(7) Diisi dengan uraian kerusakan/dampak yang dialami akibat gangguan *malware*.
Misalnya perangkat, *file*, atau data yang terinfeksi.
(8) Diisi dengan uraian langkah-langkah penanggulangan yang dilakukan terkait gangguan *malware* yang terjadi
(9) Diisi dengan kota dan tanggal penyusunan laporan
(10) Diisi dengan nama lengkap Pejabat Keamanan Informasi
(11) Diisi dengan nama lengkap Petugas Keamanan Informasi
(12) Diisi dengan NIP Pejabat Keamanan Informasi
(13) Diisi dengan NIP Petugas Keamanan Informasi