LAMPIRAN
SURAT EDARAN DIREKTUR JENDERAL PAJAK
NOMOR : SE- 9/PJ/2011
TANGGAL : 17 JANUARI 2011
TENTANG : PEDOMAN TINDAKAN PERBAIKAN DAN PENCEGAHAN SERTA PENGELOLAAN GANGGUAN KEAMANAN INFORMASI

Pedoman Tindakan Perbaikan dan Pencegahan serta Pengelolaan Gangguan Keamanan Informasi

Direktorat Jenderal Pajak

Kementerian Keuangan Republik Indonesia

(versi 1.0)

Klasifikasi: TERBATAS

Tanggal 17 Januari 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

HALAMAN REVISI

Bab/Sub-Bab	Halaman	Revisi	Tanggal	Uraian Revisi
		v 1.0	Des 2010	

DAFTAR ISI

A. Deskripsi 1

B. Acuan..... 1

C. Dokumen Terkait..... 1

D. Pedoman Tindakan Perbaikan dan Pencegahan..... 1

E. Pedoman Pengelolaan Gangguan Keamanan Informasi..... 3

F. Definisi..... 6

Lampiran I Laporan Ketidaksesuaian dan Gangguan Keamanan Informasi

Lampiran II Tata Cara Tindak Lanjut Laporan Ketidaksesuaian dan Gangguan Keamanan Informasi

Lampiran III Laporan Tindakan Perbaikan dan Pencegahan serta Pengelolaan Gangguan Keamanan Informasi

A. Deskripsi

Pedoman Tindakan Perbaikan dan Pencegahan serta Pengelolaan Gangguan Keamanan Informasi disusun dengan tujuan untuk memberikan panduan dalam upaya melakukan tindakan perbaikan dan pencegahan serta pengembalian fungsi dan layanan operasional secepatnya bila terdapat ketidaksesuaian terhadap Kebijakan Pengelolaan Keamanan Informasi atau terjadinya gangguan keamanan informasi. Hal ini perlu diatur dalam rangka menjamin tindak lanjut ketidaksesuaian atau gangguan keamanan informasi yang sistematis dan tuntas, serta mencegah terulangnya kejadian tersebut sehingga aset informasi yang dimiliki DJP dapat terlindungi dari ancaman-ancaman yang merugikan.

B. Dasar Hukum

1. Kebijakan Pengelolaan Keamanan Informasi DJP
2. Kebijakan Pengelolaan Layanan Teknologi Informasi dan Komunikasi DJP

C. Acuan

1. ISO/IEC 27001 :2009: *Preventive Action*
2. ISO/IEC 27001 :2009: *Corrective Action*
3. ISO/IEC27001 :2005: *Information Security Incident Management*

D. Dokumen Terkait

Keputusan Direktur Jenderal Pajak Nomor KEP - 323/PJ/2010 tentang Pembentukan Tim Keamanan Informasi Direktorat Jenderal Pajak Periode 2010

E. Pedoman Tindakan Perbaikan dan Pencegahan

1. Setiap pegawai Direktorat Jenderal Pajak (DJP) yang melihat, mendengar, atau menerima keluhan terjadinya pelanggaran terhadap Kebijakan Pengelolaan Keamanan Informasi, harus melaporkannya ke Pejabat Keamanan Informasi terkait.

2. Pelaporan pelanggaran sebagaimana dimaksud pada angka 1 dilakukan dengan mengisi formulir Laporan Ketidaksesuaian dan Gangguan Keamanan Informasi sebagaimana terdapat pada lampiran I Pedoman ini.

3. Setelah menerima laporan sebagaimana dimaksud pada angka 2, Pejabat Keamanan Informasi menugaskan Petugas Keamanan Informasi untuk menganalisis laporan terjadinya pelanggaran terhadap Kebijakan Pengelolaan Keamanan Informasi. Jika berdasarkan analisis ternyata benar bahwa telah terjadi ketidaksesuaian, maka Petugas Keamanan Informasi menetapkan tingkat ketidaksesuaian yang terjadi, yaitu:
   3.1. Ketidaksesuaian menyebabkan insiden/gangguan keamanan informasi.

   Tindak lanjut atas tingkat ketidaksesuaian ini dilakukan mengacu pada Pedoman Pengelolaan Gangguan Keamanan Informasi sebagaimana dimaksud pada huruf E;
   3.2. Ketidaksesuaian tidak menyebabkan insiden/gangguan keamanan informasi tetapi berpotensi menjadi insiden. Tindak lanjut atas tingkat ketidaksesuaian ini dilakukan dengan menetapkan rencana tindakan perbaikan atau pencegahan ketidaksesuaian tersebut.
   3.3. Ketidaksesuaian tidak menyebabkan insiden/gangguan keamanan informasi dan tidak berpotensi menjadi insiden. Tindak lanjut atas tingkat ketidaksesuaian ini dilakukan dengan memberikan adanya laporan ketidaksesuaian ini kepada unit kerja terkait untuk dilakukan perbaikan dan pencegahan sesuai dengan ketentuan yang berlaku.

