[PT XYZ]

KEBIJAKAN KEAMANAN INFORMASI

Code:	
Version:	1.0
Tanggal:	September 2013
Dibuat oleh:	HWS
Disetujui oleh:	
Tingkat kerahasiaan:	

Riwayat Perubahan

Tanggal	Versi	Dibuat Oleh	Penjelasan
31/08/2013	1.0	Helvry WS	Sistem Manajemen Keamanan Informasi

Daftar Isi

1. Pendahuluan

Informasi adalah aset bagi organisasi. Karena itu organisasi berkewajiban dan bertanggung jawab untuk melindunginya. Ketersediaan informasi yang lengkap dan akurat merupakan hal yang sangat penting untuk mendukung fungsi organisasi yang terkait dengan penyediaan kebutuhan informasi bagi pihak internal maupun eksternal organisasi. Dalam kaitannya memroses informasi, organisasi memiliki tanggung jawab untuk mengamankan informasi dan mencegah penyalahgunaan informasi.

Hal penting yang patut dilakukan adalah menselaraskan antara risiko keamanan informasi dengan risiko bisnis perusahaan secara keseluruhan. Karena itu dengan penyerasian sistem keamanan informasi dengan strategi penanganan risiko bisnis, dapat menunjang keefektifan manajemen risiko perusahaan.

2. Tujuan, lingkup, dan pengguna

Tujuan kebijakan ini adalah untuk mendefinisikan tujuan, prinsip-prinsip dasar terkait dengan manajemen sistem keamanan informasi. Tujuan pengendalian keamanan informasi adalah melindungi perusahaan maupun reputasi perusahaan dengan pemliharaan hal-hal sebagai berikut:

- *Confidentiality* (kerahasiaan) : mengetahui bahwa data dan informasi dapat diakses oleh hanya orang-orang yang berhak melakukannya.
- *Integrity (*Integritas) : mengetahui bahwa data dan informasi adalah akurat dan up-to-date (mutakhir) dan tidak terdapat kesengajaan maupun ketidaksengajaan pemodifikasian data dan informasi dari versi yang disetujui sebelumnya.
- *Availibily* (Ketersediaan) *:* mengetahui bahwa data dan informasi dapat diakses kapan saja.

Kebijakan ini diterapkan ke seluruh sistem manajemen keamanan informasi (SMKI).

Organisasi dan Lokasi:
Seluruh unit kerja terkait di perusahaan dan lokasi kerja yang digunakan untuk mengelola dan menyediakan layanan internal dan eksternal .

Aset yang dicakup meliputi, tetapi tidak terbatas pada:

- Data dan Informasi

  Termasuk data dan informasi meliputi:dokumen pengadaan dan kontrak, data pelanggan, data gaji, data karyawan, sistem dokumentasi manajemen, dokumen teknis &konfigurasi jaringan, hasil penetration test, materi pelatihan, prosedur operasional, business continuity plan, dan hasil audit;

- Software

  Yang termasuk dalam aset perangkat lunak atau software antara lain : software aplikasi, operating system, development tool, dan software tool (antivirus, audit tool);

- Hardware

  Yang termasuk dalam aset perangkat keras atau hardware misalnya :Server, PC, Laptop, media penyimpan data;

- Perangkat Jaringan Komunikasi
  Yang termasuk dalam aset perangkat jaringan komunikasi antara lain Router, Modem, Switch, Kabel, Firewall

- Fasilitas Pendukung

Yang termasuk dalam aset fasilitas pendukung antara lain Ruang Server / Ruang Data Center, Ruang Kerja, Ruang Disaster Recovery Center (DRC), UPS, Genset, A/C, CCTV, Fire Extinguisher, Access Door Electronic, dan sebagainya;

- Sumber Daya Manusia

  Yang termasuk dalam aset sumber daya manusia misalnya karyawan tetap, calon karyawan tetap, karyawan kontrak, mitra, vendor dan pihak ketiga lainnya yang menyediakan layanan, jasa, serta produk yang menunjang bisnis Instansi penyelenggara layanan publik.

Pengguna dokumen kebijakan ini adalah seluruh karyawan PT XYZ dan pihak eksternal yang memiliki peran dalam Sistem Manajemen Keamanan Informasi, termasuk:

- Karyawan tetap, karyawan paruh waktu (part-time), karyawan magang, atau karyawan yang bekerjauntukdan atas nama PT XYZ;
- Mahasiswa yang melakukan penelitian/karya tulis di perusahaan;
- Rekanan atau pihak ketiga,konsultan yang bekerja untuk dan atas nama perusahaan;
- Seluruh individu maupun grup yang diberikan akses oleh perusahaan terhadap jaringan perusahaan maupun layanan teknologi informasi.

3. Dokumen Referensi

- ISO/IEC 27001 standard,
- ISO/IEC 13335-1:2004

4. Terminologi keamanan informasi*

Confidentiality - the property that information is not made available or disclosed to unauthorised individuals, entities, or processes

Integrity - the property of safeguarding the accuracy and completeness of assets

Availability - the property of being accessible and usable upon demand by an authorized entity

Information security - preservation of confidentiality, integrity and availability of information

Information Security Management System - that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security

* definitions taken from ISO/IEC 27001:2005

5. Pengorganisasian Keamanan Informasi

Untuk menunjang keberhasilan penerapan sistem keamanan informasi, pihak manajemen harus mendukung dalam bentuk pengorganisasian keamanan informasi yang jelas.

5.1. Tujuan dan Ruang Lingkup

Tujuan pengorganisasian keamanan informasi adalah untuk mengatur dan mengelola keamanan informasi di PT XYZ. Ruang lingkup pengorganisasian keamanan informasi ini dibatasi pada divisi teknologi informasi untuk kemudian dapat dikembangkan di seluruh unit kerja di PT XYZ.

5.2. Kontrol

Kontrol yang berkaitan dengan pengorganisasian keamanan informasi adalah sebagai berikut:

a. pada setiap unit kerja ditunjuk personil yang bertanggung jawab untuk memonitor keamanan informasi pada unitnya berkoordinasi dengan *security officer.*
b. Usulan masukan pengamanan informasi dilakukan secara berkala oleh penanggung jawab keamanan kepada *security officer.*
c. Jika terjadi pelanggaran keamanan, pengguna dapat melaporkan kepada penanggung jawab pada bagiannya, untuk diteruskan kepada security officer, untuk mendapatkan tindak lanjut.
d. Jika permasalahan tersebut tidak dapat diselesaikan oleh security officer atau permasalahan tersebut dinilai memilki risiko tinggi terhadap sistem keamanan informasi, maka dilaporkan kepada security head untuk diambil keputusan.

6. Manajemen Risiko

Manajemen risiko merupakan pondasi dari sebuah sistem manajemen keamanan informasi. Manajemen risiko adalah proses mengidentifikasi risiko, menilai kemungkinan keterjadiannya, lalu kemudia mengambil langkah untuk mengurangi risiko hingga ke level diterima (mitigasi). Beberapa langkah-langkah manajemen risiko adalah sebagai berikut:

6.1. Kepemilikan dan Pemeliharaan Kebijakan

Kebijakan ini dimiliki oleh divisi teknologi informasi, dipelihara, direview dan diubah oleh divisi teknologi informasi bersama dengan internal audit sesuai dengan kebijakan perusahaan, prosedur, dan panduan.
Kebijakan ini akan dilakukan review secara periodik (tahunan) dan diajukan kemana komite audit bila terjadi perubahan substansial atau melakukan pemodifikasian konsep kebijakan agar sesuai dengan kebutuhan yang relevan maupun pengelolaan yang efektif.

