KEAMANAN SISTEM INFORMASI

3 SKS | Semester 8 | S1 Sistem Informasi

Pertemuan 3

Nizar Rabbi Radliya
nizar.radliya@yahoo.com

Kebijakan Keamanan Sistem Informasi

Setiap organisasi harus memiliki pedoman bagi anggotanya untuk mencapai sasaran.

Kebijakan KSI disusun oleh:

- ✓ **Pimpinan Operasional**
- ✓ **ICT**
- ✓ **Pimpinan Organisasi**

Kebijakan Keamanan Sistem Informasi

Keamanan SI merupakan urusan dan tanggung jawab semua karyawan.

Memunculkan tanggung jawab karyawan dapat dilakukan dengan cara:

a. Mengadakan pelatihan atau sosialisi,

b. Mencantumkan ketentuan pada surat kontrak,

c. Memberikan surat peringatan pada setiap pelanggaran.

Kebijakan Keamanan Sistem Informasi

Penetapan pemilik sistem informasi.

- ✓ Menunjuk atau menetapkan seorang karyawan sebagai pemilik sistem (sub sistem) >> administrator / operator
- ✓ Dijadikan sebagai contact person bagi ICT

Kebijakan Keamanan Sistem Informasi

Langkah keamanan harus sesuai dengan peraturan dan undang-undang.

- ✓ Mematuhi undang-undang yang telah ditetapkan yang berikaitan dengan proteksi data, cyber law, dan hak cipta.

Kebijakan Keamanan Sistem Informasi

Antisipasi terhadap kesalahan.

- ✓ Diakibatkan meningkatnya proses transaksi secara online dan real time.
- ✓ Apabila terjadi kesalahan tidak dapat langsung diperbaiki atau akan menyita banyak waktu.

Kebijakan Keamanan Sistem Informasi

Pengaksesan ke dalam sistem harus berdasarkan kebutuhan fungsi.

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

Kebijakan Keamanan Sistem Informasi

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

- ✓ Sistem komputer milik perusahaan beserta jaringannya hanya dipakai demi kepentingan bisnis perusahaan.
- ✓ Data yang diperbolehkan disimpan dalam sistem hanya data-data yang berkaitan dengan proses bisnis perusahaan.

Kebijakan Keamanan Sistem Informasi

Pekerjaan yang dilakukan oleh pihak ketiga.

- ✓ Pengaturan pada surat kontrak
- ✓ Menunjuk seseorang sebagai perwakilan perusahaan

Kebijakan Keamanan Sistem Informasi

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

- ✓ Dianjurkan untuk diadakan pemisahan secara fungsional antara pengembang sistem, pengoperasian sistem harian dan pemakai akhir sistem.

Kebijakan Keamanan Sistem Informasi

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).

Kebijakan Keamanan Sistem Informasi

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

- ✓ Keseragaman bahasa pemrograman
- ✓ Keseragaman DBMS
- ✓ Melakukan pengujian (QA) berkaitan dengan keamanan sistem

Kebijakan Keamanan Sistem Informasi

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

- ✓ Memperhatikan keseragaman bahasa pemrograman, DBMS dan teknologi lainnya
- ✓ Melakukan pengujian (QA) berkaitan dengan keamanan sistem

Kebijakan Keamanan Sistem Informasi

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

- ✓ Semua aktivitas yang dilakukan oleh ID yang bersangkutan harus terekam dalam sebuah sistem.

Standar Keamanan SI pada ISO

ISO 17799

Perkembangan:

BS 7799 – Tahun 1995

ISO/IEC 17799:2000

ISO/IEC 17799:2005

ISO/IEC 27002 – Tahun 2005-2007

Daftar Singkatan:

BS (British Standard)

IOS (International Organization of Standardization)

IEC (International Electro-Technical Commission)

ISO 17799

Komponen-komponen dari ISO 17799 meliputi:

10 control clauses

36 control objectives

127 controls

ISO 17799

Control Clouse: Kebijakan Keamanan (Security Policy)

Control Objective:

1. **Information security infrastructure**
2. **Information security policy**

Control Clouse: Organisasi Keamanan (Security Organisation)

Control Objective:

1. **Security of third party access**
2. **Outsourcing**

ISO 17799

Control Clouse: Penggolongan Asset dan Kendali (Asset Classification and Control)

Control Objective:

1. **Accountability for assets**
2. **Information classification**

Control Clouse: Keamanan Personil (Personnel Security)

Control Objective:

1. **Compliance with legal requirements**
2. **Reviews of security policy and technical compliance**
3. **System audit and consideration**

ISO 17799

Control Clouse: Keamanan Fisik dan Lingkungan (Physical and Environmental Security)

Control Objective:

1. **Secure areas**
2. **Equipment security**
3. **General control**

ISO 17799

Control Clouse: Komunikasi dan Manajemen Operasi (Communication and Operations Management)

Control Objective:

1. **Operational procedures and reponsibilities**
2. **System planning and acceptance**
3. **Protection against malicious software**
4. **Housekeeping**
5. **Network management**
6. **Media handling and security**
7. **Exchange of information and software**

ISO 17799

Control Clouse: Kendali Akses Sistem (System Access Control)

Control Objective:

1. **Access control**
2. **User access management**
3. **User responsibilities**
4. **Network access control**
5. **Operation system access control**
6. **Application access control**
7. **Monitor system access and use**
8. **Mobile computing and telenetworking**

ISO 17799

Control Clouse: Pengembangan Sistem dan Pemeliharaan (System Development and Maintenance)

Control Objective:

1. **Security requirements of system**
2. **Security in application system**
3. **Cryptographic control**
4. **Security of system files**
5. **Security in development and support process**

ISO 17799

Control Clouse: Perencanaan Kesinambungan Bisnis (Business Continuity Planning)

Control Objective:

1. **Aspects of business continuity management.**

Control Clouse: Pemenuhan (Compliance)

Control Objective:

1. **Compliance with legal requirements**
2. **Reviews of security policy and technical comliance**
3. **System audit and consideration**

ISO 17799

Keuntungan dari ISO 17799 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

Materi Minggu Ke 4

Manajemen Resiko Sistem Informasi

1. Definisi resiko
2. Proses manajemen resiko

KEAMANAN SISTEM INFORMASI

3 SKS | Semester 8 | S1 Sistem Informasi

Nizar Rabbi Radliya
nizar.radliya@yahoo.com