Tata Kelola dan Kepatuhan

Mohamad Iqbal

Tata Kelola

Tata kelola keamanan TI menentukan siapa yang berwenang untuk membuat keputusan tentang risiko keamanan siber dalam suatu organisasi.
Hal ini menunjukkan akuntabilitas dan memberikan pengawasan untuk memastikan bahwa setiap risiko telah dimitigasi secara memadai dan bahwa strategi keamanan selaras dengan tujuan bisnis organisasi dan mematuhi peraturan.

Peran Kunci

Data owner

Seseorang yang memastikan kepatuhan terhadap kebijakan dan prosedur, menetapkan klasifikasi yang tepat untuk aset informasi, dan menentukan kriteria untuk mengakses aset informasi.

Data processor

Seseorang atau organisasi yang memproses data pribadi atas nama pengontrol data.

Data Custodian

Seseorang yang melaksanakan klasifikasi dan pengendalian keamanan data sesuai dengan aturan yang ditetapkan oleh pemilik data. Dengan kata lain, penjaga data bertanggung jawab atas pengendalian teknis data.

Data controller

Seseorang yang menentukan tujuan dan cara pemrosesan data pribadi.

Data steward

Seseorang yang memastikan bahwa data mendukung kebutuhan bisnis organisasi dan memenuhi persyaratan peraturan.

Data protection officer

Seseorang yang mengawasi strategi perlindungan data organisasi.

Kebijakan Keamanan Siber

Kebijakan keamanan siber adalah dokumen tingkat tinggi yang menguraikan visi organisasi mengenai keamanan siber, termasuk tujuan, kebutuhan, ruang lingkup, dan tanggung jawabnya.

- **Menunjukkan komitmen organisasi terhadap keamanan.**
- **Menetapkan standar perilaku dan persyaratan keamanan untuk menjalankan aktivitas, proses, dan operasi, serta melindungi aset teknologi dan informasi dalam suatu organisasi.**
- **Memastikan bahwa akuisisi, penggunaan, dan pemeliharaan operasi sistem, perangkat lunak, dan perangkat keras konsisten di seluruh organisasi.**
- **Mendefinisikan konsekuensi hukum dari pelanggaran kebijakan.**
- **Memberi tim keamanan dukungan yang mereka perlukan dari manajemen senior.**

Kebijakan Keamanan Siber

- **Master cybersecurity policy**
  - Sebagai cetak biru program keamanan siber suatu organisasi, kebijakan ini berfungsi sebagai rencana strategis untuk menerapkan kontrol keamanan siber.

- **System-specific policy**
  - Kebijakan ini dikembangkan untuk perangkat atau sistem komputer tertentu dan bertujuan untuk menetapkan standarisasi aplikasi, perangkat lunak, konfigurasi sistem operasi, perangkat keras, dan tindakan pencegahan yang disetujui dalam suatu organisasi.
- **Issue-specific policy**
  - Kebijakan ini dikembangkan untuk masalah, keadaan, atau kondisi operasional tertentu yang mungkin memerlukan persyaratan dan arahan yang lebih rinci.

Jenis Kebijakan Keamanan

Identification and authentication policy	Menentukan siapa yang harus diizinkan mengakses sumber daya jaringan dan prosedur verifikasi apa yang diterapkan untuk memfasilitasi hal ini.
Password policy	Menentukan persyaratan kata sandi minimum.
Acceptable use policy	Menyoroti serangkaian aturan yang menentukan akses dan penggunaan sumber daya jaringan.
Remote access policy	Menetapkan cara terhubung dari jarak jauh ke jaringan internal organisasi dan menjelaskan informasi apa saja yang dapat diakses dari jarak jauh.
Network maintenance policy	Menguraikan prosedur untuk memperbarui sistem operasi tertentu dan aplikasi pengguna akhir organisasi.
Incident handling policy	Memberikan panduan tentang cara melaporkan dan merespons insiden terkait keamanan dalam suatu organisasi.
Data policy	Menetapkan aturan terukur untuk memproses data dalam suatu organisasi, seperti menentukan lokasi penyimpanan data, cara data diklasifikasikan, dan cara data ditangani dan dibuang.
Credential policy	Menerapkan aturan untuk membuat kredensial.
Organizational policy	Memberikan panduan tentang bagaimana pekerjaan harus dilakukan dalam suatu organisasi.

