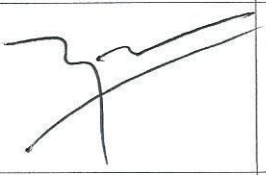
KEBIJAKAN
SISTEM MANAJEMEN KEAMANAN INFORMASI
DAN
KEAMANAN INFORMASI
PT EDI INDONESIA

No. Dokumen	001
No. Versi	4.1
Tanggal Pengesahan	9 Mei 2017

LEMBAR PENGESAHAN

	Dibuat Oleh :	Diperiksa Oleh :	Disahkan Oleh:
Jabatan	Wakil Manajemen Rep	Manajemen Rep	Direktur Utama
Tanda Tangan			
Nama	Yanuar Tri Jayadi	Yudo Budi Pramono	E Helmi Wantono

KONTROL DOKUMEN

No	Tanggal Review	Hasil Keputusan	Versi	Tanggal Efektif
1	10 Juli 2013	Merubah sasaran SMKI dalam sub bab 5.3.2. Sasaran Sistem Manajemen Keamanan Informasi	2.0	12 Juli 2013
2	9 Juli 2015	Merubah ruang lingkup dalam bab 3, dan versi ISO 27001	3.0	9 Juli 2015
3	7 Agustus 2015	Diupdate sesuai versi ISO 27001: 2013	3.1	14 Agustus 2015
4	27 Mei 2016	Diupdate sesuai versi ISO 27001: 2013	4.0	27 Mei 2016
5	9 Mei 2017	Diupdate sesuai versi ISO 27001: 2013	4.1	9 Mei 2017

DAFTAR ISI

1. PENDAHULUAN 1
2. TUJUAN 1
3. RUANG LINGKUP SMKI 1
   3.1 Ruang Lingkup Organisasi 1
   3.2 Isu Internal dan Eksternal 2
4. REFERENSI 2
5. SISTEM MANAJEMEN KEAMANAN INFORMASI (SMKI) 3
   5.1. Pernyataan Kebijakan SMKI 3
   5.2. Kerangka Kerja Proses SMKI 4
   5.3. Tujuan dan Sasaran SMKI 6
      5.3.1. Tujuan SMKI 6
      5.3.2. Sasaran SMKI 7
   5.4. Proses Manajemen Resiko 10
      5.4.1. Penerapan Manajemen Risiko Keamanan Informasi 10
      5.4.2. Keluaran Manajemen Risiko Keamanan Informasi 11
6. KEBUTUHAN DOKUMENTASI 11
   6.1. Struktur Dokumentasi SMKI 11
   6.2. Pengendalian Dokumen 12
   6.3. Pengendalian Rekaman / Catatan (*Record*) Pelaksanaan SMKI 12
7. TANGGUNG JAWAB MANAJEMEN 12
   7.1. Komitmen Manajemen 12
      7.1.1 Struktur Organisasi SMKI 12
      7.1.2 Wewenang dan Tanggung Jawab Organisasi SMKI 13
   7.2. Manajemen Sumber Daya dan Pelatihan 15
      7.2.1 Penyediaan Sumber Daya 15

8. AUDIT INTERNAL SMKI 16
9. TINJAUAN MANAJEMEN SMKI 16
10. PENINGKATAN SMKI 16
10.1. *Continual Improvement* 16
10.2. Tindakan Perbaikan dan Pencegahan 16
11. *COMPLIANCE* 17
12. *DOMAIN* KEAMANAN INFORMASI 17
13. PENINJAUAN DOKUMEN KEBIJAKAN SMKI DAN KEAMANAN INFORMASI 18

1. PENDAHULUAN

Informasi merupakan elemen yang sangat penting di lingkungan PT. EDI Indonesia (PT. EDII) dalam rangka kegiatan bisnis perusahaan. Untuk menjamin kesesuaian dan kebenaran informasi, terdapat 3 aspek yang harus dijaga yaitu:

1. Kerahasiaan (*confidentiality*), informasi tidak bocor atau diketahui oleh pihak yang tidak berwenang.
2. Integritas (*integrity*), akurasi, kebenaran, dan kelengkapan dari informasi tetap terjaga.
3. Ketersediaan (*availability*), informasi tersedia untuk diakses oleh pihak yang berwenang pada saat informasi tersebut dibutuhkan.

Kebijakan Sistem Manajemen Keamanan Informasi (SMKI) ini bertujuan untuk memberikan panduan dalam membangun, mengimplementasikan, mengoperasikan, memonitor, memelihara, dan meningkatkan sistem manajemen keamanan informasi di lingkungan PT. EDII. Kebijakan SMKI ini juga ditujukan untuk meningkatkan pemahaman umum mengenai penerapan SMKI yang disesuaikan dengan standar ISO 27001:2013.