6.2. Tujuan dan Ruang Lingkup

Menentukan tujuan dan ruang lingkup manajemen risiko adalah langkah untuk melakukan penilaian risiko. Mengidentifikasi aset, mengidentifikasi lokasi aset, dan mengidentifikasi detil sistem informasi lain yang akan dinilai. Hasil dari analisis risiko akan menjadi dasar melakukan proses manajemen risiko. Elemen utama dari manajemen risiko adalah:

- Pengidentifikasian aset informasi
- Analisis kerentanan *(vulnerability)*
- Pengidentifikasian ancaman *(threat)*
- Penentuan kemungkinan keterjadian *(likelihood)*
- Penentuan nilai risiko

- Pemilihan kontrol untuk memitigasi risiko
- Rencana kegiatan saat genting

Ruang lingkup manajemen risiko ini hanya diimplementasikan pada risiko yang berhubungan dengan aset informasi.

6.3. Dokumen terkait

- ISO 27001
- Database pengguna
- Prosedur instruksi kerja

6.4. Prosedur

6.4.1. Pengidentifikasian aset informasi

Sehubungan dengan berkembangnya bisnis dan teknlogi, menyebabkan dapat berubah atau bergantinya aset yang dimiliki. Untuk itu, sangat penting untuk melakukan monitoring terhadap perkmbangan aset yang dimiliki. Daftar aset tersebut memuat informasi sebagai berikut:

- Kelompok Aset
- Nama aset
- Penanggung jawab aset
- Pengguna Aset
- Lokasi Aset
- Dampak terhadap sistem

Menurut ISO 27001, kelompok aset dibagi sebagai berikut:

- Informasi *(information)*;
- Perangkat lunak *(software)*;
- Perangkat keras *(hardware)*;
- Perlengkapan umum *(services)*;
- Sumber daya manusia *(people)*; dan
- Aset tak berwujud *(intangible assets)*.

Nama aset harus tertulis dengan jelas. Identifikasi berupa kode barang inventaris aset dapat ditambahkan. Penanggung jawab aset juga harus tertulis dengan jelas (meski secara umum aset tersebut adalah aset perusahaan). Nama pengguna aset harus tertulis dengan jelas termasuk karyawan, klien, dan rekan bisnis PT XYZ. Lokasi aset harus menunjukkan dimana aset tersebut berada dalam lingkup perusahaan. Keterangan pengguna aset maupun lokasi aset harus dilakukan pemutakhiran sesuai kondisi terakhir.

Dampak aset terhadap sistem diberikan nilai untuk memperlihatkan seberapa besar dampak yang mungkin ditimbulkan. Penilaian dampak aset terhadap sistem dapat dilakukan oleh *security officer*, namun direview secara berkala oleh *IT Head*. Setiap kali analisis risiko dilakukan, hasil analisis sebelumnya dapat dilakukan evaluasi. Penilaian dampak aset terhadap sistem dapat dilihat pada tabel berikut.

Nilai	Penjelasan
0	Aset bukan merupakan bagian dari sistem manajemen keamanan informasi. Contoh AC
1	Aset tidak memiliki peran penting dalam sistem keamanan informasi, tapi jika ada kerusakan harus segera diperbaiki. Cth. Monitor dan keyboard
2	Aset memiliki peran penting terhadap sistem keamanan informasi, jika rusak harus segera diperbaiki atau diganti.
3	Aset sangat penting (critical)
4	Asat sangat sangat penting (super critical). Cth

6.4.2. Analisis kerentanan

Berdasarkan daftar aset yang telah dibuat, *security officer* bersama *system administrator*, dan *security leader* membuat daftar kerentanan aset. Daftar tersebut harus memuat aspek teknis, aspek organisasi, dan fitur aset yang potensial bagi lolosnya ancaman. Kegiatan penganalisisan kerentanan tersebut harus dikerjakan secara hati-hati. Kesalahan dalam menganalisis akan menyebabkan sistem akan memiliki celah keamanan *(insecure)*.

6.4.3. Pengidentifikasian ancaman

Daftar aset beserta kerentanannya akan menjadi dasar bagi *security officer* dalam membuat daftar ancaman *(threat list)*. Hasil pengidentifikasian ancaman dapat dipisahkan dalam dokumen katalog sebagai bahan evaluasi analisis risiko di kemudian hari. Informasi dari katalog tersebut dapat dipertukarkan dengan klien dan pihak ketiga untuk memastikan bahwa sistem keamanan informasi telah terproteksi.

6.4.4. Penentuan kemungkinan keterjadian (likelihood)

Setiap ancaman memiliki kemungkinan keterjadian. Kegiatan ini dapat dilakukan oleh security officer bersama security leader dan system administrator. Nilai yang diberikan antara 0 sampai dengan 5 yang menggambarkan jumlah keterjadian. Contoh skoring jumlah keterjadian dapat dilihat pada tabel berikut.

Nilai	***Penjelasan***
0	*Dapat diabaikan*
1	*Kemungkinan keterjadiannya kecil*
2	*Kemungkinan keterjadiannya sedang*
3	*Kemungkinan keterjadiannya besar*
4	*Kemungkinan keterjadiannya sangat besar dalam segala situasi*
5	*Dapat diabaikan*

6.4.5. Penentuan nilai risiko

Nilai risiko adalah hasil perkalian antara nilai aset dengan kemungkinan keterjadian *(likelihood)*. Dari hasil perkalian tersebut dapat ditentukan mana risiko yang tinggi, sedang, dan rendah. Jika risiko dinilai tinggi maka tindakan pencegahan harus dilakukan, jika risiko dinilai sedang, maka tindakan

pengamanan dapat diturunkan, namun tetap dilakukan. Jika risiko dinilai rendah, maka tidak perlu ada tindakan pengamanan, namun tetap mengontrolnya. Tabel nilai risiko tersebut dapat dilihat pada tabel berikut.

Skoring		**Likelihood**
1	Sangat kecil	Dapat diabaikan
2	Kecil	Kemungkinan keterjadiannya kecil
3	Sedang	Kemungkinan keterjadiannya sedang
4	Besar	Kemungkinan keterjadiannya besar
5	Sangat besar	Kemungkinan keterjadiannya sangat besar dalam segala situasi

6.4.6. Pemilihan kontrol untuk memitigasi risiko

Berdasarkan nilai risiko di atas, harus disusun langkah-langkah untuk mengimplementasikan perlindungan terhadap risiko secara spesifik. Risiko tinggi harus ditekan hingga risiko tersebut dapat diterima *(accepted risk).* Untuk risiko sedang dan rendah, harus ditentukan juga kontrol yang tepat untuk menanganinya.

6.4.7. Rencana kegiatan saat genting

Dari hasil analisis risiko pada prosedur di atas, dapat disusun rencana kegiatan saat genting *(contingency plan).* Rencana tersebut menjelaskan mengenai tindakan apa yang mesti diambil pada saat kritis agar organisasi dapat terus melangsungkan operasionalnya. Rencana tersebut harus menginformasikan nama-nama orang atau insitusi yang harus dihubungi ketika terjadi hal genting. Selain itu, dapat dibuat daftar aset penting dan bersama IT Head menentukan dimana menempatkan aset penting tersebut agar aman dan terjamin hingga masa-masa kritis terlewati.