4. Dalam hal hasil analisis sebagaimana dimaksud pada angka 3.2, Petugas Keamanan Informasi melengkapi Laporan Ketidaksesuaian dan Gangguan Keamanan Informasi dengan rencana tindakan yang akan dilakukan dan melaporkannya kepada Pejabat Keamanan Informasi.

5. Berdasarkan hasil laporan dari Petugas Keamanan Informasi sebagaimana dimaksud pada angka 4, Pejabat Keamanan Informasi bertugas untuk:
   5.1. Meneruskan laporan ketidaksesuaian kepada Pimpinan unit kerja tempat kejadian untuk ditindaklanjuti;
   5.2. Menugaskan Petugas Keamanan Informasi untuk mengoordinasikan tindakan perbaikan dengan pihak terkait;
   5.3. Melakukan pemantauan terhadap pelaksanaan tindakan perbaikan atas laporan ketidaksesuaian; dan
   5.4. Melaporkan ketidaksesuaian ke Pejabat Keamanan Informasi Kantor Pusat DJP jika tindakan perbaikan tidak dapat dilakukan pada unit kerja tempat kejadian atau tindakan perbaikan merupakan kewenangan Kantor Pusat DJP.

6. Pejabat Keamanan Informasi mengoordinasikan tindakan pencegahan atas ketidaksesuaian yang terjadi dengan unit kerja terkait agar ketidaksesuaian tersebut tidak terulang kembali.

7. Tata cara pelaporan dan tindak lanjut dalam tindakan perbaikan dan pencegahan dilaksanakan sesuai Tata Cara Tindak Lanjut Laporan Ketidaksesuaian dan Gangguan Keamanan Informasi sebagaimana terdapat dalam Lampiran II Pedoman ini.

8. Petugas Keamanan Informasi membuat laporan mengenai ketidaksesuaian dan tindakan perbaikan atau pencegahan yang telah dilakukan di lingkungan penugasannya dan menyampaikannya kepada

Pejabat Keamanan Informasi Kantor Pusat setiap 3 (tiga) bulan sekali dengan format sebagaimana terdapat pada lampiran III Pedoman ini untuk keperluan tinjauan manajemen *(management review)* pengelolaan keamanan informasi.

F. Pedoman Pengelolaan Gangguan Keamanan Informasi

1. Setiap Pegawai DJP yang menemukan terjadinya insiden/gangguan keamanan informasi harus mencatat gangguan tersebut untuk dilaporkan.

2. Insiden atau gangguan keamanan informasi sebagaimana dimaksud pada angka 1 yang harus dilaporkan antara lain:
   2.1. Terjadinya pengungkapan, perubahan, atau penghancuran aset informasi penting milik DJP oleh pihak yang tidak berwenang, baik secara sengaja maupun tidak sengaja.
   2.2. Adanya upaya dari pihak yang tidak berwenang untuk mendapatkan akses ke aset informasi DJP.
   2.3. Terjadinya kehilangan atau pencurian aset informasi DJP, termasuk data elektronik yang bisa dipakai untuk mendapatkan akses ke dalam sistem informasi DJP (sebagai contoh: *security token,* kunci enkripsi, atau *password).*

3. Pelaporan insiden/gangguan keamanan informasi sebagaimana dimaksud pada angka 1 dilakukan dengan mengisi formulir Laporan Ketidaksesuaian dan Gangguan Keamanan Informasi sebagaimana terdapat pada lampiran I Pedoman ini.