2. TUJUAN

Dokumen ini disusun untuk memenuhi persyaratan standard internasional ISO 27001:2013 di PT. EDII. Evaluasi berkala terhadap proses sistem manajemen dilakukan sebagai bagian dari rencana peningkatan berkelanjutan.

3. RUANG LINGKUP SMKI

1.1 Ruang Lingkup Organisasi

Ruang Lingkup Sistem Manajemen Keamanan Informasi (SMKI) di PT. EDII ini adalah Kantor Pusat PT. EDII yang berlokasi di Wisma SMR, Jakarta yang meliputi bagian-bagian sebagai berikut :

- **Divisi Sales Private - Sub Divisi Biro Administrasi Efek (BAE);**
- **Divisi IT Operation;**
- **Divisi IT Development.**

Aset – aset informasi dan teknologi informasi yang menjadi bagian dari proses keamanan informasi yang diatur dalam kebijakan dan prosedur yang ditetapkan merupakan aset yang berada di lokasi kantor pusat PT EDII dan terkait dengan tugas pokok berdasarkan ruang lingkup SMKI.

1.2 Isu Internal dan Eksternal

Efektifitas penerapan Sistem Manajemen Keamanan Informasi dilaksanakan dengan memperhatikan isu yang datang dari internal maupun eksternal.

Isu internal yang dapat mempengaruhi SMKI adalah sebagai berikut:

- Struktur Organisasi
- Ketentuan dan Tanggung Jawab
- Strategi Bisnis Perusahaan
- Sumber Daya dan Kemampuan Sumber Daya
- Budaya Organisasi
- Sistem Informasi dan Proses Sistem Informasi
- Hubungan yang didasarkan pada adanya Kontrak

Isu eksternal yang dapat mempengaruhi SMKI adalah sebagai berikut:

- Para Pelanggan
- Para Pengguna Jasa
- Pemegang Saham
- Para Pihak Berwenang
- Jajaran Direksi
- Rekanan/Vendor

Kebutuhan para pihak yang berkepentingan di atas diantaranya adalah terkait dengan:

- Kontrak perjanjian
- Peraturan dan perundang-undangan (Cyber Law dan Perlindungan Data Pribadi)

4. REFERENSI

Untuk tujuan penggunaan dokumen ini dan penerapan SMKI yang dilakukan di PT EDII, maka definisi yang diterapkan mengikuti panduan standard ISO 27001:2013.

5. SISTEM MANAJEMEN KEAMANAN INFORMASI (SMKI)

Dalam rangka proses pengamanan informasi, PT EDII menyusun, mengimplementasikan, mengoperasikan, memonitor, memelihara dan menyempurnakan dokumen SMKI dalam konteks aktivitas keseluruhan bisnis PT EDII dan risiko-risiko yang dihadapinya.