7. Kebijakan Keamanan Personil

7.1. Tujuan dan Ruang Lingkup

Tujuan kebijakan keamanan personil adalah untuk memastikan bahwa karyawan, klien, dan pihak ketiga memahami tugas dan tanggung jawabnya sesuai dengan kepentingannya untuk meminimalisasi risiko pencurian informasi dan penyalahgunaan wewenang. Ruang lingkup pengorganisasian keamanan informasi ini dibatasi pada divisi teknologi informasi untuk kemudian dapat dikembangkan di seluruh unit kerja di PT XYZ.

Untuk keperluan tujuan pengguna dari kebijakan ini adalah pengguna dari layanan teknologi informasi yang disediakan oleh perusahaan, yang menjadi salah satu kelompok berikut:

- Karyawan perusahaan: yaitu orang-orang yang menjadi karyawan tetap perusahaan.
- Karyawan magang : yaitu orang yang mendapat izin magang bekerja di perusahaan.

- Mahasiswa : yaitu orang yang mendapat izin melakukan penelitian untuk keperluan penulisan karya tulis ilmiah seperti jurnal, skripsi, tesis, dan sebagainya.
- Tamu : yaitu orang-orang yang mendapatkan izin sementara untuk mengakses layanan maupun fasilitas teknologi informasi dari perusahaan.
- Pengguna eksternal : yaitu pihak ketiga/rekanan/kontraktor yang diberikan izin akses pada sistem TI perusahaan untuk keperluan pengembangan aplikasi, pemeliharaan data center, jaringan perusahaan.

Terkait dengan pegawai baru atau pihak-pihak dari luar perusahaan yang bekerja sementara di perusahaan, maka divisi sumber daya manusia harus memastikan agar:

- Perjanjian kerahasiaan menjadi bagian dari syarat dan ketentuan perjanjian kerja.
- Informasi atas latar belakang karyawan diperiksa dan tersimpan dengan baik.
- Untuk uraian pekerjaan yang spesifik akan peran keamanan informasi, dilakukan pemeriksaan yang mendalam atas calon karyawan.
- calon karyawan mengerti akan pentingnya keamanan informasi, dan bagi calon karyawan yang belum pernah mendapat training keamanan informasi, diberikan jadwal pelatihan bagi mereka.
- Untuk pihak luar seperti auditor diberikan jangka waktu akses ke sistem dan jaringan teknologi informasi sepanjang waktu penugasannya di perusahaan.

Terkait dengan pegawai yang meninggalkan perusahaan, maka divisi teknologi informasi harus memastikan agar:

- Seluruh *IT account* ditutup bagai karyawan yang berhenti/meninggalkan perusahaan.
- Seluruh files, folder segera dihapus setelah pengguna selesai masa tugasnyadi perusahaan.
- Bila seorang *user* ditingkatkan accountnya menjadi lebih tinggi, maka IT account yang lama segera dihapus, dan untuk migrasi account tersebut harus seizin tertulis dari atasannya atau seizin dari kepala divisi IT.

7.2. Kontrol

Kontrol yang berkaitan dengan kebijakan keamanan personil adalah sebagai berikut:

a. Seluruh karyawan, klien, dan pihak ketiga yang menggunakan fasilitas yang berhubungan dengan aset informasi harus menandatangani perjanjian kerahasiaan *(non disclosure agreement).*
b. Seluruh karyawan mesti tunduk pada syarat dan ketentuan-ketentuan tertulis perusahaan ketika mereka mendaftar untuk memperoleh IT account. Prosedur pendaftaran untuk memperoleh IT account dilakukan oleh subdivisi layanan dukungan TI. Dokumentasi atas persetujuan tersebut disimpan oleh team administrasi subdivisi layanan dukungan TI.
c. Pelatihan prosedur keamanan dan penggunaan aset yang berhubungan informasi dilakukan secara berkala atau disosialisasikan melalui media *intranet* perusahaan.
d. Bagi karyawan, klien, maupun pihak ketiga yang telah selesai menggunakan aset informasi perusahaan harus menyerahkan kembali aset tersebut dengan menggunakan berita acara pengembalian aset.

e. Bagi karyawan, klien, dan pihak ketiga yang melanggar perjanjian kerahasiaan maupun prosedur keamanan perusahaan dapat ditindak sesuai dengan ketentuan perusahaan.
f. Bagi tamu yang datang harus mengisi daftar buku yang tamu (minimal berisi informasi nama, tanggal, dan keperluan). Dokumentasi buku tamu tersebut harus dikelola oleh team administrasi subdivisi dukungan layanan TI.
g. Akses yang dilarang untuk digunakan oleh tamu meliputi: sistem jaringan perusahaan, sumber daya elektronik yang sensitif, e-mail server perusahaan, akses file dan folder di PC perusahaan.
h. Untuk tamu dibedakan PC dan jaringan (contoh wifi khusus guest).

8. Kebijakan keamanan fisik dan lingkungan

8.1. Tujuan dan Ruang Lingkup

Tujuan kebijakan keamanan fisik dan lingkungan adalah untuk memastikan bahwa aset informasi bebas dari masuknya pihak yang tidak berhak, pencegahan terhadap kerusakan dan kehilangan aset informasi. Ruang lingkup pengorganisasian keamanan informasi ini dibatasi pada divisi teknologi informasi untuk kemudian dapat dikembangkan di seluruh unit kerja di PT XYZ.

8.2. Kontrol

Kontrol yang berkaitan dengan kebijakan keamanan fisik dan lingkungan adalah sebagai berikut:

a. Akses untuk memasuki infrastruktur informasi PT XYZ harus dikontrol. Karena itu, personil maupun vendor yang ditunjuk dan diotorisasi oleh *security manager* yang dapat mengakses area fisik informasi yang sifatnya sensitif.
b. Pengamanan area fisik meliputi batas fisik antara ruang kerja dan ruang publik (ruang rapat, ruang tunggu tamu, ruang kerja pihak ketiga, pintu darurat).
c. karyawan, klien, dan pihak ketiga diberi otorisasi tertentu untuk mengakses tempat kerja dan *data center*.
d. Berkaitan dengan akses terhadap area yang sensitif terhadap kerentanan gangguan informasi hanya diberikan kepada personil tertentu dengan izin tertulis *security head.*
e. Peralatan CCTV terpasang pada area yang sensitif terhadap kerentanan gangguan informasi terpasang sesuai dengan standar. Peralatan tersebut harus diuji secara berkala untuk memastikan operasionalnya dengan baik.
f. Buku petunjuk internal yang menginformasikan area aset-aset informasi yang sensitif dipastikan agar tidak terakses oleh publik dengan mudah.
g. Personil pihak ketiga dapat diberikan akses terbatas ke area aset informasi yang sensitif jika diberikan izin oleh *security head.*
h. Verifikasi terhadap latar belakang pihak ketiga yang dipekerjakan oleh divisi IT antara lain: ijazah, transkrip nilai, tanda pengenal. Pengenalan yang baik akan latar belakang pihak ketiga akan mengurangi risiko pelanggaran keamanan informasi.
i. Saluran listrik dan telekomunikasi ke area aset-aset informasi yang sensitif harus dipantau secara berkala.
j. Dokumentasi petunjuk perlindungan dari penyedia aset informasi terinformasi dengan baik.