4. Pencatatan, analisis, dan tindak lanjut insiden/gangguan keamanan informasi
   4.1. Hal-hal yang harus dicatat atas terjadinya gangguan sebagaimana dimaksud pada angka 1 meliputi waktu dan tempat ditemukannya gangguan, observasi atas kejadian tersebut, dan data pendukung lainnya yang dapat berupa data elektronik, *e-mail,* alamat situs, dan lain sebagainya.
   4.2. Gangguan keamanan informasi sebagaimana dimaksud pada angka 1 dilaporkan kepada Pejabat Keamanan Informasi terkait selambat-lambatnya 1 hari kerja setelah kejadian dengan menyertakan identitas pelapor dan detil informasi terkait gangguan tersebut. Khusus untuk kejadian yang diketahui sebagai gangguan berat harus dilaporkan selambat-lambatnya 1 (satu) jam setelah kejadian.
   4.3. Setelah menerima pelaporan sebagaimana dimaksud pada angka 4.2 Pejabat Keamanan Informasi menugaskan Petugas Keamanan Informasi untuk menggali data pendukung yang ada pada pelapor dengan cara antara lain memberikan bimbingan kepada pelapor untuk menjelaskan tampilan di layar, membacakan pesan yang ditampilkan oleh komputer, atau mengidentifikasi aset informasi yang dilaporkan.
   4.4. Dari hasil penggalian data pendukung sebagaimana dimaksud pada angka 4.3 Petugas Keamanan Informasi harus memahami bentuk insiden yang dilaporkan dan memastikan bahwa kejadian tersebut merupakan gangguan keamanan informasi, bukan gangguan layanan Teknologi Informasi dan Komunikasi (TIK). Dalam hal insiden yang dilaporkan merupakan gangguan layanan TIK, penanganannya mengacu pada Pedoman Pengelolaan Gangguan Layanan TIK.
   4.5. Petugas Keamanan Informasi membahas insiden yang dilaporkan dengan administrator baik sistem, jaringan, maupun aplikasi terkait untuk menentukan rencana penanggulangan insiden, kemudian melakukan hal-hal sebagai berikut:
      4.5.1. Mencatat insiden pada *log* insiden dengan mencantumkan tanggal dan waktu terjadinya insiden dan semua aktifitas yang dilakukan untuk menindaklanjutinya.
      4.5.2. Mengamankan data elektronik seperti *files, image,* dan lain-lain yang terkait dengan insiden paling lambat 1 jam setelah insiden tersebut dilaporkan.
      4.5.3. Mengidentifikasi risiko dan dampak insiden terhadap aset informasi milik DJP.
      4.5.4. Menerapkan rencana penanggulangan insiden paling lambat 24 jam setelah insiden tersebut dilaporkan.
      4.5.5. Dalam hal diperlukan tindakan penanggulangan insiden yang membutuhkan sumber daya yang besar atau memerlukan keputusan pihak lain, melaporkan kebutuhan ini kepada Pejabat Keamanan Informasi.
      4.5.6. Melaporkan status penyelesaian insiden keamanan informasi kepada pihak terkait.
   4.6. Pejabat Keamanan Informasi memimpin kegiatan analisis insiden dan memberi rekomendasi kepada Ketua Tim Keamanan Informasi guna memutuskan tindakan tertentu yang dapat mencegah meluasnya dampak insiden dan hilangnya bukti-bukti/rekaman yang akan digunakan sebagai jejak audit, kemudian melakukan hal-hal sebagai berikut:
      4.6.1. Berperan aktif secara teknis di lapangan dalam menangani insiden keamanan informasi, mengkoordinasi, mengawasi, dan memonitor proses pengelolaan insiden keamanan informasi.
      4.6.2. Mengawasi status penyelesaian insiden dan perkembangan kondisi penanggulangan insiden.
      4.6.3. Menerima laporan dari para petugas keamanan informasi dan menugaskan pegawai yang berkompeten di bidang yang terkait insiden tersebut untuk membantu pelaksanaan penyelesaian insiden.
   4.7. Ketua Tim Keamanan Informasi berkoordinasi dengan pihak-pihak yang terkait tindak lanjut insiden yaitu:
      4.7.1. Pimpinan Unit Kerja dan/atau Tim Pengarah Tata Kelola TIK, dalam hal insiden bersifat kritis, menyangkut hal yang strategis, atau memerlukan tindak lanjut dari

penegak hukum seperti Kepolisian atau penegak hukum lainnya.

4.7.2. Pemilik Aset Informasi yang terkena dampak insiden keamanan informasi.

4.7.3. Pimpinan Unit Kerja, dalam hal adanya keterlibatan dari pegawainya dalam insiden keamanan informasi.

4.7.4. Direktorat KITSDA dan Bagian Kepegawaian, dalam hal tindak lanjutnya berupa sanksi kepegawaian terhadap pegawai yang terlibat insiden keamanan informasi.

5. Penyelesaian Insiden Berat

5.1. Dalam hal insiden masuk dalam kategori insiden berat, Petugas Keamanan Informasi mengeskalasikannya kepada Pejabat Keamanan Informasi terkait untuk dilaporkan kepada Ketua Tim Keamanan Informasi.

5.2. Setelah menerima laporan terjadinya insiden berat, Ketua Tim Keamanan Informasi membentuk Tim Penyelesaian Insiden Keamanan Informasi untuk mengkaji dan menindaklanjuti laporan serta melaksanakan penyelesaian insiden tersebut. Anggota Tim harus terdiri dari pegawai yang ahli di bidang yang terkait insiden tersebut dan pegawai tersebut harus teruji integritasnya.

5.3. Tim Penyelesaian Insiden Keamanan Informasi sebagaimana dimaksud pada angka 5.2 berkewajiban untuk menyelesaikan insiden dan melaporkan penyelesaiannya kepada Pejabat Keamanan Informasi KPDJP dan Ketua Tim Keamanan Informasi paling lambat 2 (dua) hari setelah penugasan diterima.