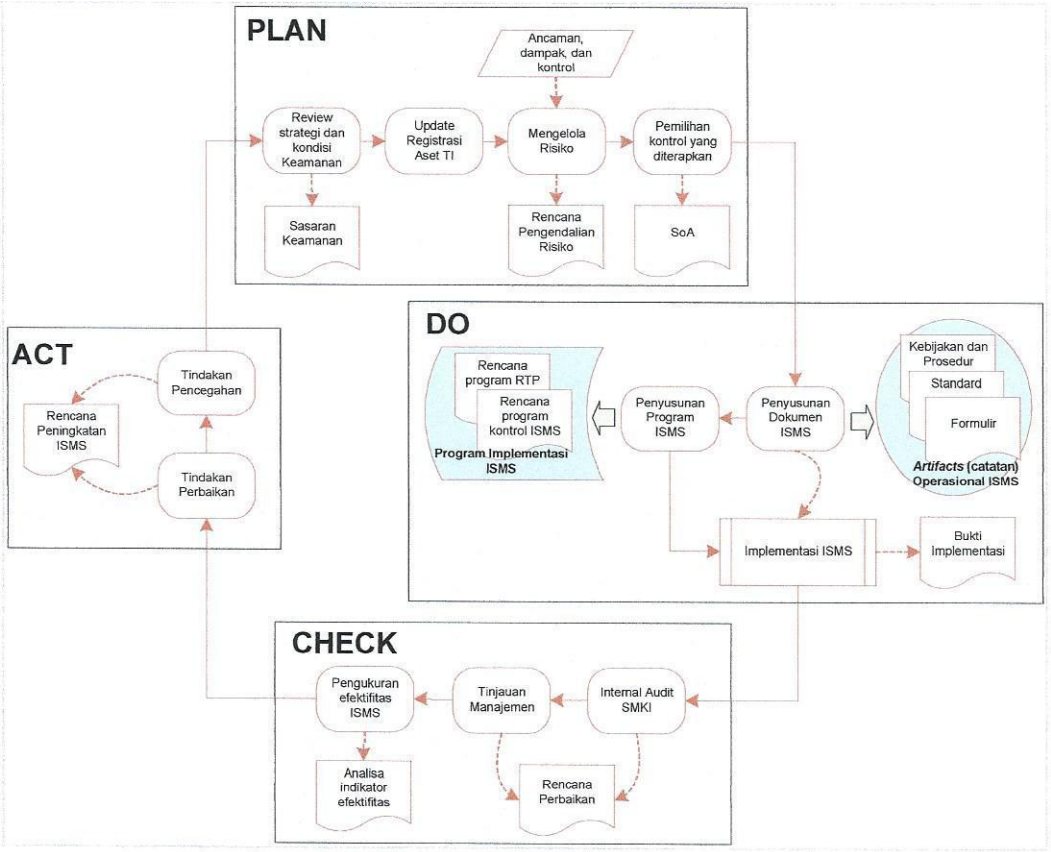
Pernyataan Kebijakan SMKI

PT EDII berkomitmen penuh untuk membentuk sebuah SMKI yang efektif dan efisien, serta selaras dengan strategi bisnis PT EDII dengan :

1. Mengembangkan, mengoperasikan, memonitor dan mengembangkan secara terus menerus SMKI perusahaan;
2. Mengembangkan, mengoperasikan, memonitor dan mengembangkan secara terus menerus kebijakan dan proses keamanan informasi perusahaan untuk menjamin keamanan informasi perusahaan dari ancaman baik dari pihak internal maupun eksternal;
3. Menjaga aspek kerahasiaan, integritas dan ketersediaan dari seluruh aset informasi milik perusahaan dari ancaman pihak internal maupun eksternal;
4. Memastikan bahwa SMKI perusahaan mendukung kebutuhan bisnis dan operasional perusahaan;
5. Mematuhi seluruh peraturan perundang-undangan, regulasi dan kewajiban kontrak yang berlaku;
6. Menyediakan sumber daya yang dibutuhkan untuk menjamin terciptanya SMKI perusahaan yang efektif dan efisien;
7. Mengembangkan dan memelihara *business continuity plan* perusahaan, untuk menjamin keberlangsungan dari layanan perusahaan;
8. Mengembangkan dan memelihara proses manajemen risiko terkait dengan keamanan informasi perusahaan;
9. Memastikan bahwa kebijakan ini dimengerti dan dijalankan di seluruh perusahaan, serta ditinjau dan dikembangkan secara terus menerus.

Kerangka Kerja Proses SMKI

Dalam pelaksanaan SMKI di PT. EDII, dilaksanakan proses P-D-C-A (*plan-do-check-act*) terhadap seluruh pemrosesan informasi dengan memperhatikan aspek *people*, *process,* dan *technology*.



Gambar 1. Konsep Pelaksanaan SMKI

- **Fase *Plan***

  Seluruh unit di PT. EDII bertanggung jawab atas terselenggaranya proses keamanan Informasi untuk melindungi informasi dan menjaga keberlangsungan bisnis perusahaan secara keseluruhan melalui pemahaman arahan dan tujuan keamanan informasi dengan menekankan penerapan kontrol SMKI.

  Perencanaan yang perlu diperhatikan meliputi:

a. Penetapan sasaran pelaksanaan manajemen keamanan informasi yang dievaluasi secara berkala setiap tahun;
b. Pendekatan yang akan dilakukan dalam mengenali, menilai dan mengelola risiko untuk mencapai tujuan yang ditetapkan;
c. Sumber daya, fasilitas dan anggaran yang diperlukan untuk mencapai tujuan operasional keamanan informasi yang ditetapkan;
d. Proses terhadap rencana penerapan kontrol keamanan informasi.

- **Fase *Do***

Untuk memastikan penerapan sistem manajemen keamanan informasi yang efektif di PT. EDII sesuai dengan kebijakan, kontrol, proses, dan prosedur yang telah dibentuk. Dalam proses penerapan harus :

a. Mengimplementasikan rencana penanganan risiko untuk mencapai kesesuaian terhadap objektif kontrol keamanan informasi.
b. Mengimplementasikan program pelatihan dan pemahaman proses sistem manajemen keamanan informasi.
c. Mengatur pengoperasian proses manajemen kontrol keamanan informasi.
d. Mengelola sumber daya untuk penerapan kontrol keamanan informasi antara lain termasuk anggaran yang diperlukan.
e. Mengimplementasikan kebijakan, prosedur, dan kontrol lain yang berfungsi untuk mengoperasikan manajemen keamanan informasi dan mendeteksi kelemahan pengamanan dan merespon sebuah insiden pengamanan.

