Materi 3

Keamanan Sistem Informasi

3 SKS | Semester 8 | S1 Sistem Informasi | UNIKOM | 2015
Nizar Rabbi Radliya | nizar.radliya@yahoo.com

Nama Mahasiswa	
NIM	
Kelas	

Kompetensi Dasar

Memahami kebijakan dan strategi keamanan sistem informasi.

Pokok Bahasan

Kebijakan dan Strategi Keamanan Sistem Informasi
1. Kebijakan keamanan sistem informasi
2. ISO 17799
3. Dampak dari pemanfaatan komputer
4. Kebutuhan atas strategi keamanan sistem informasi

I. Kebijakan Keamanan Sistem Informasi

Setiap organisasi harus memiliki pedoman bagi anggotanya untuk mencapai sasaran. Begitu juga dengan implementasi sistem informasi pada sebuah perusahaan diperlukan pedoman kebijakan bagi para karyawan dalam penggunaannya. Setiap karyawan tidak dapat bertindak semaunya sendiri dan tidak berdisiplin dalam melaksanakan tugasnya. Contoh apabila karyawan sudah ditentukan jam kerjanya maka waktu tersebut harus secara disiplin dipegang, karena setiap output tugas merupakan input bagi karyawan yang lainnya. Hal ini akan berpengaruh pada kelancaran proses sistem informasi dan berkaitan dengan keuntungan atau kerugian perusahaan. Oleh karena itu garis pedoman ini dalam bentuk prosedur harus ditaati oleh semua pihak.

Kebijakan keamanan sistem informasi biasanya disusun oleh pimpinan operasional beserta pimpinan ICT dengan pengarahan dari pimpinan organisasi atau perusahaan. Rangkaian konsep secara garis besar dari prosedur keamanan sistem informasi adalah:

1. Keamanan sistem informasi merupakan urusan dan tanggung jawab semua karyawan.

Semua karyawan harus mengetahui dampak apabila peraturan keamanan sistem informasi diabaikan. Semua manajer atau pihak ICT bertanggung jawab untuk mengkomunikasikan kepada semua karyawannya mengenai pengamanan yang dilakukan di perusahaan dan meyakinkan bahwa mereka mengetahi dan memahami

semua peraturan yang diterapkan di perusahaan dan bagiannya. Akan tetapi dilain pihak, setiap karyawan bertanggung jawab dan harus mematuhi peraturan keamanan sistem informasi yang diterapkan perusahaan. Memunculkan tanggung jawab karyawan dapat dilakukan dengan cara:

a. Mengadakan pelatihan atau sosialisi tentang pedoman keamanan sistem informasi,
b. Mencantumkan ketentuan yang berkaitan dengan keamanan sistem informasi pada surat kontrak ketika karyawan tersebut mulai bekerja,
c. Memberikan surat peringatan terhadap karyawan yang melanggar ketentuan keamanan sistem informasi.

Contoh: tidak ada gunanya apabila *username* dan *password* untuk mengakses data diberikan atau diketahui oleh pihak yang tidak berwenang. Misalnya dengan menempelkan *password* di atas *keyboard* atau di *monitor*.

2. Penetapan pemilik sistem informasi.

Sebaiknya menunjuk atau menetapkan seorang karyawan sebagai pemilik sistem (atau subsistem) yang bertanggung jawab atas keamanan sistem dan data yang diolahnya. Beliau juga berhak untuk mengajukan permintaan atas pengembangan sistem lebih lanjut atau perbaikan sistem yang menyangkut bagiannya. Personal ini merupakan *contact person* dengan bagian ICT.

Contoh: Perusahaan menunjuk seseorang dari salah satu divisi untuk dapat mengakses halaman *backdoor* website resmi perusahaan dan mengolah data yang ada di dalam website tersebut. Personal tersebut juga dapat mengajukan permintaan dan pengembangan sistem website apabila ditemukan kekurangan atau kelemahan.

3. Langkah keamanan harus sesuai dengan peraturan dan undang-undang.

Tergandung bidang yang ditekuni, perusahaan harus mematuhi undang-undang yang telah ditetapkan yang berikaitan dengan proteksi data, *cyber law*, dan hak cipta.

Contoh: sebuah bank harus mematuhi peraturan yang dikeluarkan oleh Bank Indonesia, misalnya berkatian dengan sistem pengiriman uang atau perlindungan data nasabah.

4. Antisipasi terhadap kesalahan.

Dengan meningkatnya proses transaksi secara *online* dan *real time* yang terkoneksi ke dalam jaringan komputer, maka transaksi akan terlaksana dalam hitungan beberapa detik atau lebih cepat. Transaksi semacam ini apabila terjadi kesalahan tidak dapat langsung diperbaiki atau akan menyita banyak waktu dan upaya dalam perbaikannya.