9. Kebijakan manajemen aset

9.1. Tujuan dan Ruang Lingkup

Tujuan kebijakan manajemen aset adalah memastikan kelengkapan dan kebenaran data untuk aset perangkat keras dan aset jaringan komunikasi yang digunakan oleh divisi IT. Ruang lingkup manajemen aset ini dibatasi pada aset yang menjadi tanggung jawab divisi IT.

9.2. Kontrol

Kontrol yang berkaitan dengan manajemen aset adalah sebagai berikut:

a. Menentukan orang/fungsi yang bertanggung jawab atas pengelolaan aset di divisi IT.
b. Menghitung jumlah aset yang menjadi tanggung jawab divisi IT yang terdaftar di database register aset.
c. Mengumpulkan data aset perangkat keras dan aset jaringan komunikasi yang terdaftar di database aset.
d. Melakukan pengecekan dengan observasi ke masing-masing personil dengan melihat apakah kepemilikan aset telah sesuai dengan database aset.
e. Melakukan pengecekan fisik dengan observasi ke personil pihak ketiga yang dipekerjakan divisi IT dengan melihat apakah penguasaan aset oleh pihak ketiga sesuai dengan database aset.

10.Kebijakan penanganan media

10.1. Tujuan dan Ruang Lingkup

Tujuan kebijakan penanganan media ini untuk menghindari rusak dan hilangnya disks, tapes, dan removable media lainnya yang dapat merugikan perusahaan. Ruang lingkup penanganan media ini dibatasi pada divisi IT.

10.2. Kontrol

Kontrol yang berkaitan dengan penanganan media adalah sebagai berikut:

a. Media yang tidak diperbolehkan adalah yang mempunyai port USB.
b. Media penyimpanan yang di dalamnya terdapat informasi perusahaan, dibutuhkan untuk tujuan bisnis tertentu.
c. Bila tujuan bisnis telah terpenuhi,maka informasi dalam media penyimpan harus dimusnahkan dan tidak dapat dipulihkan kembali.
d. Media penyimpan secara fisik seharusnya dilindungi dari kehilangan, kerusakan, penyalahgunaan ketika digunakan.
e. Kegiatan audit perlu dilakukan untuk memastikan dilakukannya kebijakan ini.pelanggaran akan kebijakan tersebut akan dilaporkan pada atasan langsung dan diproses sesuai dengan peraturan/perjanjian.
f. Semua insiden yang melibatkan media penyimpan, harus dilaporkan kepada *security manager* dan diproses sesuai dengan prosedur pelaporan insiden.

11.Kebijakan pertukaran informasi

11.1. Tujuan dan Ruang Lingkup

Tujuan kebijakan pertukaran informasi adalah untuk memberikan petunjuk pada seluruh karyawan, klien, maupun pihak ketiga dalam kaitannya dengan perlindungan informasi rahasia milik perusahan, klien, dan pihak ketiga. Ruang lingkup manajemen aset ini dibatasi pada divisi IT, klien dan pihak ketiga yang berhubungan dengan divisi IT.

11.2. Kontrol

a. Pertukaran informasi melalui jaringan harus dilengkapi dengan kontrol untuk memastikan bahwa semua informasi yang dikirim dapat diterima dan setiap modifikasi selama transmisi dapat dideteksi dan dilaporkan.
b. Semua pengiriman informasi pada pihak ketiga, tidak hanya penerima yang harus memiliki otorisasi untuk menerima informasi tersebut,tetapi prosedur pengamanannya harus dapat diyakini.

12.Kontrol akses jaringan

12.1. Tujuan dan Ruang Lingkup

Tujuan kontrol akses jaringan ini adalah untuk menjamin pengguna yang memiliki akses ke jaraingan tidak menyalahgunakan sistem keamanan jaringan. Ruang lingkup manajemen aset ini dibatasi pada pengguna di divisi IT dan dapat dikembangkan pada seluruh pengguna di perusahaan.

12.2. Kontrol

Kontrol yang berkaitan dengan akses jaringan adalah sebagai berikut:

a. Pengguna dilarang melakukan instalasi router, akses wireless ke jaringan tanpa persetujuan tertulis *network administrator*.
b. Pengguna dilarang mengunduh, menginstall aplikasi atau tools tanpa izin tertulis network administrator.

13.Kebijakan kontrol kriptografi

13.1. Tujuan dan Ruang Lingkup

Tujuan kebijakan kontrol kriptografi untuk melindungi kerahasiaan,keaslian, dan keutuhan informasi. Ruang lingkup kriptografi ini dibatasi pada divisi IT untuk kemudian dapat dikembangkan di seluruh unit kerja di perusahaaan.

13.2. Kontrol

a. Informasi atau data sensitif harus selalu ditransmisikan dalam keadaan terenkripsi. Pertimbangan harus selalu dilakukan pada prosedur yang digunakan antara pihak yang

mengirimkan dan menerima dan setiap kemungkinan permasalahan hukum atas penggunaan teknik enkripsi.

b. Semua message sebaiknya diproteksi dengan berbagai teknik kontrol untuk memastikan *confidentiality, integrity* dan *availibility.*

14.Kebijakan Monitoring dan Information Security Incident Management

14.1. Tujuan dan Ruang Lingkup

Tujuan *monitoring* adalah untuk mendeteksi apakah terdapat perbedaan/ketidaksesuaian antara kontrol yang diteranpkan dengan keadaan yang terjadi di lapangan. Selain itu, monitoring bertujuan untuk mencegah pelanggaran keamanan yang berulang. Pencatatan setiap kejadian menjadi hal penting, karena bisa menampilkannya secara kronologis mencatat semua kegiatan yang dilakukan tiap *user* dalam suatu tabel log secara rinci. Selain itu, hal tersebut akan menjadi bukti/masukan bagi pengembangan kebijakan keamanan di masa mendatang.

Tujuan manajemen insiden dan event adalah untuk memastikan bahwa setiap event tercatat dan setiap insiden terkelola dengan baik.

Ruang lingkup manajemen aset ini dibatasi pada aset yang menjadi tanggung jawab divisi IT.

14.2. Kontrol

Kontrol yang berkaitan dengan monitoring adalah sebagai berikut:

a. Membuat *audit logs*,informasi minimal dalam *audit logs:* identitas pengguna, waktu *log on* dan *log off,* lokasi, data maupun jaringan yang diakses, lokasi,
b. *Audit logs* harus disimpan dalam jangka waktu tertentu untuk kepentingan analisis. Periode yang disarankan adalah tiap satu tahun.
c. Membuat *administrator dan operator logs*, informasi minimal dalam *administrator dan operator logs*: identitas pengguna, waktu *log on* dan *log off*, detil *system error* dan tindakan yang diambil.
d. Review terhadap *audit logs* dan *administrator dan operator log* dilakukan secara berkala terkait dengan manajemen risiko keamanan informasi maupun oleh internal audit.
e. Peyimpanan *audit logs* dan *administrator dan operator log* harus dilakukan dengan mekanisme memadai.