- **Fase *Check***

Setiap unit di PT. EDII harus menetapkan, menerapkan dan memelihara proses untuk secara berkala memantau dan mengukur penerapan sistem manajemen keamanan informasi melalui:

a. Melakukan pengawasan dan pengkajian kontrol untuk:
   - mendeteksi insiden dalam proses keamanan informasi.
   - menilai apakah kontrol keamanan informasi yang dilakukan telah berjalan seperti yang diharapkan.
   - membantu dalam mendeteksi kelemahan pengamanan dan mencegah terjadinya insiden pengamanan akibat dari kelemahan yang ada.

- menentukan apakah tindakan perbaikan yang dilakukan untuk menanggulangi insiden telah berjalan dengan efektif.

b. Melakukan pengkajian efektivitas kontrol keamanan informasi secara berkesinambungan berdasarkan hasil audit, laporan insiden, serta saran dan masukan dari pihak-pihak yang terkait.
c. Melakukan *Review Risk Assessment* secara berkala.
d. Melaksanakan audit internal pada interval tertentu.
e. Melakukan tinjauan manajemen atas pelaksanaan ISMS setiap 1 tahun sekali untuk memastikan pelaksanaan keamanan informasi tetap berjalan dan mengidentifikasi peningkatan proses.

- **Fase *Act***

Setiap Unit di PT EDII secara kontinyu perlu meningkatkan sistem manajemen keamanan informasi dalam rangka menjaga dan melindungi informasi yang dikelola. Tindakan perbaikan dilakukan untuk menghilangkan penyebab ketidaksesuaian untuk mencegah terulangnya dari ketidaksesuaian yang dihadapi.

Proses peningkatan harus mendefinisikan:

a. Mengidentifikasi dan memperbaiki ketidaksesuaian (non conformity) dan mengambil tindakan untuk mengurangi dampak.
b. Mengimplementasikan tindakan yang sesuai dengan tujuan mencegah terulang kembali.
c. Mengkaji efektivitas dari tindakan perbaikan dan tindakan pencegahan untuk memastikan bahwa peningkatan mencapai objektif yang direncanakan.

Tujuan dan Sasaran SMKI

Tujuan SMKI

SMKI yang diterapkan di PT EDII bertujuan untuk:

- Mengembangkan, mengimplementasikan, memonitor, dan memperbaiki secara terus menerus sistem manajemen keamanan informasi dengan memastikan

tersedianya kebijakan dan proses yang dibutuhkan untuk menjamin terjaganya keamanan informasi di seluruh lingkungan PT. EDII.

- Menjaga aspek kerahasiaan, integritas, dan ketersediaan seluruh aset informasi dan aset lainnya milik PT. EDII terhadap risiko kehilangan, penyalahgunaan, pencurian, dan berbagai jenis kerusakan lainnya yang dapat menimbulkan kerugian bagi PT. EDII.
- Mematuhi seluruh peraturan perundang-undangan, regulasi, dan kewajiban kontrak yang berlaku.
- Menyediakan sumber daya yang dibutuhkan bagi pelaksanaan proses keamanan informasi PT. EDII dalam kondisi normal maupun darurat untuk menjamin keberlangsungan proses bisnis perusahaan.
- Mengembangkan dan mengimplementasikan proses manajemen risiko terkait dengan keamanan informasi dan selaras dengan rencana pengendalian risiko PT. EDII.

Sasaran SMKI

Sasaran sistem manajemen keamanan informasi ini merupakan panduan dalam proses pengukuran efektifitas dari SMKI di PT. EDII dalam rangka pencapaian tingkat keamanan yang memadai sbb :

No	Nama pengukuran (Metrik pengukuran)	Jenis Pengukuran	Frekuensi pengukuran	Ambang batas pengukuran
1	Pengetahuan dan pemahaman karyawan mengenai SMKI	Rasio karyawan yang memahami SMKI dibandingkan dengan jumlah seluruh karyawan	1 kali dalam 1 tahun	• Target tahun pertama >70% karyawan sudah memiliki pemahaman yang baik mengenai SMKI • Target tahun kedua dan seterusnya >90% karyawan sudah memiliki pemahaman yang baik mengenai SMKI
2	Efektifitas penegakkan (*enforcement*) dari kebijakan, standar, prosedur atau panduan keamanan informasi perusahaan	Jumlah pelanggaran keamanan informasi di perusahaan	1 kali dalam 1 tahun	• Target tahun pertama <10 pelanggaran per bulan • Target tahun kedua dan seterusnya <5 pelanggaran per bulan
3	Efektifitas dari SMKI serta kebijakan keamanan informasi perusahaan	Jumlah temuan dalam internal audit SMKI perusahaan	1 kali dalam 1 tahun	• Target tahun pertama <4 temuan major & 20 temuan minor • Target tahun kedua <2 temuan major & 15 temuan minor • Target tahun ketiga dan seterusnya <10 temuan minor

