Etika dan Keamanan SI

Etika dalam Sistem Informasi

- Etika : kepercayaan tentang hal yang benar dan salah atau yang baik dan yang tidak
- Etika dalam SI dibahas pertama kali oleh Richard Mason (1986), yang mencakup PAPA:
  1. Privasi
  2. Akurasi
  3. Properti
  4. Akses

Etika dalam Sistem Informasi

- **PRIVASI** menyangkut hak individu untuk mempertahankan informasi pribadi dari pengaksesan oleh orang lain yang memang tidak diberi izin untuk melakukannya
- Kasus:
  - *Junk mail*
  - Manajer pemasaran mengamati *e-mail* bawahannya
  - Penjualan data akademis

Etika dalam Sistem Informasi

- **AKURASI** terhadap informasi merupakan faktor yang harus dipenuhi oleh sebuah sistem informasi
- Ketidakakurasian informasi dapat menimbulkan hal yang menggangu, merugikan, dan bahkan membahayakan.
- Kasus:
  - Terhapusnya nomor keamanan sosial yang dialami oleh Edna Rismeller (Alter, 2002, hal. 292)
  - Kasus kesalahan pendeteksi misil Amerika Serikat

Etika dalam Sistem Informasi

- Perlindungan terhadap hak PROPERTI yang sedang digalakkan saat ini yaitu yang dikenal dengan sebutan HAKI (hak atas kekayaan intelektual).
- HAKI biasa diatur melalui hak cipta (*copyright*), paten, dan rahasia perdagangan (*trade secret*).

Etika dalam Sistem Informasi

- **Hak cipta** adalah hak yang dijamin oleh kekuatan hukum yang melarang penduplikasian kekayaan intelektual tanpa seizin pemegangnya
- Hak seperti ini mudah untuk didapatkan dan diberikan kepada pemegangnya selama masa hidup penciptanya plus 70 tahun.

Etika dalam Sistem Informasi

- **Paten** merupakan bentuk perlindungan terhadap kekayaan intelektual yang paling sulit didapatkan karena hanya akan diberikan pada penemuan-penemuan inovatif dan sangat berguna. Hukum paten memberikan perlindungan selama 20 tahun.

Etika dalam Sistem Informasi

- **Hukum rahasia perdagangan** melindungi kekayaan intelektual melalui lisensi atau kontrak.
- Pada lisensi perangkat lunak, seseorang yang menandatangani kontrak menyetujui untuk tidak menyalin perangkat lunak tersebut untuk diserahkan pada orang lain atau dijual.

Etika dalam Sistem Informasi

- Berkaitan dengan dengan kekayaan intelektual, banyak masalah yang belum terpecahkan (Zwass, 1998); Antara lain:
  - Pada level bagaimana informasi dapat dianggap sebagai properti?
  - Apa yang harus membedakan antara satu produk dengan produk lain?
  - Akankah pekerjaan yang dihasilkan oleh komputer memiliki manusia penciptanya? Jika tidak, lalu hak properti apa yang dilindunginya?

Etika dalam Sistem Informasi

- Fokus dari masalah AKSES adalah pada penyediaan akses untuk semua kalangan
- Teknologi informasi diharapkan malah tidak menjadi halangan dalam melakukan pengaksesan terhadap informasi bagi kelompok orang tertentu, tetapi justru untuk mendukung pengaksesan untuk semua pihak

Keamanan Sistem Informasi

- Keamanan merupakan faktor penting yang perlu diperhatikan dalam pengoperasian sistem informasi
- Tujuannya adalah untuk mencegah ancaman terhadap sistem serta untuk mendeteksi dan membetulkan akibat segala kerusakan sistem.