15. Manajemen Kesinambungan Bisnis

15.1. Tujuan dan Ruang Lingkup

Tujuan Manajemen Kesinambungan Bisnis atau *Business Continuity Management (BCM)* adalah untuk memastikan dimulainya kembali kegiatan bisnis dalam hal terjadi suatu gangguan atau kegagalan utama sistem informasi dan memastikan keberlanjutannya secara tepat waktu. RuanG lingkup kebijakan ini pada aktivitas yang memberikan aktivitas signifikan pada pencapaian tujuan stratejik maupun reputasi perusahaan

15.2. Tanggung Jawab

Penanggung jawab manajemen kesinambungan bisnis ini adalah *General Manager* perusahaan, dengan bertanggung jawab pada komite audit perusahaan.

Terkait dengan orang yang bertanggung jawab pada pengembangan dan pengelolaan renacana kesinambungan bisnis, ditanggungjawabi oleh para manager/kepala divisi.

15.3. Rencana kesinambungan bisnis

Rencana kesinambungan bisnis diusulkan mencakup hal-hal berikut:

- Rencana manajemen krisis (untuk seluruh manajemen krisis)
- Rencana keadaan-keadaan luar biasa/khusus (contoh: keadaan pandemik)
- Rencanan pemulihan bencana IT (fokus pada perencanaan teknologi)
- Rencana tanggap darurat (untuk keamanan karyawan/pihak ketiga dalam keadaan darurat).

Kepala unit dukungan teknologi informasi bersama system administrator yang terkait meyakinkan bahwa kesinambungan bisnis dan rencana pemulihan bencana *(disaster recovery plan)* telah dibuat pada informasi-informasi kritis, aplikasi, sistem dan jaringan. System administrators memiliki tanggung jawab untuk menjaga dan mengelola integritas sistem rencana kesinambungan berikutnya dalam area mereka.

16.Information Systems Audit Control

16.1. Tujuan dan Ruang Lingkup

Tujuan pengendalian sistem informasi termasuk pengendalian umum dan pengendalian aplikasi. Perusahaan harus memiliki pengendalian umum dan pengendalian aplikasi yang efektif untuk mencapai *confidentiality,integrity*, dan *availibility* dari informasi kritikal dan sistem informasi. Pada dasarnya dengan memiliki serta menjalankan serangkaian kebijakan dan prosedur pada lingkup perusahaan yang lebih luas, maka pengendalian umum telah dilakukan. Tanpa pengendalian umum, maka pengendalian aplikasi menjadi rentan akan gangguan yang tidak diinginkan.

Ruang lingkup pengendalian ini dilakukan di divisi IT dan direview kembali agar bisa berjalan pada seluruh perusahaan.

16.2. Kontrol

Kontrol yang berkaitan dengan manajemen keamanan sistem informasi dapat berupa:

a. Perencanaan manajemen keamanan yang efektif;
b. Penilaian dan validasi risiko secara periodik;
c. Pengimplementasian prosedur dan kebijakan keamanan;
d. Melakukan training kesadaran keamanan informasi dan isu keamanan lain terkait personil;
e. Melakukan penguiandan evaluasi atas efektivitaskebijakan keamanan informasi, prosedur dan instruksi kerja;
f. Melakukan remediasi atas kelemahan keamanan informasi;
g. Jaminan keamanan atas kegiatan yang dilakukan oleh pihak ketiga.

Kontrol yang berkaitan dengan akses

a. Mekanisme identifikasi dan otensifikasi;
b. Pengendalian otorisasi;
c. Perlindungan atas sumber-sumber daya yang sensitif;
d. Melakukan audit dan pemantauan kapabilitas termasuk penanganan insiden.

17.Kebijakan manajemen password

17.1. Tujuan dan Ruang Lingkup

Tujuan kebijakan manajemen password adalah mencegah masuknya pihak-pihak yang tidak berhak ke dalam sistem. Ruang lingkup manajemen password ini dibatasi pada pengguna, dan pihak ketiga di divisi IT dan dapat diterapkan ke seluruh pengguna di perusahaan.

17.2. Kontrol

Kontrol yang berkaitan dengan manajemen password adalah sebagai berikut:

a. Masing-Masing pengguna diberikan password sesuai otoritas untuk mengakses sistem maupun aplikasi.
b. Untuk memasuki area yang sensitif, pengguna harus masuk dengan menggunakan *smartcard*/*biometric*/token.
c. Memastikan password memiliki kriteria yang kuat. Kriteria password yang kuat dapat berupa:
    - minimal 6 karakter dimana 3 karakter diantaranya adalah: karakter huruf kecil, karakter huruf besar, angka, tanda baca, karakter khusus (misalnya @#$%^&_+<>)
    - minimal 15 karakter alphanumeric. Alphanumeric adalah kombinasi abjad A-Z dan angka 0-9 (misalnya: 5664hws32sy65tg)

d. Kebijakan manajemen password ini harus dipublikasikan ke seluruh karyawan di perusahaan, di dalamnya termasuk:
    - Agar tidak memberikan password kepada siapapun
    - Kriteria password yang kuat/aman
    - Arahan agar mengganti password secara berkala
    - Prosedur ketika karyawan lupa password
e. Password akses ke wireless tidak boleh ditempelkan di ruang publik.
f. Akses terhadap audit logs terbatas pada *internal audit.*

18.Kebijakan keamanan jaringan

18.1. Tujuan dan Ruang Lingkup

Tujuan kebijakan keamanan jaringan adalah untuk memastikan perlindungan informasi dalam jaringan dan perlindungan infrastruktur pendukung. Ruang lingkup manajemen aset ini dibatasi pada aset yang menjadi tanggung jawab divisi IT.

18.2. Kontrol

19.Kebijakan Keamanan Aplikasi

19.1. Tujuan dan Ruang Lingkup

Tujuan keamanan aplikasi adalah untuk memastikan bahwa perangkat lunak dan informasi di dalamnya terlindungi dari perangkat lunak berbahaya serta memastikan . Ruang lingkup manajemen aset ini dibatasi pada aset yang menjadi tanggung jawab divisi IT. Selain itu, sehubungan dengan banyaknya aplikasi di perusahaan yang dibangun oleh pihak ketiga, maka harus ada design keamanan yang bisa diterapkan secara menyeluruh pada aplikasi-aplikasi yang sedang dibangun maupun yang sedang ada perubahan.

Ruang lingkup kebijakan ini ditujukan pada seluruh aplikasi yang dibangun dan dikembangkan oleh PT XYZ dalam hal ini direpresentasikan oleh divisi IT sebagai IT Lead di perusahaan.

19.2. Kontrol

Kontrol yang berkaitan dengan perencanaan keamanan aplikasi adalah sebagai berikut:

a. Melakukan review atas kebutuhan bisnis sekarang dan masa depan dan tujuan keamanan;
b. Menganalisis aset sistem terkait dengan nilai dan sensivitasnya terhadap data.
c. Menganalisis aplikasi tersebut terkait dengan risiko potensial terhadap aset.
d. Mereview kebutuhan aplikasi terkait dengan keamanan dan kerahasiaan data.
e. Menganalisis baik internal maupun eksternal terkait dengan ancaman terhadap keamanan.