No	Nama pengukuran (Metrik pengukuran)	Jenis Pengukuran	Frekuensi pengukuran	Ambang batas pengukuran
4	Komitmen manajemen untuk meningkatkan pengetahuan dan pemahaman karyawan terkait SMKI	Rasio karyawan yang telah mengikuti pelatihan dan program peningkatan kesadaran serta kompetensi karyawan terkait SMKI	1 kali dalam 1 tahun	• Target tahun pertama >70% karyawan yang telah mengikuti pelatihan dan program peningkatan kesadaran serta kompetensi karyawan terkait SMKI • Target tahun kedua dan seterusnya >90% karyawan telah mengikuti pelatihan dan program peningkatan kesadaran serta kompetensi karyawan terkait SMKI
5	*Backup* informasi	Rasio jumlah aset informasi yang telah di-*backup* dengan jumlah seluruh aset informasi	1 kali dalam 1 tahun	• Target tahun pertama >60% aset informasi telah di-*backup* • Target tahun kedua dan seterusnya >80% aset informasi telah di-*backup*
6	Kepatuhan terhadap hak atas kekayaan intelektual	Rasio pelanggaran hak atas kekayaan intelektual dalam perangkat keras yang dimiliki perusahaan	1 kali dalam 1 tahun	• Target tahun pertama <15 pelanggaran • Target tahun kedua dan seterusnya <5 pelanggaran

No	Nama pengukuran (Metrik pengukuran)	Jenis Pengukuran	Frekuensi pengukuran	Ambang batas pengukuran
7	Komitmen pegawai dalam menjaga kerahasiaan informasi	Rasio karyawan yang telah menandatangani Surat Perjanjian Menjaga Kerahasiaan Informasi (NDA)	1 kali dalam 1 tahun	• Target tahun pertama >75% pegawai telah menandatangani NDA • Target tahun kedua dan seterusnya >95% pegawai telah menandatangani NDA
8	Tanggung jawab pegawai dalam penggunaan password	Rasio jumlah pegawai yang mengikuti ketentuan penggunaan password yang berkulitas	1 kali dalam 1 tahun	• Target tahun pertama >75% pegawai telah mengikuti ketentuan penggunaan password yang berkualitas • Target tahun kedua dan seterusnya >95% pegawai telah mengikuti ketentuan penggunaan password yang berkualitas

Sasaran pengamanan informasi ini harus ditinjau minimal satu kali dalam satu tahun dan apabila relevan dan memungkinkan perlu ditingkatkan secara terus menerus untuk mendorong peningkatan SMKI di PT EDII secara terus menerus.

Proses Manajemen Resiko

5.1.1. Penerapan Manajemen Risiko Keamanan Informasi

Tindakan pengendalian pengamanan informasi di PT EDII diterapkan berdasarkan penerapan manajemen risiko keamanan informasi yang perlu ditinjau secara berkala dengan mempertimbangkan hal-hal berikut:

- Proses bisnis yang dijalankan oleh PT. EDII;
- Tingkat kepentingan dan kritikalitas aset informasi dan pemrosesan informasi terhadap pelaksanaan proses bisnis;
- Lingkungan pemrosesan informasi;
- Tren insiden keamanan informasi;
- Tindakan pengendalian keamanan informasi yang sudah diterapkan;
- Dampak kerugian bisnis yang mungkin terjadi saat terjadi gangguan dan atau insiden keamanan informasi;
- Perhitungan secara reallistis mengenai kemungkinan terjadinya (*likelihood*) gangguan dan atau insiden keamanan informasi dengan memperhitungkan ancaman (*threats*), kerentanan (*vulnerability*) dan kontrol pengendalian keamanan informasi yang sudah diterapkan;
- Ketentuan perundang-undangan, regulasi, dan perjanjian kontrak yang terkait dengan keamanan informasi.

5.1.2. Keluaran Manajemen Risiko Keamanan Informasi

Manajemen risiko keamanan informasi diterapkan dengan hasil proses yang diharapkan antara lain:

- *Database* risiko keamanan informasi di PT. EDII.
- Penentuan penerimaan risiko keamanan informasi di PT. EDII.
- Rencana peningkatan tindakan pengendalian risiko keamanan informasi di PT. EDII.

Keluaran manajemen risiko harus mendapat persetujuan manajemen PT. EDII sebelum dapat diterapkan.