Keamanan Sistem Informasi

- Ancaman terhadap sistem informasi dapat dibagi menjadi dua macam: ancaman aktif dan ancaman pasif
- **Ancaman aktif** mencakup kecurangan dan kejahatan terhadap komputer
- **Ancaman pasif** mencakup kegagalan sistem, kesalahan manusia, dan bencana alam

Keamanan Sistem Informasi

Macam Ancaman	Contoh
Bencana alam dan politik	• Gempa bumi, banjir, kebakaran, perang
Kesalahan manusia	• Kesalahan pemasukan data • Kesalahan penghapusan data • Kesalahan operator (salah memberi label pada pita magnetik)
Kegagalan perangkat lunak dan perangkat keras	• Gangguan listrik • Kegagalan peralatan • Kegagalan fungsi perangkat lunak
Kecurangan dan kejahatan komputer	• Penyelewengan aktivitas • Penyalahgunaan kartu kredit • Sabotase • Pengaksesan oleh orang yang tidak berhak
Program yang jahat/usil	• Virus, cacing, bom waktu, dll

Keamanan Sistem Informasi

- Metode yang umum digunakan oleh orang dalam melakukan penetrasi terhadap sistem berbasis komputer ada 6 macam (Bodnar dan Hopwood, 1993), yaitu
  1. Pemanipulasian masukan
  2. Penggantian program
  3. Penggantian berkas secara langsung
  4. Pencurian data
  5. Sabotase
  6. Penyalahgunaan dan pencurian sumber daya komputasi.

Keamanan Sistem Informasi

- Berbagai teknik yang digunakan untuk melakukan *hacking*:
- **Denial of Service**

  Teknik ini dilaksanakan dengan cara membuat permintaan yang sangat banyak terhadap suatu situs sehingga sistem menjadi macet dan kemudian dengan mencari kelemahan pada sistem si pelaku melakukan serangan terhadap sistem.

  Sniffer

  Teknik ini diimplementasikan dengan membuat program yang dapat melacak paket data seseorang ketika paket tersebut melintasi Internet, menangkap *password* atau menangkap isinya.

  Spoofing

  Melakukan pemalsuan alamat *e-mail* atau Web dengan tujuan untuk menjebak pemakai agar memasukkan informasi yang penting seperti *password* atau nomor kartu kredit

Keamanan Sistem Informasi

- Penggunaan Kode yang Jahat:

1. Virus
2. Cacing (worm)
3. Bom waktu
4. Kuda Trojan

Pengendalian Sistem Informasi

- Untuk menjaga keamanan sistem informasi diperlukan pengendalian terhadap sistem informasi
- Kontrol mencakup:

1. Kontrol administratif
2. Kontrol pengembangan dan pemeliharaan sistem
3. Kontrol operasi
4. Proteksi terhadap pusat data secara fisik
5. Kontrol perangkat keras
6. Kontrol terhadap akses komputer
7. Kontrol terhadap akses informasi
8. Kontrol terhadap perlindungan terakhir
9. Kontrol aplikasi

Kontrol Administratif

- Mempublikasikan kebijakan kontrol yang membuat semua pengendalian sistem informasi dapat dilaksanakan dengan jelas dan serius oleh semua pihak dalam organisasi
- Prosedur yang bersifat formal dan standar pengoperasian disosialisasikan dan dilaksanakan dengan tegas. Termasuk dalam hal ini adalah proses pengembangan sistem, prosedur untuk *backup*, pemulihan data, dan manajemen pengarsipan data
- Perekrutan pegawai secara berhati-hati, yang diikuti dengan orientasi, pembinaan, dan pelatihan yang diperlukan

Kontrol Administratif (lanjutan…)

- Supervisi terhadap para pegawai. Termasuk pula cara melakukan kontrol kalau pegawai melakukan penyimpangan terhadap yang diharapkan
- Pemisahan tugas-tugas dalam pekerjaan, dengan tujuan agar tak seorangpun yang dapat menguasai suatu proses yang lengkap. Sebagai contoh, seorang pemrogram harus diusahakan tidak mempunyai akses terhadap data produksi (operasional) agar tidak memberikan kesempatan untuk melakukan kecurangan

Kontrol terhadap Pengembangan dan Pemeliharaan Sistem

- Melibatkan Auditor sistem, dari masa pengembangan hingga pemeliharaan sistem, untuk memastikan bahwa sistem benar-benar terkendali, termasuk dalam hal otorisasi pemakai sistem
- Aplikasi dilengkapi dengan *audit trail* sehingga kronologi transaksi mudah untuk ditelusuri

Kontrol Operasi

- Tujuan agar sistem beroperasi sesuai dengan yang diharapkan
- Termasuk dalam hal ini:

1. **Pembatasan akses terhadap pusat data**
2. **Kontrol terhadap personel pengoperasi**
3. **Kontrol terhadap peralatan** (terhadap kegagalan)
4. **Kontrol terhadap penyimpan arsip**
5. **Pengendalian terhadap virus**

Perlindungan Fisik terhadap Pusat Data

- Faktor lingkungan yang menyangkut suhu, kebersihan, kelembaban udara, bahaya banjir, dan keamanan fisik ruangan perlu diperhatikan dengan benar
- Untuk mengantisipasi kegagalan sumber daya listrik, biasa digunakan UPS dan mungkin juga penyediaan generator

Kontrol Perangkat Keras

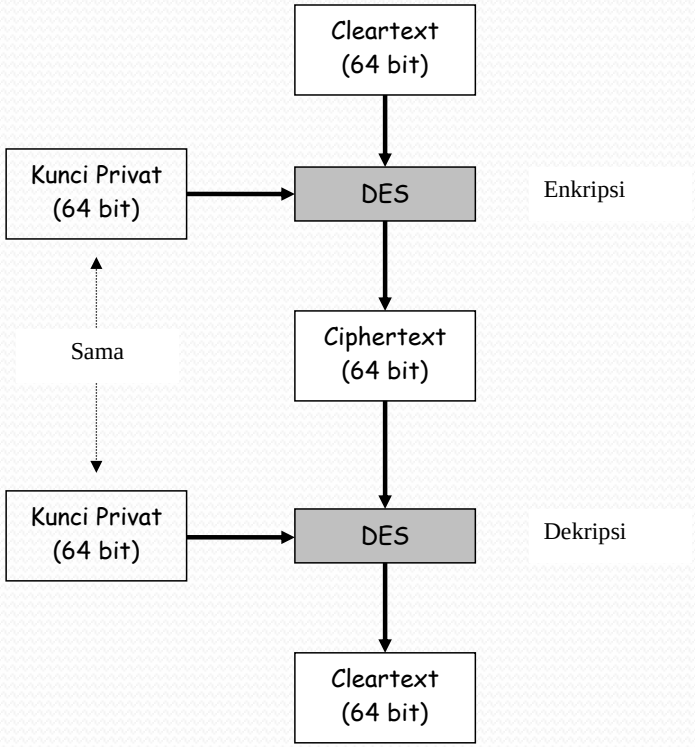
- Untuk mengantisipasi kegagalan sistem komputer, terkadang organisasi menerapkan sistem komputer yang berbasis *fault-tolerant* (toleran terhadap kegagalan)
- Toleransi terhadap kegagalan pada penyimpan eksternal antara lain dilakukan melalui *disk mirroring* atau *disk shadowing*, yang menggunakan teknik dengan menulis seluruh data ke dua *disk* secara paralel

Kontrol Akses terhadap Sistem Komputer

- Setiap pemakai sistem diberi otorisasi yang berbeda-beda
- Setiap pemakai dilengkapi dengan nama pemakai dan *password*
- Penggunaan teknologi yang lebih canggih menggunakan sifat-sifat biologis manusia yang bersifat unik, seperti sidik jari dan retina mata, sebagai kunci untuk mengakses sistem

Kontrol terhadap Akses Informasi

- Penggunaan enksripsi



Kontrol terhadap Bencana

- Rencana darurat (*emergency plan*) menentukan tindakan-tindakan yang harus dilakukan oleh para pegawai manakala bencana terjadi
- Rencana cadangan (*backup plan*) menentukan bagaimana pemrosesan informasi akan dilaksanakan selama masa darurat.
- Rencana pemulihan (*recovery plan*) menentukan bagaimana pemrosesan akan dikembalikan ke keadaan seperti aslinya secara lengkap, termasuk mencakup tanggung jawab masing-masing personil
- Rencana pengujian (*test plan*) menentukan bagaimana komponen-komponen dalam rencana pemulihan akan diuji atau disimulasikan

Kontrol terhadap Perlindungan Terakhir

- Rencana pemulihan dari bencana
- Asuransi

Kontrol Aplikasi

- Masukan
- Keluaran
- Pemrosesan
- Basis data
- Telekomunikasi