Kontrol pada tahap pengerjaan proyek

a. Membuat penilaian risiko secara tertulis yang dibahas antara pemilik proyek dan develpoer IT untuk menentukan kebutuhan bisnis serta level security yang dibutuhkan
b. Dalam menganalisis risiko, pemimpin proyek harus mempertimbangkan hal-hal seperti: kecurangan, pencurian, pengrusakan, pelanggaran privasi, penolakan layanan.

Kontrol pada tahap implementasi

a. Pemimpin proyek bersama dengan pihak developer melakukan review bersama atas semua aspek keamanan untuk memverifikasi apakah semua analisa risiko sudah didokumentasikan.
b. Mereview kontrol-kontrol yang direkomendasikan untuk meminimalisasi risiko.
c. Melakukan testing yang diperlukan untuk menguji keamanan aplikasi secara keseluruhan.
d. Membuat dokumentasi bahwa aplikasi telah melalui proses pengujian dan dinyatakan sesuai dengan kebutuhan bisnis.

20.Kebijakan penggunaan internet/intranet

20.1. Tujuan dan Ruang Lingkup

Tujuan kebijakan penggunaan internet/intranet ini adalah menentukan parameter akses internet/intranet yang yang diberikan izin, pembatasan, dan pemantauan. Ruang lingkup kebijakan ini kepada seluruh pegawai yang mengakses internet/intranet sebagai bagian dari tugas sehari-hari maupun bagi orang yang telah diberikan otorisasi.

20.2. Kontrol

Karyawan/pegawai maupun orang-orang yang diberikan otorisasi untuk mengakses internet/intranet, harus setuju dengan ketentuan-ketentuan internal perusahaan terkait dengan tugasdan tanggung jawab mereka. Secara formal, setiap orang harus mengkonfirmasi bahwa mereka menerima ketentuan tersebut sebelum diberikan *account access* oleh divisi IT.

Kontrol yang berkaitan dengan kebijakan penggunaan internet/intranet adalah sebagai berikut:

a. Karyawan dan pegawai yang diberikan akses ke internet/intranet tidak diperbolehkan melakukan hal-hal berikut:
    - Aktivitas yang melanggar hukum.
    - Mempromosikan bisnis ilegal.
    - Mengunduh piranti lunak ilegal atau yang tidak terdaftar.
    - Berpartisipasi dalam global chat room.
    - Mengakses situs yang berisikan materi dewasa atau kekerasan.
    - Mempublikasikan informasi rahasia.
    - Melakukan promosi/iklan produk atau partai politik.
    - Menyebarluaskan materi produk komersial.
b. Sehubungan dengan keamanan protokol jaringan, maka pengguna yang mengakses internet/intranet:
    - Tidak memberitahukan passwordnya kepada pihak lain.
    - Memutakhirkan account dan password bila dibutuhkan.
    - Tidak membuka atau memforward email dari sumber yang tidak dikenal.
    - Meyakinkan bahwa ketika pengguna tidak sedang di depan komputernya, orang lain tidak dapat menggunakan internet/intranet dengan account mereka sendiri.

21. Kebijakan Penggunaan Electronic Mail

21.1. Tujuan dan Ruang Lingkup

Tujuan kebijakan ini yaitu menginformasikan kepada pengguna bentuk penggunaan surat elektronikdan dokumen disamakan perlakuannya dengan dokumen lain yang bentuknya tertulis, menyediakan panduan kepada para pengguna bahwa tanggung jawab untuk menjaga *confidentiality* terletak pada tiap pengguna. Kebijakan iniditujukan kepada seluruh karyawan baik yang tetap maupun yang sementara serta seluruh vendor yang mendapat otorisasasi.

21.2. Kontrol

Masing-masing pengguna memperoleh alamat email dengan akhiran @xyz.co.id dan hanya dapat diakses dari lingkungan kantor.

Kontrol yang berkaitan dengan penggunaan *electronic mail* adalah sebagai berikut:

a. Masing-masing pengguna tidak diperbolehkan menampilkan informasi dalam surat elektronik seperti hal-hal berikut:
    - Propaganda politik
    - Materi seks, kekerasan, diskriminasi,
    - Materi ilegal
    - Pencemaran nama baik

b. Penggunaan email hanya untuk keperluan perusahaan, dilarang untuk kepeluan pribadi,
c. Pengguna dilarang mengeset autoforward pada settingan surat elektroniknya ke alamat surat elektronik eksternal atau ke jaringan publik lainnya.
d. Pengguna dilarang mengeset autoforward pada settingan surat elektroniknya ke alamat surat elektronik pribadi
e. Fasilitas surat elektronik tidak diperbolehkan untuk menyebarkan content komersial selain bisnis perusahaan.
f. Melakukan audit secara periodik untuk memastikan tidak adanya file yang sensitif yang disimpan dalam area publik.
g. Untuk mengurangi beban kerja server, hindari mengirim email dengan file yang berukuran lebih dari 2 MB.

INSTRUKSI KERJA

1. INSTRUKSI PEMBUATAN FILE PRIBADI (PERSONAL FILE CREATION INSTRUCTION)	
Penjelasan	File pribadi berisikan informasi yang berkaitan dengan karir karyawan di perusahaan.
Penanggung Jawab	Kepala Divisi Sumber Daya Manusia
Tujuan teknis	Untuk mengetahui latar belakang karyawan dan kondisi sekarang.
Kebutuhan informasi	Nama karyawan, alamat, nomor telepon, curriculum vitae dan dokumen lain yang relevan seperti kontrak kerja, daftar tugas dan tanggungjawabnya, jenis-jenis pelatihan/training yang sudah diikuti, proyek-proyek yang diikuti serta peranannya dalam proyek tersebut.

2. INSTRUKSI PEMBUATAN DAFTAR AKSES (ACCESS LIST CREATION INSTRUCTION)	
Penjelasan	Daftar Akses adalah daftar *user account* yang ada dalam perusahaan.
Penanggung Jawab	System Administrator Security officer
Tujuan teknis	Untuk mengetahui hak akses tiap user terhadap aset informasi.
Kebutuhan informasi	Nama user account,hak akses,daftar aset beserta karyawan yang berhak mengaksesnya.

3. INSTRUKSI PEMBUATAN DATABASE PENGGUNA (USER DATABASE CREATION INSTRUCTION)	
Penjelasan	Database pengguna adalah daftar yang berisikan informasi atas apa saja yang menjadi hak akses pengguna
Penanggung Jawab	System Administrator Security officer
Tujuan teknis	Untuk melihat akses/login yang dilakukan oleh tiap user kepada setiap aset informasi.
Kebutuhan informasi	User database berisi nama user, password, dan grup-grup dimana saja ia tergabung.

4. INSTRUKSI KETIKA KEADAAN DARURAT (EMERGENCY RESPONDING INSTRUCTION)	
Penjelasan	Keadaan darurat adalah keadaan yang dapat mengancam keselamatan karyawan dan semua orang, termasuk keberadaan perusahaan. Untuk itu perlu disiapkan prosedur tetap untuk menanggulanginya dengan tujuan utama: melindungi semua orang dan melindungi aset perusahaan yang utama.
Penanggung Jawab	System Administrator Security officer
Tujuan teknis	Untuk memastikan pekerjaan penanganan keadaan darurat sesuai prosedur sehingga dapat menekan risiko informasi yang berpotensi hilangnya confidentiality (kerahasiaan), integritas (integrity) dan ketersediaan (availibility).
Kebutuhan informasi	• Daftar aset-aset utama perusahaan. • Daftar semua kejadiaan yang terklasifikasikan sebagai keeadaan darurat. • Langkah-langkah mendetil yang harus dilakukan untuk setiap keadaan darurat. • Daftar contact person yang dapat dihubungi bila keadaan darurat, baik dari internal perusahaan, maupun eksternal perusahaan.