5.4. Dalam hal setelah 2 hari Tim belum melaporkan penyelesaian insiden, Pejabat Keamanan Informasi KPDJP bertanggung jawab untuk mengoordinasikan penyelesaian insiden tersebut dalam jangka waktu 2 (dua) hari.

5.5. Insiden yang telah selesai ditanggulangi harus dilaporkan kepada Pemilik Aset Informasi terkait. Pengamanan catatan *(record)* penanganan insiden tersebut menjadi tanggung jawab Petugas Keamanan Informasi KPDJP.

6. Tata cara pelaporan dan tindak lanjut dalam pengelolaan gangguan keamanan informasi dilaksanakan sesuai Tata Cara Tindak Lanjut Laporan Ketidaksesuaian dan Gangguan Keamanan Informasi sebagaimana terdapat dalam Lampiran II Pedoman ini.

7. Petugas Keamanan Informasi membuat laporan mengenai gangguan keamanan informasi dan menyampaikannya kepada Pejabat Keamanan Informasi Kantor Pusat setiap 3 (tiga) bulan sekali dengan format sebagaimana terdapat pada lampiran III Pedoman ini untuk keperluan tinjauan manajemen *(management review)* pengelolaan keamanan informasi.

8. Kajian Ulang Insiden Keamanan Informasi

8.1. Secara berkala setiap 3 (tiga) bulan sekali atau dalam hal terdapat keperluan yang mendesak, Pejabat Keamanan Informasi bersama-sama dengan Petugas Keamanan Informasi melakukan evaluasi terhadap catatan insiden yang ada untuk:

8.1.1. Menganalisis dan menyusun tindakan perbaikan *(corrective)* lanjutan yang perlu diterapkan untuk menghindari terulangnya kejadian serupa;

8.1.2. Menerapkan inisiatif tindakan pencegahan *(preventive)* terhadap area yang disinyalir rentan terhadap insiden sejenis; dan/atau

8.1.3. Melakukan evaluasi terhadap efektifitas penyelesaian insiden termasuk pengendalian keamanan *(security control)* yang terkait dengan insiden tersebut.

G. Definisi

1. **Insiden/gangguan keamanan informasi** adalah suatu kejadian yang terjadi akibat adanya suatu kegiatan, aktifitas, atau proses yang mengancam ketersediaan, keutuhan, dan/atau kerahasiaan aset informasi yang ada.

   Insiden diklasifikasikan menjadi 3 (tiga) yaitu:

   1.1. Insiden Berat

   Suatu insiden yang mengakibatkan dampak yang besar terhadap aset informasi milik DJP apabila tidak ditanggulangi secepatnya. Termasuk dalam klasifikasi ini adalah insiden yang terkait aset informasi dengan kategori SANGAT RAHASIA. Insiden yang terkait dengan aktifitas intrusi atau penyerangan ke dalam sistem informasi DJP masuk dalam kategori ini.

   1.2. Insiden Sedang

   Suatu insiden yang dampaknya mengakibatkan terhentinya kegiatan DJP atau hilangnya fungsi/proses kerja inti DJP untuk jangka waktu yang singkat. Termasuk dalam klasifikasi ini adalah penyingkapan aset informasi DJP dengan kategori RAHASIA atau TERBATAS dalam jumlah besar atau dengan frekuensi yang tinggi.

   1.3. Insiden Ringan

   Suatu insiden yang dampaknya mengakibatkan terganggunya operasional DJP khususnya dari segi ketersediaan dan keutuhan aset informasi.

2. **Pengelolaan Keamanan Informasi** adalah seluruh perangkat berupa kebijakan, prosedur, dan instruksi kerja yang menjelaskan komitmen, pengelolaan, penerapan, dan pelaksanaan keamanan informasi di lingkungan DJP.

3. **Ketidaksesuaian *(non-conformity)*** adalah keadaan tidak terpenuhinya persyaratan pengelolaan keamanan informasi sebagaimana ditetapkan dalam Kebijakan Pengelolaan Keamanan Informasi. Bentuk ketidaksesuaian yang mungkin terjadi di DJP misalnya: pelanggaran terhadap ketentuan pengelolaan *user account/password* DJP, pelanggaran terhadap ketentuan akses pihak ketiga, tidak

terpenuhinya persyaratan keamanan fisik perangkat server, dan sebagainya.

4. **Tindakan perbaikan** ***(corrective action)*** adalah tindakan yang diperlukan untuk menangani suatu ketidaksesuaian agar hal tersebut tidak terjadi lagi.

5. **Tindakan pencegahan** ***(preventive action)*** adalah tindakan yang diperlukan untuk mencegah agar kemungkinan terjadinya ketidaksesuaian dapat dihilangkan.