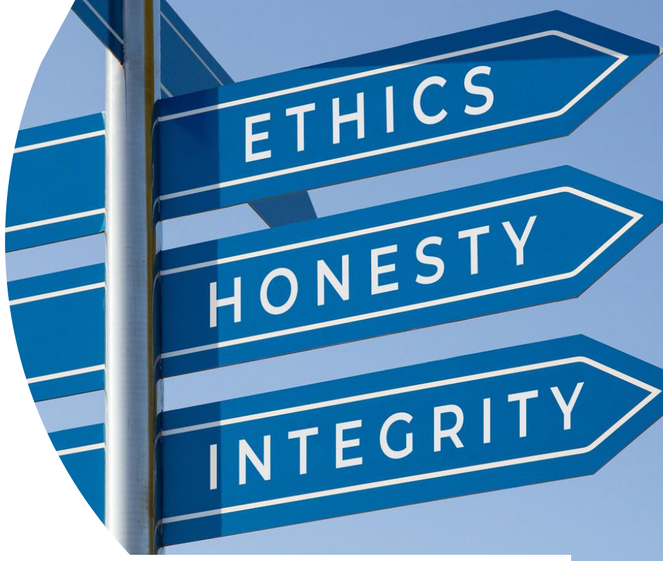
Etika Keamanan Siber

Etika adalah suara kecil di kepala Anda yang memberi tahu Anda apa yang benar dan apa yang salah, membimbing Anda untuk mengambil keputusan yang tepat.

Pakar keamanan siber perlu memahami hukum dan kepentingan organisasi agar dapat mengambil keputusan.

Etika Spesialis Keamanan Siber

3 Sudut Pandang



Utilitarian ethics	Hal ini didasarkan pada prinsip pedoman bahwa konsekuensi suatu tindakan merupakan faktor terpenting dalam menentukan apakah tindakan tersebut bermoral atau tidak. Misalnya, tindakan yang memaksimalkan kebaikan bagi sebanyak mungkin orang adalah pilihan etis.
The rights approach	Hal ini berpedoman pada asas yang menyatakan bahwa setiap individu mempunyai hak untuk menentukan pilihannya sendiri, yang tidak dapat dilanggar oleh keputusan orang lain. Keputusan ini harus menghormati dan mempertimbangkan hak-hak dasar individu. Hak-hak dasar ini mencakup hak atas kebenaran, privasi, keamanan, dan hak masyarakat untuk menerapkan hukum secara adil kepada seluruh anggota masyarakat.
The common good approach	Ia mengusulkan bahwa tindakan etis adalah tindakan yang bermanfaat bagi seluruh masyarakat. Hal ini menantang individu untuk mengenali dan mengejar nilai-nilai dan tujuan bersama dengan anggota komunitas lainnya.

Etika Penggunaan Teknologi Digital

- Pada hakikatnya semua etika dan moral lingkungan fisik dan lingkungan digital sama.

- Yang berbeda adalah alat bantu, media yang digunakan dan proses terkait.

- Tidak menggunakan teknologi digital untuk mencelakakan orang lain
- Tidak menggunakan teknologi digital untuk mengganggu pekerjaan orang lain
- Tidak mengakses data dan informasi milik orang lain tanpa hak
- Tidak menggunakan teknologi digital untuk mencuri
- Tidak menggunakan teknologi digital untuk bersaksi palsu
- Tidak menggunakan atau menggandakan perangkat lunak tanpa hak
- Tidak menggunakan perangkat digital tanpa ijin atau memenuhi kewajiban
- Tidak menggunakan hak kekayaan intelektual orang lain tanpa hak
- Memperhatikan dampak terhadap orang lain dari perancangan atau pembuatan sistem yang dilakukan
- Menggunakan teknologi digital dengan selalu menghormati kepentingan orang lain

→

Kejahatan Siber

- Kejahatan bertarget komputer ketika komputer menjadi sasaran aktivitas kriminal. Contohnya termasuk malware, peretasan, atau serangan penolakan layanan.