5. INSTRUKSI PENANGANAN INSIDEN KEAMANAN (SECURITY INCIDENT HANDLING INSTRUCTION)	
Penjelasan	Sebuah insiden keamanan adalah sebuah komputer, jaringan, atau kegiatan berbasis kertas yang menghasilkan (atau dapat mengakibatkan) penyalahgunaan, kerusakan, penolakan layanan, kompromi integritas, atau hilangnya kerahasiaan, jaringan komputer, aplikasi, atau data, dan ancaman , kekeliruan identitas, atau kesalahan individu menggunakan sumber daya tersebut.
Penanggung Jawab	System Administrator Security officer
Tujuan teknis	Untuk memastikan bahwa setiap insiden terhadap keamanan informasi ditangani dengan baik.
Kebutuhan informasi	• Daftar insiden yang mungkin terjadi • Instruksi penanganan atas insiden tersebut

Contoh pelaporan insiden keamanan

Daftar Insiden	Kontak	Langkah-langkah
Sebuah komputer laptop yang berisi data pribadi hilang atau dicuri. (kehilangan)		
Seorang pegawai melakukan pelanggaran akses mereka ke data pribadi untuk melihat data pribadi tidak terkait dengan pekerjaan mereka, karena alasan pribadi atau lainnya atau rasa ingin tahu yang sederhana. (penggunaan tidak sah)		
Sebuah ruangan berisikan komputer yang menyimpan data pribadi ditinggalkan dan terkunci.		
Hacker mengeksploitasi untuk mendapatkan akses ke file password server. (Akses tidak sah)		
Sebuah worm menggunakan file sharing untuk menginfeksi dari satu sampai ratusan komputer desktop dan laptop dalam perusahaan. (Kode berbahaya)		

6. INSTRUKSI PEMBUATAN KRITERIA KLASIFIKASI INFORMASI (CREATING INFORMATION CLASSIFICATION CRITERIA)	
Penjelasan	Pekerjaan mengklasifikasi memudahkan dalam mengelola aset informasi.
Penanggung Jawab	Security officer dan pihak lain terkait
Tujuan teknis	Hal ini penting untuk mengklasifikasikan informasi yang sesuai dengan nilai aktual dan tingkat sensitivitas untuk menentukan tingkat keamanan yang sesuai
Kebutuhan informasi	Mengklasifikasikan informasi dalam 5 kategori berikut: • Top secret • Highly confidential • Proprietary • Internal Use Only • Public Documents

Contoh

Klasifikasi	**Jenis aset informasi**	**Level security**
Top Secret	Strategi pengembangan bisnis, strategi investasi	tertinggi
Highly confidential	Informasi akuntansi, rencana bisnis, profil Anggota Kliring, data karyawan	Sangat tinggi
Proprietary	Prosedur tetap, rencana proyek, design dan spesifikasi aplikasi bursa	Tinggi
Internal use only	Nota dinas, laporan proyek,notulensi rapat	Terkontrol
Public documents	Berita perusahaan, laporan tahunan	Minimal

7. INSTRUKSI MONITORING IT SECURITY(IT SECURITY MONITORING WORK INSTRUCTION)	
Penjelasan	Prosedur ini untuk mendefinisikan akses jaringan yang perlu dimonitor secara periodik oleh tim
Penanggung Jawab	Security officer dan team
Tujuan teknis	Untuk melakukan pemantauan atas aktivitas dalam jaringan perusahaan.
Kebutuhan informasi	Informasi yang dibutuhkan tekait dengan instruksi ini antara lain: • Intrusion detection monitoring • Anomalous network activity monitoring • Firewall traffic monitoring • SiteScope • Network and server availability monitoring • Domain monitor • Monitoring network resource access • Alert/log review • RSA token authentication • Domain accounts and privileges • Server access • Application access
Rincian monitoring	1. Harian • Webmail • Remote dial-up access (RAS) • Security eventlogs • Server configurations 2. Mingguan • Mereview kebijakan account apakah sesuai dengan kebijakan perusahaan • Mereview size dari eventlogs untuk meyakinkan bahwa masih dalam size minimum records • Mereview file dan direktori yang dishare,memastikan bahwa admin masih sebagai pemilik file dan folder tersebut. • Mereview aktivitas internet untuk memastikan apakah aktivitas tersebut masih sesuai dengan kebijakan perusahaan. • Mereview aplikasi antivirus apakah sudah terkonfigurasi *system realtime protction* pada seluruh komputer yang tersambung ke jaringan perusahaan. • Mereview aplikasi antivirus sudah terjadwal untuk mengupdate antivirus definition, mininal sekali dalam seminggu. • Mereview service packs, security roll-ups dan critical updates yang terpasang di komputer adalah yang termutakhir.

	3. Bulanan • Mereview aktivitas internet untuk memastikan apakah aktivitas tersebut masih sesuai dengan kebijakan perusahaan. • Mereview account yang ditinggalkan/dihapus untuk memastikan tidak ada celah keamanan bagi jaringan perusahaan. 4. Triwulan • Mereview semua account-account yang diberikan kepada user,apakah sudah sesuai dengan kebijakan perusahaan. • Mereview penggunaan/aktivitas internet, apakah sudah sesuai dengan kebijakan perusahaan. • Mereview konfigurasi server.

8. INSTRUKSI PEMBUATAN IDENTIFIKASI DAN KLASIFIKASI ASET (IDENTIFICATION AND CLASSIFICATION OF ASSETS WORK INSTRUCTION)	
Penjelasan	Identifikasi dan klasifikasi aset merupakan langkah penting untuk mengelola risiko-risiko yang mungkin terjadi maupun dalam perencanaan pengelolaan aset perusahaan secara menyeluruh.
Penanggung Jawab	Chief Security Officer, Security officer, information manager,information user dan pihak lain terkait
Tujuan teknis	Tujuan mengidentifikasi dan mengklasifikasi aset untuk mengelola aset secara efektif. Dengan memperhatikan tingkat kegunaannya bagi perusahaan,maka harus dipastikan bahwa aset sudah dikelompokkan dan disimpan dengan baik.
Kebutuhan informasi	Mengklasifikasikan aset dalam dengan atribut sebagai berikut: • Nama divisi • Kelompok aset • Nama aset • Tipe aset • Penanggung jawab aset/pemilik aset • Lokasi Penyimpanan • Format aset • Hak akses • Dampak terhadap sistem

Contoh pembuatan profil risiko

A. Informasi umum

1. Tentukan kelompok atau individu yang mengakses sumber daya informasi

☐ Karyawan
☐ Anggota Kliring
☐ Rekanan
☐ Outsources
☐ Regulators
☐ Vendor
☐ Otoritas Jasa Keuangan
☐ Bapepam
☐ Lainnya

2. Apakah pernah dilakukan penetration test?

☐ Ya
☐ Tidak

Jika ya,
2.1 Kapan dilakukan penetration test terakhir kali?_____
2.2 Siapa yang melakukan penetration test? _____
2.3 Jelaskan isu-isu terkait keamanan informasi yang terjadi terakhir _____
_____
_____
_____