Antisipasi dan pencegahan dengan tindakan keamanan yang ketat akan memberikan garansi atas integritas, keberlangsungan, dan kerahasiaan transaksi.

Contoh: transaksi ini biasanya terjadi pada sistem perbankan misalnya pemindahan dana melalui ATM. Berbeda halnya dengan proses transaksi pemesanan barang yang tidak langsung dapat dikirim, kesalahan pemesanan masih dapat dikoreksi misalnya melalui kontak telepon, email atau melalui fasilitas yang tersedia pada sistem.

5. Pengaksesan ke dalam sistem harus berdasarkan kebutuhan fungsi.

Pengguna sistem harus disesuaikan dengan kebutuhan fungsi pengguna tersebut. Dalam artian akses yang diberikan hanya dapat digunakan pada bagian-bagian sistem yang sesuai dengan fungsionalitas karyawan dalam perusahaan.

Contoh: bagian personalia hanya diberikan akses terhadap sistem penggajian, tidak ada akses terhadap data hasil penjualan dari setiap personal bagian pemasaran. Atau beberapa personal bagian personalia (misalnya untuk bagian *rekrutment/hiring*) tidak diperbolehkan untuk memiliki akses ke data penggajian karyawan.

6. Hanya data bisnis yang ditekuni perusahaan yang diperbolehkan untuk diproses di sistem komputer.

Sistem komputer milik perusahaan beserta jaringannya hanya diperbolehkan untuk dipakai demi kepentingan bisnis perusahaan. Data yang diperbolehkan disimpan dalam sistem hanya data-data yang berkaitan dengan proses bisnis perusahaan dan data tersebut hanya digunakan untuk kebutuhan perusahaan.

Contoh: Pengguna tidak diperbolehkan menyimpan data pribadi (yang tidak berkaitan dengan kebutuhan bisnis) pada komputer atau database sistem. Contoh lainnya adalah aplikasi yang dikembangkan oleh perusahaan *software house* tidak dapat digunakan oleh karyawan untuk keperluan pribadi.

7. Pekerjaan yang dilakukan oleh pihak ketiga.

Apabila terdapat pekerjaan yang diserahkan kepada pihak ketiga, maka perusahaan harus dilindungi oleh keamanan atas informasi perusahaan. Di dalam kontrak harus diatur agar pihak ketiga tidak menyebarkan data dan informasi yang berkaitan dengan perusahaan. Selain hal tersebut untuk antisipasinya perusahaan harus menunjuk seseorang sebagai perwakilan perusahaan untuk terlibat (melakukan pengawasan) dalam proyek yang dikerjakan oleh pihak ketiga.

Contoh: apabila dalam pengembangan sistem informasi melibatkan *software house* dalam pengerjaannya, maka pada saat tahap uji coba akhir yang mengharuskan

melibatkan data sungguhan perusahaan. Data ini tidak diperbolehkan oleh pihak *software house* untuk disalin atau disebarluaskan baik dalam bentuk *hardcopy* maupun *softcopy,* apalagi kalau sampai digunakan sebagai contoh untuk perusahaan lain atau kompetitor.

8. Pemisahan aktivitas antara pengembang sistem, pengoperasian sistem, dan pemakai akhir sistem informasi.

   Untuk menjaga kestabilan sistem informasi di perusahaan, maka dianjurkan untuk diadakan pemisahan secara fungsional antara pengembang sistem, pengoperasian sistem harian dan pemakai akhir sistem.

   Contoh: tidak dibenarkan apabila pengembang sistem (*programmer, system analys*) diberikan tanggung jawab secara bersamaan dalam menangangi pengoperasian sistem (*system administrator, database administrator*) atau diberikan tugas-tugas sebagai pengguna akhir (*user*).

9. Implementasi sistem baru atau permintaan perubahan terhadap sistem yang sudah ada harus melalui pengontrolan yang ketat melalui prosedur sistem akseptasi dan permintaan perubahan (*Change Request*).

   Setiap permintaan perubahan harus disertai alasan yang kuat serta keuntungan yang akan didapatkan dan pemohon harus dapat meyakini manajer terkait dan pemilik sistem mengenai perubahan ini. Harus pula diingat bahwa perubahan program akan memakan biaya dan waktu.

   Contoh: tidak dibenarkan apabila pemakai secara inidividu meminta atau melakukan perubahan terhadap sistem tanpa sepengetahuan pemilik sistem atau tanpa melalui prosedur *change request*.