- Kejahatan dengan bantuan komputer terjadi ketika komputer digunakan untuk melakukan kejahatan, seperti pencurian atau penipuan.

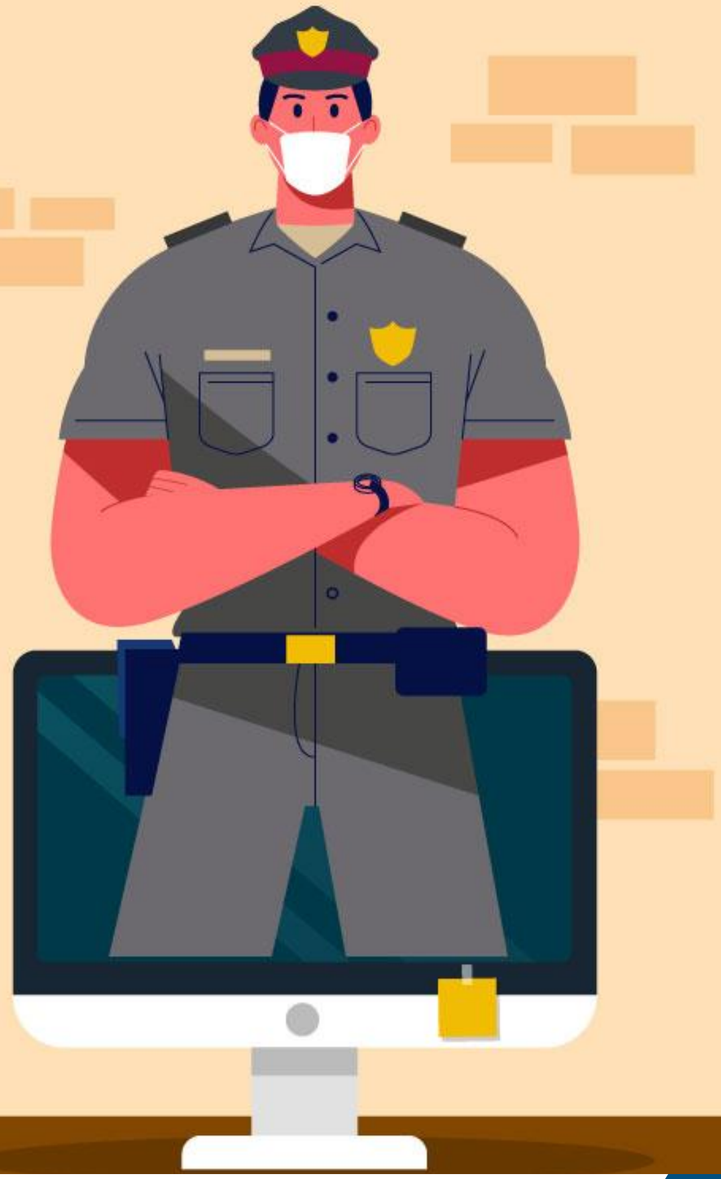
- Kejahatan insidental komputer saat komputer memberikan informasi yang bersifat insidentil terhadap kejahatan yang sebenarnya. Misalnya, komputer digunakan untuk menyimpan video yang diunduh secara ilegal, bukan alat sebenarnya yang digunakan untuk melakukan kejahatan.

Poin Penting Penanganan UU ITE

Indonesia baik.id

WSIS PRIZES 2018 WINNER

1. Mengikuti perkembangan pemanfaatan ruang digital yang terus berkembang
2. Memahami budaya beretika yang terjadi di ruang digital
3. Mengedepankan upaya preemtif dan preventif melalui ***virtual police*** dan ***virtual alert***
4. Dalam menerima laporan dari masyarakat, penyidik harus dapat dengan tegas membedakan antara kritik, masukan, hoaks, dan pencemaran nama baik
5. Berkomunikasi dengan para pihak terutama korban (tidak diwakilkan) dan memfasilitasi untuk mediasit