B. Sensitivitas Informasi

3. Beri jawaban spesifik atas data Anggota Kliring yang digunakan atau dikumpulkan

Data	**Bernilai? (Ya/Tidak)**
Informasi keuangan	
Informasi kartu kredit	
Nomor Induk Kependudukan	
Alamat	
Telpon kantor atau Handphone	
Informasi Medical	
Tanggal lahir	
Informasi Personal (misal nama Ibu Kandung)	
Suku	
Agama	
Catatan Kepolisian	

4. **Beri jawaban spesifik atas data karyawan yang digunakan atau dikumpulkan**

Data karyawan	**Bernilai? (Ya/Tidak)**
Tanggal lahir	
Informasi kartu kredit	
Nomor Induk Kependudukan	
Alamat	
Telpon rumah atau Handphone	
Informasi Medical	
Tanggal bergabung dengan perusahaan	
Status Perkawinan	
Informasi Personal (misal nama Ibu Kandung)	
Suku	
Agama	
Catatan Kepolisian	
Catatan evaluasi kinerja	
Informasi Gaji	

5. **Beri jawaban spesifik attas informasi internal yang digunakan atau dikumpulkan**

Data korporasi	**Bernilai? (Ya/Tidak)**
Data klien/anggota kliring	
Proyeksi keuangan	
Dokumen kontrak/legal	
Rencana Pengembangan Bisnis	
Rencana Strategis	

6. **Beri jawaban spesifik attas informasi pihak ketiga yang digunakan atau dikumpulkan**

Data pihak ketiga	**Bernilai? (Ya/Tidak)**
Properti intelektual	
Software berlisensi hasil pengembangan internal	
Syarat-syarat Non-Disclosure Agreement (NDA)	

7. **Apakah sumber daya informasi menggunakan atau memproses beberapa data/informasi yang rahasia?**
   - ☐ **Ya, yaitu _____**
   - ☐ **Tidak**

8. **Apakah adminisitrator sumber informasi menggunakan atau memberikan akses atas data sensitif pada sistem lain?**
   - ☐ **Ya**
   - ☐ **Tidak**

Mohon jelaskan bagaimana mekanisme administrator mengakses data sensitif atau memberikan akses pada data sensitif

_____
_____

9. **Apakah sumber daya informasi memproses transaksi keuangan?**
   ☐ **Ya**
   ☐ **Tidak**

   Bila sumber daya informasi mengelola data keuangan (internal organisasi) berapakah nilai uang yang diproses?
   ☐ Dibawah Rp100.000.000
   ☐ Antara Rp100.000.000 hingga Rp500.000.000
   ☐ Antara Rp500.000.000 hingga Rp5.000.000.000
   ☐ Antara Rp5.000.000.000 hingga Rp10.000.000.000
   ☐ Di atas Rp10.000.000.000

10. **Dapatkah informasi yang yang disalahgunakan merusak organisasi yang menyebabkan kegagalan transaksi bisnis,kehilangan uang atau terpenjara waktu?**
    ☐ **Ya**
    ☐ **Tidak**

    Bila sumber daya informasi terganggu oleh srangan pihak luar?
    ☐ tindakan kriminal
    ☐ Antara Rp5.000.000.000 hingga Rp10.000.000.000
    ☐ Antara Rp10.000.000.000 hingga Rp50.000.000.000
    ☐ Antara Rp50.000.000.000 hingga Rp100.000.000.000
    ☐ Di atas Rp100.000.000.000

C. Kesesuaian dengan peraturan

11. **Apakah sumber daya informasi mengacu pada peraturan tertentu?**
    ☐ **Ya**
    ☐ **Tidak**

    Silahkan pilih peraturan apa saja yang terkait?
    ☐ Keputusan Ketua Bapepam No.10/PM/1996 tentang tatacara penyusunan dan pengajuan rencana anggaran dan penggunaan laba lembaga kliring dan penjaminan
    ☐ Keputusan Ketua Bapepam No.66/PM/1996 tentang Laporan Lembaga Kliring dan Penjaminan
    ☐ Keputusan Ketua Bapepam No.67/PM/1996 tentang Pemeliharaan Dokumen oleh Lembaga Kliring dan Penjaminan
    ☐ PP No. 45 Tahun 1995 Tentang Penyelenggaraan Kegiatan di Bidang Pasar Modal
    ☐ Lainnya _____

    Sebutkan aspek regulasi tersebut yang berkaitan dengan sumber daya informasi
    _____
    _____
    _____

12. **Apakah ada kebutuhan lain (misalnya ketentuan kontrak) yang mengharuskan pengamanan informasi untuk confidentiality, integrity, availability atau akuntabilitas**

☐ **Ya**
☐ **Tidak**

Sebutkan apa kebutuhan kontraktual tersebut yang berkaitan dengan sumber daya informasi _____
_____
_____

D. Kebutuhan bisnis

13. Beri rating pada kebutuhan confidentiality (kerahasiaan) atas konsekwensi pengungkapan yang tidak diotorisasi dari data yang disimpan, diproses atau ditransmisikan dari sumber daya informasi
☐ Tinggi
☐ Sedang
☐ Rendah

14. Beri rating pada kebutuhan integrity (keutuhan) atas konsekwensi modifikasi dari pihak tak berhak pada data yang disimpan, diproses atau ditransmisikan dari sumber daya informasi
☐ Tinggi
☐ Sedang
☐ Rendah

15. Beri rating pada kebutuhan availibility (ketersediaan) atas konsekwensi kehilangan gangguan akses pada data yang disimpan, diproses atau ditransmisikan dari sumber daya informasi ke pengguna nonperusahaan
☐ Tinggi
☐ Sedang
☐ Rendah
☐ Tidak tersedia

16. Beri rating pada kebutuhan availibility (ketersediaan) atas konsekwensi kehilangan gangguan akses pada data yang disimpan, diproses atau ditransmisikan dari sumber daya informasi ke pengguna perusahaan (tidak termasuk akses untuk mendukung aplikasi atau system itu sendiri)
☐ Tinggi
☐ Sedang
☐ Rendah
☐ Tidak tersedia

17. Beri rating pada kebutuhan accountability (akuntabilitas) atas konsekwensi ketidakmampuan atau kemampuan yang terkompromikan untuk memegang akuntabilitas user yang beraktivitas pada sumber daya informasi
☐ Tinggi
☐ Sedang
☐ Rendah

18. Beri rating pada kebutuhan accountability (akuntabilitas) atas konsekwensi ketidakmampuan atau kemampuan yang terkompromikan untuk memegang akuntabilitas user pada layanan atau pengguna administrasi
☐ Tinggi
☐ Sedang
☐ Rendah

19. Beri rating kerusakan reputasi pada organisasi bila diketahui oleh pengguna atau pasar bahwa sumber daya informasi telah dilanggar atau dirusak

☐ Tinggi
☐ Sedang
☐ Rendah

Referensi

[1] ISO/IEC 27001:2005
[2] SNI ISO/IEC 27001:2009
[3] Federal Information System Controls Audit Manual. GAO. 2009
[4] State of Vermont Minimum Security Standards for Application Development Policy, 2010
[5] Australian National Audit Office Business Continuity Management. Building resilience in public sector entities. Better Practice Guide June 2009