10. Sistem yang akan dikembangkan harus sesuai dengan standar metode pengembangan sistem yang diemban oleh organisasi.

    Sistem yang akan dikembangkan harus memakai bahasa pemrograman yang sudah ditetapkan. Begitu pula dengan sistem database yang digunakan harus memiliki keseragaman. Sebelum implementasi sistem yang dikembangkan, maka diwajibkan melakukan evaluasi dan menilai keandalan keamanan sistem agar sesuai dengan standar keamanan yang sudah ditetapkan.

11. Pemakai bertanggung jawab penuh atas semua aktivitas yang dilakukan dengan memakai kode identitasnya (*User-ID*).

Semua pemakai harus berhati-hati menyimpan username dan password. Semua aktivitas yang dilakukan oleh ID yang bersangkutan harus terekam dalam sebuah sistem. Apabila terjadi kesalahan yang berkaitan dengan ID tersebut yang mengakibatkan kerugian terhadap perusahaan, maka pengguna yang bersangkutan akan diminta pertanggung jawabannya.

II. ISO 17799

ISO 17799 adalah standar keamanan sistem informasi yang telah diakui oleh dunia dan disahkan pada tahun 2000, dimana ia mengalami revisi pada tahun 2005 (ISO/IEC 17799:2005). Pada tahun 2007, ISO dan International Electrotechnical Commission (IEC) mengubah penomoran ISO 17799 menjadi ISO/IEC 27002.

Komponen-komponen dari ISO 17799 meliputi:

1. 10 control clauses
2. 36 control objectives
3. 127 controls

Kesepuluh ketentuan ISO 17799 meliputi:

1. Kebijakan Keamanan (*Security Policy*);

Hal ini bertujuan untuk memberikan arahan atau bantuan terhadap manajemen dalam merumuskan kebijakan keamanan sistem informasi. *Security Policy* (kebijakan keamanan), mengarahkan visi dan misi manajemen agar kontinuitas bisnis dapat dipertahankan dengan mengamankan dan menjaga integritas/keutuhan informasi-informasi krusial yang dimiliki oleh perusahaan.

Security Policy sangat diperlukan mengingat banyak ditemuinya masalah-masalah non teknis salah satunya penggunaan *password* oleh lebih dari satu orang. Hal ini menunjukan tidak adanya kepatuhan dalam menerapkan sistem keamanan informasi. Harus dilakukan inventarisasi data-data perusahaan. Selanjutnya dibuat peraturan yang melibatkan semua departemen sehingga peraturan yang dibuat dapat diterima oleh semua pihak. Setelah itu rancangan peraturan tersebut diajukan ke pihak direksi. Setelah disetujui, peraturan tersebut dapat diterapkan.

Security Policy meliputi berbagai aspek, yaitu:

a. *Information security infrastructure*
b. *Information security policy*

2. Organisasi Keamanan (*Security Organisation*);

Hal ini membahas bagaimana mengelola sistem keamanan di dalam organisasi sendiri, menjaga agar sistem tidak disalahgunakan oleh pihak ketiga yang terlibat dalam pekerjaan perusahaan (contohnya pihak ketiga yang melakukan proses pengolahan data atau pengembangan sistem yang melibatkan data perusahaan). Aspek yang terlingkupi, yaitu:

a. *Security of third party access*
b. *Outsourcing*

3. Penggolongan Asset dan Kendali (*Asset Classification and Control*);

Hal ini bertujuan untuk membahas proteksi yang tepat bagi aset perusahaan yang berkaitan dengan sistem informasi agar memiliki tingkat keamanan yang tepat dan baik. Membahas tentang penjagaan aset yang ada meliputi berbagai aspek, diantaranya:

a. *Accountability for assets*
b. *Information classification*

4. Keamanan Personil (*Personnel Security*);

Hal ini bertujuan untuk mengurangi resiko kesalahan orang, kecurangan, atau penyalahgunaan fasilitas. Membekali setiap pengguna sistem dengan peraturan keamanan sistem informasi dalam melaksanakan tugas mereka. Kepatuhan yang mengarah kepada pembentukan prosedur dan aturan-aturan sesuai dengan hukum yang berlaku meliputi berbagai aspek, yaitu:

a. *Compliance with legal requirements*
b. *Reviews of security policy and technical compliance*
c. *System audit and consideration*