6. **Pejabat Keamanan Informasi** adalah Kepala Subdirektorat Pemantauan Sistem dan Infrastruktur Direktorat Teknologi Informasi Perpajakan untuk lingkup Kantor Pusat DJP, Kepala Bidang Pemindaian Dokumen dan Perekaman Data untuk lingkup Pusat Pengolahan Data Dokumen Perpajakan, serta Kepala Bidang Dukungan Teknis dan Konsultasi untuk lingkup setiap Kantor Wilayah dan unit kerja di bawahnya.

7. **Petugas Keamanan Informasi** adalah Kepala Seksi Pemantauan Keamanan Sistem dan Jaringan Komunikasi Data Direktorat Teknologi Informasi Perpajakan untuk lingkup Kantor Pusat DJP, Kepala Seksi Perekarnan dan Transfer Data untuk lingkup Pusat Pengolahan Data dan Dokumen Perpajakan, serta Kepala Seksi Dukungan Teknis Komputer untuk lingkup setiap Kantor Wilayah dan unit kerja di bawahnya.

8. **Unit kerja TIK DJP** adalah Direktorat Teknologi Informasi Perpajakan (TIP) dan Direktorat Transformasi Teknologi Informasi dan Komunikasi (TTKI).

9. **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.

10. **Tim Pengarah Tata Kelola TIK** adalah tim yang dibentuk oleh Direktur Jenderal Pajak untuk mengarahkan penyelenggaraan Tata Kelola TIK agar sesuai dengan Rencana Strategis DJP.

11. **Tinjauan manajemen** ***(management review)*** adalah evaluasi terhadap pelaksanaan pengelolaan keamanan informasi dalam bentuk pertemuan/rapat rutin yang diselenggarakan oleh Tim Pengarah Tata Kelola Teknologi Informasi dan Komunikasi (TIK).

( )(13)	( )(17)
NIP..... (14)	NIP..... (18)

*) Diisi oleh Pelapor

Petunjuk Pengisian
Laporan Ketidaksesuaian dan Gangguan Keamanan Informasi

Data Kejadian (Data kejadian diisi oleh pelapor ketika melaporkan kejadian)

(1) Diisi dengan nama pelapor.

(2) Diisi dengan kejadian yang dilaporkan

(3) Diisi dengan tempat kejadian dan unit kerja tempat kejadian

Contoh: Ruang server, KPP Pratama Cilegon

(4) Diisi dengan tanggal dan jam kejadian.

(5) Diisi dengan deskripsi kejadian yang dilaporkan.

Tindak Lanjut

(6) Diisi dengan memberikan tanda pada kotak yang tersedia.

Tindakan

(7) Diisi dengan rencana tindakan yang akan dilakukan untuk menangani kejadian yang dilaporkan.

(8) Diisi dengan deskripsi akar permasalahan yang menimbulkan kejadian.

(9) Diisi dengan tindakan yang telah dilakukan untuk menangani kejadian yang dilaporkan.

(10) Diisi dengan tanggal selesainya tindakan penanganan.

(11) Jika diperlukan dapat diisi dengan bukti pendukung bahwa laporan telah selesai ditangani.

(12) Jika diperlukan dapat diisi dengan keterangan lain yang dianggap penting.

(13) Diisi dengan nama pelapor.

(14) Diisi dengan NIP pelapor jika pelapor adalah pegawai DJP.

(15) Diisi dengan kota dan tanggal ditandatanganinya dokumen.

(16) Diisi dengan nama jabatan Pejabat Keamanan Informasi atau Ketua Tim Keamanan Informasi dimana laporan ditangani. Misalnya: Pejabat Keamanan Informasi Kanwil DJP Banten; atau Ketua Tim Keamanan Informasi DJP.

(17) Diisi dengan nama lengkap Pejabat.

(18) Diisi dengan NIP Pejabat.

LAMPIRAN II
PEDOMAN TINDAKAN PERBAIKAN DAN PENCEGAHAN SERTA PENGELOIAAN GANGGUAN KEAMANAN INFORMASI

TATA CARA TINDAK LANJUT LAPORAN KETIDAKSESUAIAN DAN GANGGUAN KEAMANAN INFORMASI

A. Pihak yang Terlibat

1. Direktur TIP sebagai Ketua Tim Keamanan Informasi
2. Kasubdit/Kabid yang ditunjuk sebagai Pejabat Keamanan Informasi KPDJP
3. Kasi yang ditunjuk sebagai Petugas Keamanan Informasi KPDJP
4. Kasubdit/Kabid yang ditunjuk sebagai Pejabat Keamanan Informasi Terkait
5. Kasi yang ditunjuk sebagai Petugas Keamanan Informasi Terkait
6. Pegawai DJP sebagai Pelapor