6. KEBUTUHAN DOKUMENTASI

Struktur Dokumentasi SMKI

Dalam implementasi Sistem Manajemen Keamanan Informasi (SMKI) di lingkup PT. EDII dibutuhkan seperangkat dokumen yang berisi aturan-aturan untuk memastikan bahwa proses SMKI dilaksanakan secara konsisten. Penerapan pengendalian dokumen PT. EDII yang

diberlakukan dalam implementasi ISO 27001:2013 disesuaikan dengan penerapan Sistem Manajemen lainnya yang telah dilaksanakan di lingkungan PT EDII (jika ada).

Pengendalian Dokumen

Dokumen yang diperlukan dalam pelaksanaan SMKI harus dilindungi dan dikendalikan. Seluruh dokumen SMKI harus mendapatkan persetujuan dari pimpinan unit kerja dalam lingkup SMKI atau Direksi PT EDII.

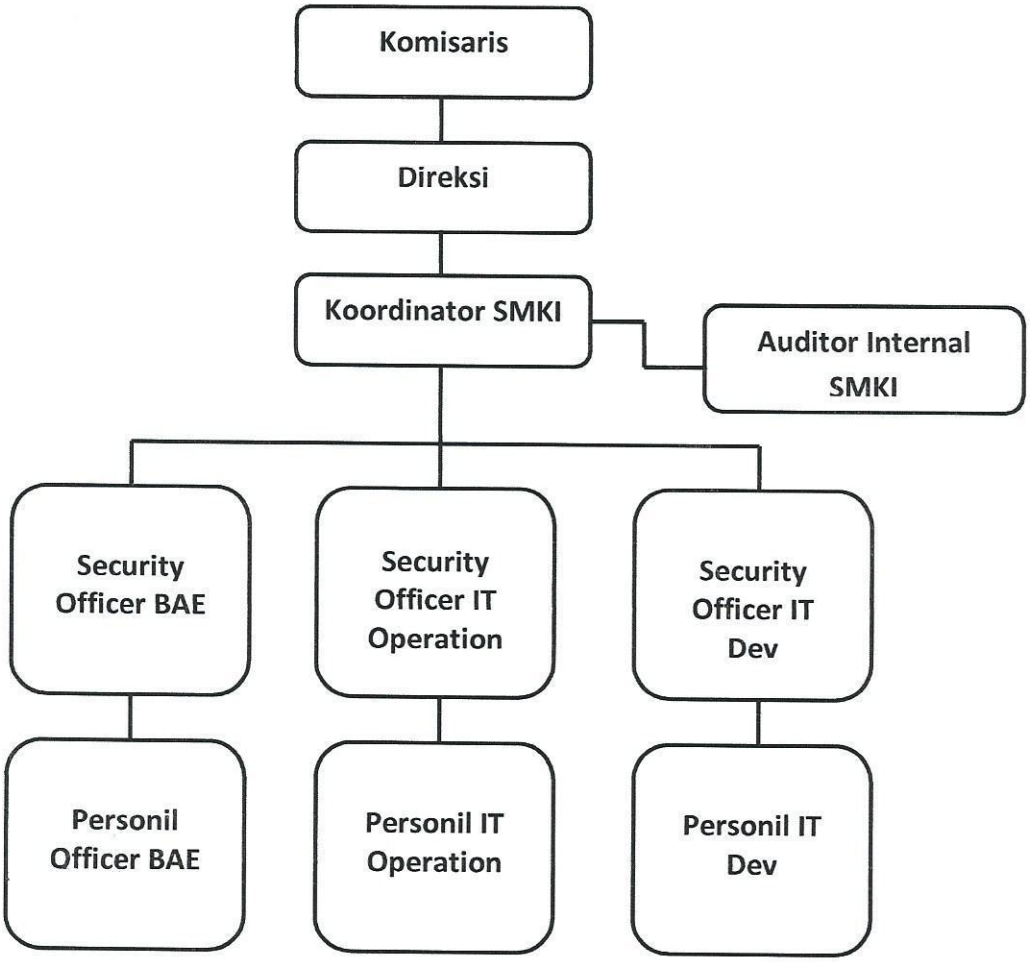
Pengendalian Rekaman / Catatan (*Record*) Pelaksanaan SMKI

Proses pengendalian rekaman/catatan pelaksanaan SMKI mencakup identifikasi, penyimpanan, perlindungan, pengambilan, masa simpan dan perlakuan terhadap dokumentasi. Rekaman / catatan pelaksanaan SMKI ditetapkan dan dipelihara untuk memberikan bukti kesesuaian pada implementasi SMKI khususnya pada pelaksanaan audit SMKI di PT EDII.