5. Keamanan Fisik dan Lingkungan (*Physical and Environmental Security*);

Hal ini berkaitan dengan pencegahan pengaksesan secara fisik oleh orang yang tidak berwenang terhadap penggunaan sistem (beserta informasinya) dan perangkat kerasnya sekaligus. Serta pencegahan terhadap gangguan lingkungan sekitar yang dapat membahayakan (hilang atau rusak) aset perusahaan baik yang berupa informasi atau perangkat sistem informasi lainnya. Aspek yang dibahas antara lain:

a. *Secure areas*
b. *Equipment security*
c. *General control*

6. Komunikasi dan Manajemen Operasi (*Communication and Operations Management*);

Menyediakan perlindungan terhadap infrastruktur sistem informasi melalui perawatan dan pemeriksaan berkala, serta memastikan ketersediaan panduan sistem yang terdokumentasi dan dikomunikasikan guna menghindari kesalahan operasional. Pengaturan tentang alur komunikasi dan operasi yang terjadi meliputi berbagai aspek, yaitu:

a. *Operational procedures and reponsibilities*
b. *System planning and acceptance*
c. *Protection against malicious software*
d. *Housekeeping*
e. *Network management*
f. *Media handling and security*
g. *Exchange of information and software*

7. Kendali Akses Sistem (*System Access Control*);

Mengendalikan/membatasi akses user terhadap informasi-informasi yang telah diatur kewenangannya, termasuk pengendalian secara mobile-computing ataupun tele-networking. Mengontrol tata cara akses terhadap informasi dan sumber daya yang ada meliputi berbagai aspek, yaitu:

a. *Access control*
b. *User access management*
c. *User responsibilities*
d. *Network access control*
e. *Operation system access control*
f. *Application access control*
g. *Monitor system access and use*
h. *Mobile computing and telenetworking*

8. Pengembangan Sistem dan Pemeliharaan (*System Development and Maintenance*);

Memastikan bahwa sistem operasi maupun aplikasi yang akan diimplementasikan mampu bersinergi melalui verifikasi/validasi terlebih dahulu sebelum diluncurkan ke *live environment*. Penelitian untuk pengembangan dan perawatan sistem yang ada meliputi berbagai aspek, yaitu:

a. *Security requirements of system*
b. *Security in application system*

c. *Cryptographic control*
d. *Security of system files*
e. *Security in development and support process*

9. Perencanaan Kesinambungan Bisnis (*Business Continuity Planning*);

Hal ini merupakan langkah yang dilakukan pada saat terjadi gangguan atau bencana sehingga tidak mengganggu atau menginterupsi aktivitas dan proses bisnis. Sehingga diperlukan pengaturan dan manajemen untuk kelangsungan proses bisnis, dengan mempertimbangkan: *Aspects of business continuity management*.

10. Pemenuhan (*Compliance*);

Hal ini bertujuan untuk menjaga agar sistem memenuhi persyaratan dan standar keamanan perusahaan. Selain itu sistem yang ada harus terhindar dari pelanggaran terhadap ketentuan hukum yang berlaku. Kepatuhan yang mengarah kepada pembentukan prosedur dan aturan-aturan sesuai dengan hukum yang berlaku meliputi berbagai aspek, yaitu:

a. *Compliance with legal requirements*
b. *Reviews of security policy and technical comliance*
c. *System audit and consideration*

Keuntungan utama dari ISO 17799 berhubungan dengan kepercayaan publik. Selain itu keuntungan yang didapat diantaranya:

1. Standar ini merupakan tanda kepercayaan dalam seluruh keamanan perusahaan.
2. Manajemen kebijakan terpusat dan prosedur.
3. Menjamin layanan informasi yang tepat guna.
4. Mengurangi biaya manajemen,
5. Dokumentasi yang lengkap atas segala perubahan/revisi.
6. Suatu metoda untuk menentukan target dan mengusulkan peningkatan.
7. Basis untuk standard keamanan informasi internal perusahaan

Suatu organisasi yang menerapkan ISO 17799 akan mempunyai suatu alat untuk mengukur, mengatur dan mengendalikan informasi yang penting bagi operasional sistem mereka. Pada gilirannya ini dapat mendorong kearah kepercayaan pelanggan, efisiensi dan efektifitas.

III. Dampak dari Pemanfaatan Komputer

Teknologi dapat memberikan solusi atas masalah-masalah yang dihadapi manusia, terutama masalah pengelolaan informasi yang semula masih dikerjakan secara manual

saat ini beralih dengan menggunakan mesin-mesin yang mutakhir seperti komputer. Akan tetapi pemanfaatan komputer ini berdampak pada munculnya beberapa masalah tambahaan untuk pemeriksaan dan pengontrolan yang sebelumnya mungkin belum pernah ada.