B. Prosedur Kerja

I. Penyampaian Laporan

1. Pelapor melaporkan ketidaksuaian terhadap kebijakan Pengelolaan Keamanan Informasi kepada Pejabat Keamanan Informasi terkait dengan cara mengisi Laporan Tindakan Perbaikan dan Pencegahan serta Pengelolaan Gangguan Keamanan Informasi.
2. Pejabat Keamanan Informasi terkait menerima laporan dan menugaskan kepada Petugas Keamanan Informasi untuk menganalisis laporan.
3. Petugas Keamanan Informasi terkait melakukan analisis terhadap laporan. Hal-hal yang dilakukan oleh Petugas Keamanan Informasi antara lain:
   3.1. Menetapkan apakah kejadian yang dilaporkan merupakan insiden/gangguan atau belum menjadi insiden tetapi berpotensi menjadi insiden;
   3.2. Jika tidak menyebabkan insiden/gangguan keamanan informasi tetapi berpotensi menjadi insiden, ditindaklanjuti dengan prosedur tindakan perbaikan dan pencegahan;
   3.3. Jika termasuk insiden, ditindaklanjuti dengan prosedur pengelolaan gangguan keamanan informasi.

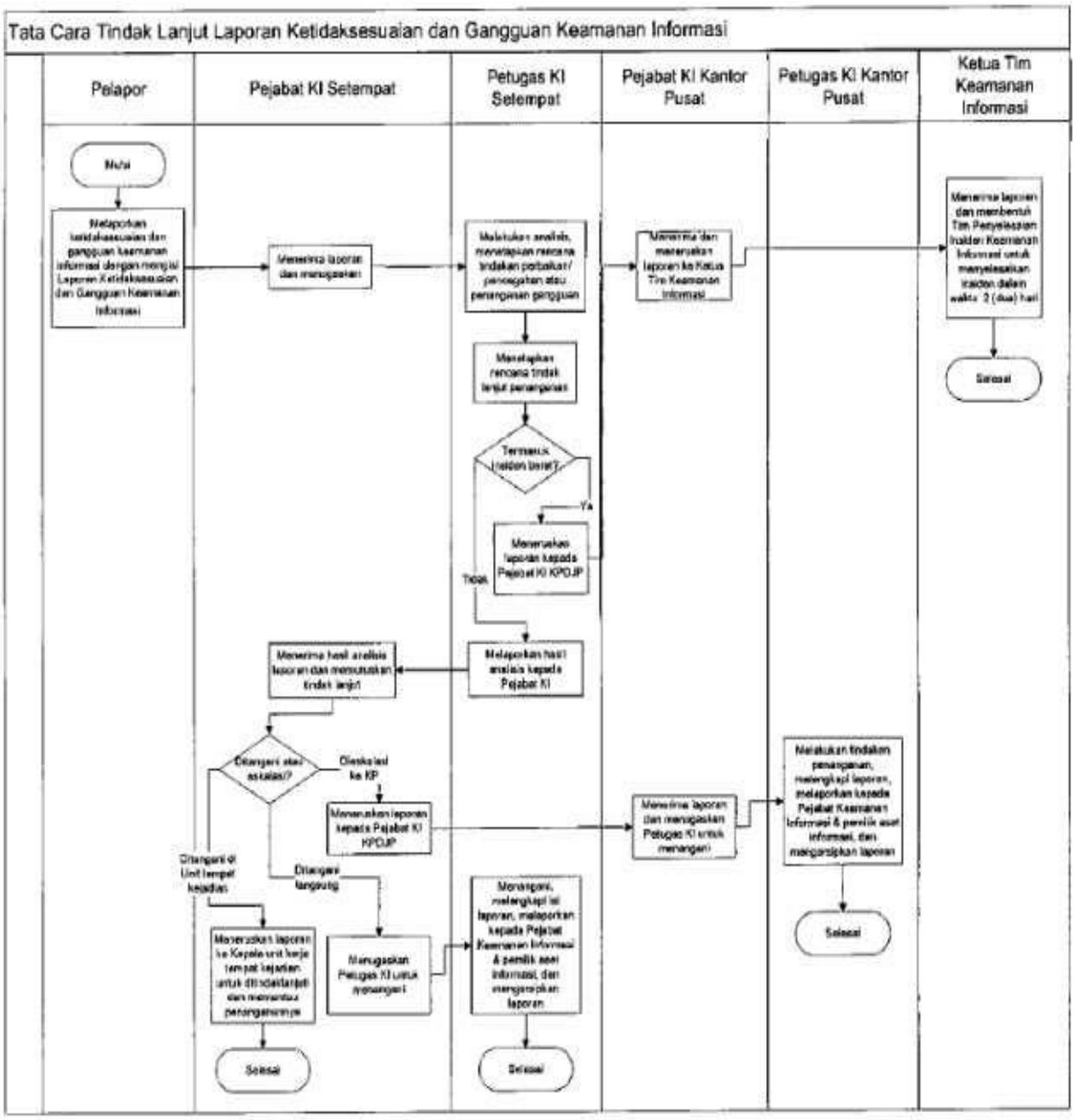
II. Tindakan Perbaikan dan Pencegahan

1. Petugas Keamanan Informasi menetapkan rencana tindakan yang akan dilakukan untuk menangani laporan.
2. Petugas Keamanan Informasi melaporkan hasil analisis kepada Pejabat Keamanan Informasi.
3. Pejabat Keamanan Informasi menetapkan tindak lanjut terhadap laporan.
4. Laporan ditindaklanjuti di unit tempat kejadian jika tindakan untuk menangani pelanggaran harus dilakukan di unit tempat kejadian, dengan cara:
   4.1. Pejabat Keamanan Informasi meneruskan laporan kepada Pimpinan unit kerja tempat kejadian untuk ditindaklanjuti;
   4.2. Pejabat Keamanan Informasi menugaskan Petugas Keamanan Informasi untuk mengoordinasikan tindakan perbaikan dengan pihak terkait dan memantau pelaksanaannya;
   4.3. Petugas Keamanan Informasi melengkapi Laporan Ketidaksesuaian dan Gangguan Keamanan Informasi dan mengarsipkannya.
5. Laporan ditindaklanjuti di unit tempat Pejabat Keamanan Informasi berada jika penanganan laporan dapat atau harus dilakukan di unit tempat Pejabat Keamanan Informasi, dengan cara:
   5.1. Pejabat Keamanan Informasi menugaskan Petugas Keamanan Informasi untuk melakukan tindakan perbaikan;
   5.2. Petugas Keamanan Informasi melakukan tindakan perbaikan, kemudian melengkapi Laporan Ketidaksesuaian dan Gangguan Keamanan Informasi dan mengarsipkannya.
6. Laporan ditindaklanjuti di Kantor Pusat jika tindakan perbaikan tidak dapat dilakukan pada unit tempat kejadian atau tindakan perbaikan merupakan kewenangan Kantor Pusat, dengan cara:
   6.1. Pejabat Keamanan Informasi meneruskan laporan kepada Pejabat Keamanan Informasi KPDJP;
   6.2. Pejabat Keamanan Informasi KPDJP menerima laporan dan menugaskan Petugas Keamanan Informasi KPDJP untuk menindaklanjuti;
   6.3. Petugas Keamanan Informasi KPDJP melakukan tindakan perbaikan, kemudian melengkapi Laporan Ketidaksesuaian dan Gangguan Keamanan Informasi dan mengarsipkannya.