7. TANGGUNG JAWAB MANAJEMEN

Komitmen Manajemen

7.1.1 Struktur Organisasi SMKI



Gambar 3. Struktur Organisasi SMKI PT EDII

7.1.2 Wewenang dan Tanggung Jawab Organisasi SMKI

Pembagian tugas dan tanggung jawab organisasi SMKI di PT EDII dalam rangka proses pengamanan informasi sebagai berikut:

- Komisaris
    - Mengarahkan dan mengevaluasi kebijakan pengelolaan keamanan informasi;
    - Melakukan koordinasi dengan Direksi agar melaporkan evaluasi penyelenggaraan keamanan informasi;
    - Mengawasi upaya peningkatan pengendalian keamanan informasi.
- Direksi
    - Menetapkan kebijakan, sistem, dan prosedur keamanan informasi;
    - Mendukung semua aspek program keamanan informasi;
    - Menetapkan pembagian tugas dan tanggung jawab untuk pengambilan keputusan terkait manajemen risiko keamanan informasi;
    - Menetapkan tingkat risiko keamanan informasi yang dapat diterima;
    - Melakukan evaluasi terhadap hasil penetapan mitigasi risiko;
    - Memantau pelaksanaan perbaikan SMKI.;
    - Memastikan tersedianya sumber daya dalam pelaksanaan SMKI;
    - Mengkomunikasikan kepada seluruh unit di PT EDII mengenai pentingnya keamanan informasi.
- Koordinator SMKI / *Management Representative*
    - Mengkoordinasikan para *Security Officer* di setiap Unit dalam rangka memantau pengamanan informasi di unit PT EDII melalui pertemuan forum yang membahas status keamanan informasi secara berkala;
    - Membuat program kerja pelaksanaan SMKI;
    - Mengkoordinasikan pelaksanaan *Risk Assessment*;
    - Memastikan dilakukannya audit internal terhadap pelaksanaan SMKI;
    - Mengkoordinasikan pengukuran efektivitas kontrol implementasi SMKI;
    - Melaporkan perkembangan pelaksanaan SMKI kepada Direksi PT EDII;
    - Meninjau dan memperbaharui kebijakan dan prosedur SMKI sesuai dengan kebutuhan dan perkembangan pemanfaatan TI.
- *Security Officer*

- Supervisi dan *monitoring* pelaksanaan SMKI di masing-masing unit;
- Mengkomunikasikan pentingnya pencapaian tujuan dan pelaksanaan kesesuaian terhadap kebijakan pengamanan informasi kepada unit lain yang terkait;
- Melaksanakan program *security awareness* terkait SMKI untuk personil unit;
- Melaksanakan *Risk Assessment* di unit;
- Memantau pengukuran efektivitas kontrol implementasi SMKI di unit;
- Memberikan laporan mengenai pelaksanaan SMKI kepada Koordinator SMKI;
- Membantu koordinasi pengujian BCP.

- *Internal Auditor* SMKI
  - Melaksanakan internal audit SMKI di PT EDII secara berkala;
  - Mengajukan saran atas tindakan perbaikan yang harus dilakukan;
  - Membuat laporan internal audit.
- Personil
  - Melaksanakan proses pengamanan informasi dalam rangka SMKI;
  - Melaporkan potensi insiden, insiden, serta ketidaksesuaian terkait dengan SMKI sesuai ketentuan yang ditetapkan.

Manajemen Sumber Daya dan Pelatihan

7.2.1 Penyediaan Sumber Daya

Manajemen PT EDII harus memastikan ketersediaan sumber daya yang diperlukan agar pelaksanaan SMKI dalam rangka menjaga efektifitas keamanan informasi terkait dengan perencanaan mitigasi risiko dan pelaksanaan kontrol keamanan informasi.

Penyediaan sumber daya tersebut termasuk penyediaan sarana pelatihan bagi seluruh personil PT EDII untuk memastikan kompetensi yang mendukung tanggung jawab dalam pelaksanaan SMKI dan melaksanakan tugas-tugas yang diperlukan. Proses efektifitas setiap pelatihan yang dilakukan mengacu kepada penilaian yang sudah diterapkan di PT EDII.

8. AUDIT INTERNAL SMKI

Audit internal SMKI harus diadakan minimal 1 (satu) kali dalam setahun dengan mencakup keseluruhan lingkup SMKI yang ditetapkan dalam dokumen ini dan dilaksanakan oleh Tim Internal Audit SMKI PT. EDII.

Tujuan pelaksanaan Audit Internal SMKI adalah untuk mengidentifikasi ketidaksesuaian beserta penyebabnya sesegera mungkin. Manajemen PT. EDII harus memastikan efektifitas tindak lanjut yang dilakukan untuk menjaga kelangsungan proses keamanan informasi berikutnya.

9. TINJAUAN MANAJEMEN SMKI

Manajemen PT. EDII wajib melakukan tinjauan terhadap pelaksanaan SMKI dalam interval 1 tahun sekali. Hasil tinjauan manajemen ini digunakan untuk mengevaluasi kondisi pelaksanaan keamanan informasi yang telah dilakukan dan menentukan peningkatan terhadap implementasi SMKI.