1. Sentralisasi data

Sebelum adanya komputer, masing-masing departemen di dalam perusahaan bertanggung jawab atas data masing-masing. Informasi yang masih berupa kertas akan disimpan dalam lemari arsip.

Saat ini data tersebut yang sudah dalam bentuk digital disimpan di sistem database terpusat. Atau ada juga yang menerapkan satu database untuk satu departemen. Hal tersebut dapat mengakibatkan terjadinya redundansi data dan kurangnya integritas data.

2. Pengaksesan data

Pengaksesan informasi dapat lebih mudah dilakukan baik dari dalam maupun dari luar organisasi. Dengan pemanfaatan teknologi berupa jaringan komputer, informasi menjadi dapat diakses oleh beberapa karyawan yang bersangkutan (tergantung kewenangan). Akan tetapi hal ini membutuhkan pengontrolan terhadap akses setiap informasi yang ada pada sistem.

3. Pemisahan tugas

Pemisahan tanggung jawab dan tugas menjadi tidak mudah lagi karena memungkinkannya beberapa tugas dilakukan bersama-sama atau satu orang melakukan beberapa tugas secara bersamaan.

4. Kekurangan bukti audit secara fisik (*audit trail*)

Masih kurangnya sistem yang dibekali dengan fasilitas informasi yang dibutuhkan oleh auditor seperti informasi mengenai kejanggalan transaksi.

5. Tidak tersedianya prosedur dan dokumentasi yang memadai

Banyak sistem komputer yang tidak memiliki buku panduaan (*manual book*). Hal ini akan menjadi faktor penghambat penggunaan sistem komputer. Khusus untuk sistem yang dikembangkan sendiri, harus dilengkapi dengan dokumentasi pembangunan. Dokumen tersebut diperlukan pada saat dibutuhkan tahapan perbaikan atau pengembangan sistem.

6. Pengetahuan teknologi yang tinggi

Saat ini sudah banyak yang memiliki pengetahuan teknologi, termasuk pengetahuan dalam pembangunan sistem. Hal ini menyebabkan kemungkinan beberapa pemakai melakukan perubahan terhadap sistem yang diterapkan di perusahaan.

7. Teknologi telah mengubah pola berbisnis

Perubahan pola berbisnis dapat disebabkan oleh penerapan teknologi, salah satunya dengan adanya jaringan internet. Sistem menjadi bersifat global yang artinya setiap orang memungkinkan mengakses terhadap sistem perusahaan. Hal tersebut menimbulkan ancaman adanya pengguna yang mengakses sistem perusahaan tanpa memiliki wewenang.

8. Tingkat otorisasi

Dengan menggunakan komputer maka tingkat otoritas pengguna menjadi lebih mudah diimplementasikan.

9. Keterlibatan audit

Keterlibatan audit menjadi lebih dibutuhkan dalam menjamin adanya kontrol di dalam penggunaan komputer untuk menjamin sistem informasi dapat berjalan dengan baik dan meminimalisir gangguan atau ancaman dari luar sistem.

IV. Kebutuhan atas Strategi Keamanan Sistem Informasi

Strategi keamanan sistem informasi dibutuhkan karena:

1. Tidak dapat dipungkiri lagi bahwa informasi yang dihasilkan oleh komputer merupakan hal yang penting untuk memenuhi kebutuhan perusahaan.
2. Teknologi baru telah mengubah pola lingkungan bisnis yang menciptakan ancaman dan serangan dari luar lingkungan.
3. Keamanan ini merupakan kunci keberhasilan dalam penggunaan alat bantu dalam proses bisnis baik dalam bentuk *software*, *hardware* beserta jaringannya.
4. Untuk menetapkan standar kebijakan dalam pengoperasian sistem informasi termasuk penggunaan alat bantu baru (*hardware*, *software*, jaringan).
5. Menjamin kepercayaan terhadap teknologi yang digunakan.

V. Daftar Pustaka

[1] IBISA. 2011. Keamanan Sistem Informasi. Yogyakarta: Andi.
[2] Isa, I. 2012. Evaluasi Pengontrolan Sistem Informasi. Yogyakarta: Graha Ilmu.
[3] Laudon, K.C. & Laudon, J.P. 2005. Sistem Informasi Manajemen: Mengelola Perusahaan Digital, Edisi 8. Yogyakarta: Andi.

[4] Sarno, R. & Iffano, I. 2010. Sistem Manajemen Keamanan Informasi (Berbasis ISO 27001). Surabaya: ITS Press.

VI. Materi Berikutnya

Pokok Bahasan	Manajemen Resiko Sistem Informasi
Sub Pokok Bahasan	1. Definisi resiko 2. Proses manajemen resiko