7. Petugas Keamanan Informasi melaporkan tindakan perbaikan dan pencegahan kepada Pejabat Keamanan Informasi.
8. Proses selesai.

III. Pengelolaan Gangguan Keamanan Informasi

1. Jika Petugas Keamanan Informasi menetapkan insiden termasuk ke dalam klasifikasi berat, maka:
   1.1. Laporan diteruskan kepada Pejabat Keamanan Informasi KPDJP;
   1.2. Pejabat Keamanan Informasi KPDJP menerima, meneliti, dan meneruskan laporan kepada Ketua Tim Keamanan Informasi untuk ditindaklanjuti;
   1.3. Ketua Tim Keamanan Informasi menerima laporan dan membentuk Tim Penyelesaian Insiden Keamanan Informasi.
   1.4. Tim Penyelesaian Insiden Keamanan Informasi berkewajiban untuk menyelesaikan insiden dan melaporkan penyelesaiannya kepada Pejabat Keamanan Informasi KPDJP dan Ketua Tim Keamanan Informasi paling lambat 2 (dua) hari setelah penugasan diterima.
   1.5. Dalam hal setelah 2 (dua) hari Tim Penyelesaian Insiden Keamanan Informasi belum melaporkan penyelesaian insiden, Pejabat Keamanan Informasi KPDJP bertanggung jawab untuk mengoordinasikan penyelesaian insiden tersebut.
2. Jika insiden bukan termasuk klasifikasi berat, maka Petugas Keamanan Informasi memutuskan:
   2.1. Laporan ditindaklanjuti di unit tempat kejadian jika tindakan untuk menangani insiden harus dilakukan di unit tempat kejadian, dengan cara:
      2.1.1. Pejabat Keamanan Informasi meneruskan laporan kepada Pimpinan unit kerja tempat kejadian untuk ditindaklanjuti;
      2.1.2. Pejabat Keamanan Informasi menugaskan Petugas Keamanan Informasi untuk mengoordinasikan tindakan penanggulangan dengan pihak terkait dan memantau pelaksanaannya;
      2.1.3. Petugas Keamanan Informasi melengkapi Laporan Ketidaksesuaian dan Gangguan Keamanan Informasi dan mengarsipkannya.
   2.2. Laporan ditindaklanjuti di unit tempat Pejabat Keamanan Informasi berada jika penanganan laporan dapat atau harus dilakukan di unit tempat Pejabat Keamanan Informasi, dengan cara:
      2.2.1. Pejabat Keamanan Informasi menugaskan Petugas Keamanan Informasi untuk melakukan tindakan penanggulangan;
      2.2.2. Petugas Keamanan Informasi melakukan tindakan penanggulangan, kemudian melengkapi Laporan Ketidaksesuaian dan Gangguan Keamanan Informasi dan mengarsipkannya.
   2.3. Laporan ditindaklanjuti di Kantor Pusat jika tindakan penanggulangan tidak dapat dilakukan pada unit tempat kejadian atau tindakan penanggulangan merupakan kewenangan Kantor Pusat, dengan cara:
      2.3.1. Pejabat Keamanan Informasi meneruskan laporan kepada Pejabat Keamanan Informasi KPDJP;
      2.3.2. Pejabat Keamanan Informasi KPDJP menerima laporan dan menugaskan Petugas Keamanan Informasi KPDJP untuk menindaklanjuti;
      2.3.3. Petugas Keamanan Informasi KPDJP melakukan tindakan penanggulangan, kemudian melengkapi Laporan Ketidaksesuaian dan Gangguan Keamanan Informasi dan mengarsipkannya.
3. Insiden yang telah selesai ditanggulangi dilaporkan kepada Pemilik Aset Informasi terkait.
4. Proses selesai.