Hasil tinjauan manajemen harus didokumentasikan dengan jelas dan catatan-catatan yang berkaitan dengannya harus dipelihara dengan baik.

10. PENINGKATAN SMKI

10.1. *Continual Improvement*

Manajemen PT. EDII secara berkelanjutan meningkatkan efektivitas SMKI melalui penggunaan kebijakan SMKI, objektif pengamanan informasi, hasil audit, analisis terhadap database insiden, tindakan perbaikan dan pencegahan serta tinjauan manajemen.

10.2. Tindakan Perbaikan dan Pencegahan

PT. EDII harus menentukan tindakan untuk menghilangkan penyebab dari insiden atau potensi insiden keamanan informasi. Mekanisme dalam pelaksanaan tindakan perbaikan dan pencegahan terhadap suatu ketidaksesuaian yang terjadi mengacu ke proses pada sistem manajemen di PT. EDII.

11.*COMPLIANCE*

Penggunaan aset informasi dan aset pemrosesan informasi harus disertai dengan kesadaran user mengenai ketentuan pengamanan informasi yang berlaku dan memahami kewajibannya sesuai dengan aturan yang ada yang mencakup:

- Peraturan dan undang-undang terkait informasi dan sistem informasi;
- Surat keputusan dewan direksi;
- Kebijakan keamanan informasi PT. EDII;
- Standar dan prosedur pengelolaan informasi dan teknologi informasi PT. EDII

12.*DOMAIN* KEAMANAN INFORMASI

Sistem manajemen keamanan informasi yang diterapkan di PT. EDII disusun berdasarkan standar ISO 27001 dan mengatur pengelolaan domain – domain kontrol keamanan informasi sebagai berikut:

1. **Kebijakan Keamanan Informasi**, mencakup pemastian tersedianya kebijakan keamanan informasi yang disetujui, dikomunikasikan, dan ditinjau secara berkala.
2. **Organisasi Keamanan Informasi**, mencakup penerapan keamanan informasi dalam berkoordinasi dan bekerjasama baik dengan pihak internal maupun eksternal.
3. **Manajemen Aset**, mencakup tata kelola aset meliputi tanggung jawab, penggunaan, hingga pemusnahan aset informasi dan aset pemrosesan informasi.
4. **Keamanan Sumber Daya Manusia**, mencakup pengelolaan sumber daya manusia dalam menerapkan pengamanan informasi.
5. **Pengamanan Fisik dan Lingkungan**, mencakup pengamanan aset informasi dan aset pemroses informasi dari ancaman fisik dan lingkungan.
6. **Manajemen Komunikasi dan Operasional Sistem Informasi**, mencakup pengaturan keamanan aset informasi dan aset pemroses informasi selama digunakan dalam operasional bisnis dan komunikasi bisnis.
7. **Pengendalian Akses**, mencakup pembatasan akses logikal sesuai kebutuhan bisnis terhadap jaringan, sistem operasi, aplikasi, dan informasi.

8. **Pengadaan, Pengembangan, dan Pemeliharaan Sistem Informasi**, mencakup pengaturan keamanan informasi dalam aplikasi.
9. **Manajemen Insiden Keamanan Informasi**, mencakup pengelolaan insiden dan potensi insiden keamanan informasi dalam hal pelaporan, analisa, penanganan, tindakan perbaikan dan pencegahan, dan evaluasi efektivitas penanganan insiden.
10. **Manajemen Keberlangsungan Bisnis**, mencakup analisa, perencanaan, pengujian, *review*, dan perbaikan atas kebutuhan kelangsungan bisnis dan rencana pemulihannya pada saat terjadi kondisi darurat atau bencana.
11. **Kepatuhan (*complience*)**, mencakup komitmen PT. EDII untuk mematuhi aturan-aturan keamanan informasi sesuai dengan yang diatur dalam peraturan, undang-undang, perjanjian, dan kebutuhan bisnis yang berlaku.

Bagi setiap domain keamanan informasi yang telah dijabarkan dalam dokumen ini akan disusun kebijakan dan prosedur terkait dalam bentuk dokumen prosedur terkait keamanan informasi.

13.PENINJAUAN DOKUMEN KEBIJAKAN SMKI DAN KEAMANAN INFORMASI

Dokumen kebijakan SMKI dan keamanan informasi ini harus ditinjau minimal satu kali dalam satu tahun dan/atau apabila terjadi perubahan signifikan terhadap perusahaan, sistem manajemen keamanan informasi dan keamanan informasi di PT. EDII.

Peninjauan dokumen ini dikoordinasikan oleh *Management Representative* dan hasilnya harus didokumentasikan.