C. Bagan Arus (Flowchart)



LAMPIRAN III
PEDOMAN TINDAKAN PERBAIKAN DAN PENCEGAHAN SERTA PENGELOIAAN GANGGUAN KEAMANAN INFORMASI

LAPORAN TINDAKAN PERBAIKAN DAN PENCEGAHAN SERTA PENGELOLAAN GANGGUAN KEAMANAN INFORMASI

PERIODE :.....(1) s/d ..... (2) tahun .....(3)

UNIT KERJA: .....(4)

No	Kejadian yang Dilaporkan	Nomor Laporan	Tanggal Laporan	Tempat Kejadian	Waktu Kejadian	Nama Pelapor	Unit Kerja Pelapor	Bukti Pendukung	Tindak Lanjut		Status Laporan
									Uraian	Unit Kerja	
(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)	(14)	(15)	(16)

..... (17)
Petugas Keamanan Informasi,

( ) (18)
NIP..... (19)

Mengetahui,
Pejabat Keamanan Inforrnasi

( ) (20)
NIP..... (21)

PETUNJUK PENGISIAN
LAPORAN TRIWULAN TINDAKAN PERBAIKAN DAN PENCEGAHAN SERTA PENGELOLAAN GANGGUAN KEAMANAN INFORMASI

(1) Diisi dengan tanggal dan bulan mulainya periode pencatatan tindakan perbaikan dan pencegahan serta pengelolaan gangguan keamanan informasi

(2) Diisi dengan tanggal dan bulan selesainya periode pencatatan tindakan perbaikan dan pencegahan serta pengelolaan gangguan keamanan informasi

(3) Diisi dengan tahun periode pencatatan tindakan perbaikan dan pencegahan serta pengelolaan gangguan keamanan informasi

(4) Diisi dengan nama unit kerja yang mengirimkan Laporan Ketidaksesuaian dan Gangguan Keamanan Informasi

(5) Diisi dengan nomor urut.

(6) Diisi dengan nama kejadian yang dilaporkan pada Laporan Ketidaksesuaian dan Gangguan Keamanan Informasi

(7) Diisi dengan nomor Laporan Ketidaksesuaian dan Gangguan Keamanan Informasi

(8) Diisi dengan tanggal Laporan Ketidaksesuaian dan Gangguan Keamanan Informasi

(9) Diisi dengan tempat kejadian pada Laporan Ketidaksesuaian dan Gangguan Keamanan Informas

(10) Diisi dengan waktu kejadian pada Laporan Ketidaksesuaian dan Gangguan Keamanan Informasi

(11) Diisi dengan nama pelapor pada Laporan Ketidaksesuaian dan Gangguan Keamanan Informasi

(12) Diisi dengan unit kerja pelapor pada Laporan Ketidaksesuaian dan Gangguan Keamanan Informasi

(13) Diisi dengan bukti pendukung pada Laporan Ketidaksesuaian dan Gangguan Keamanan Informasi

(14) Diisi dengan uraian tindak lanjut yang dilakukan

(15) Diisi dengan unit kerja yang melakukan tindak lanjut (unit keria setempatldiekskalasi ke Kantor Pusat)

(16) Diisi dengan status laporan, yaitu: selesai, dalam proses, atau belum ditindaklanjuti.

(17) Diisi dengan tanggal penyusunan laporan

(18) Diisi dengan nama lengkap Petugas Keamanan Informasi yang menyusun laporan

(19) Diisi dengan NIP Petugas Keamanan Informasi

(20) Diisi dengan nama Pejabat Keamanan Informasi

(21) Diisi dengan NIP Pejabat Keamanan Informasi