4 TINDAK PIDANA DALAM UU PDP DAN SANKSINYA

Dasar Hukum: Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi

Chatbot Hukum Pertama di Indonesia

2

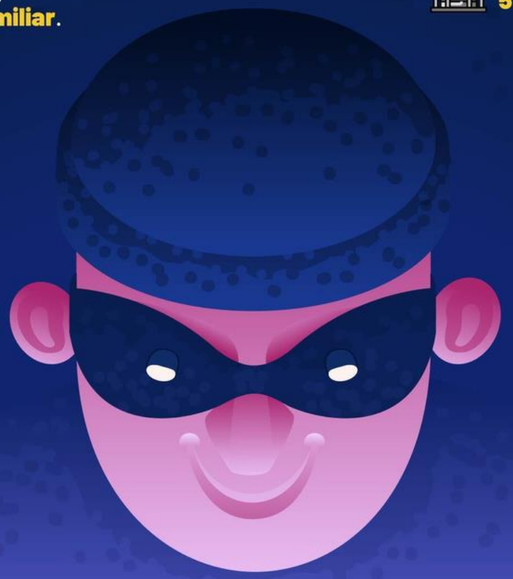
Setiap orang dengan sengaja dan melawan hukum **mengungkapkan data pribadi yang bukan miliknya**.

Maks. **4 tahun**. Maks. **Rp4 miliar**.

3

Setiap orang dengan sengaja dan melawan hukum **menggunakan data pribadi yang bukan miliknya**.

Maks. **5 tahun**. Maks. **Rp5 miliar**.



1

Setiap orang dengan sengaja dan melawan hukum **memperoleh atau mengumpulkan data pribadi yang bukan miliknya** dengan maksud menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian subjek data pribadi.

Maks. **5 tahun**. Maks. **Rp5 miliar**.

4

Setiap orang dengan sengaja **membuat data pribadi palsu atau memalsukan data pribadi** dengan maksud menguntungkan diri sendiri atau orang lain yang dapat mengakibatkan kerugian orang lain.

Maks. **6 tahun**. Maks. **Rp6 miliar**.

Kerangka Manajemen Keamanan TI

ISO/IEC 27000 merupakan serangkaian standar keamanan informasi atau praktik terbaik untuk membantu organisasi meningkatkan keamanan informasi.

Diterbitkan oleh ISO dan ICO, standar ISO 27000 menetapkan persyaratan sistem manajemen keamanan informasi (ISMS) yang komprehensif.

Dua Belas Domain Keamanan Siber

Risk assessment	Ini adalah langkah pertama dalam proses manajemen risiko, yang menentukan nilai risiko kuantitatif dan kualitatif terkait dengan situasi atau ancaman tertentu.
Security policy	Dokumen ini membahas kendala dan perilaku individu dalam suatu organisasi dan sering kali menentukan cara data dapat diakses, dan data apa yang dapat diakses oleh siapa.
Organization of information security	Ini adalah model tata kelola yang ditetapkan oleh organisasi untuk keamanan informasi.
Asset management	Ini adalah inventarisasi dan skema klasifikasi untuk aset informasi dalam suatu organisasi.
Human resources security	Hal ini mengacu pada prosedur keamanan yang diterapkan terkait dengan masuknya karyawan, pindah ke dalam, dan keluar dari organisasi.
Physical and environmental security	Hal ini mengacu pada perlindungan fisik fasilitas dan informasi organisasi.
Communications and operations management	Hal ini mengacu pada pengelolaan kontrol keamanan teknis pada sistem dan jaringan organisasi.

Dua Belas Domain Keamanan Siber

Information systems acquisition, development, and maintenance	Hal ini mengacu pada keamanan sebagai bagian integral dari sistem informasi organisasi.
Access controls	Hal ini menjelaskan cara organisasi membatasi hak akses ke jaringan, sistem, fungsi aplikasi, dan data untuk mencegah akses pengguna yang tidak sah.
Information security incident management	Hal ini menjelaskan pendekatan organisasi dalam mengantisipasi dan merespons pelanggaran keamanan informasi.
Business continuity management	Hal ini menggambarkan kemampuan organisasi untuk melindungi, memelihara, dan memulihkan aktivitas penting bisnis setelah terjadi gangguan pada sistem informasi.
Compliance	Hal ini menjelaskan proses memastikan kepatuhan terhadap kebijakan, standar, dan peraturan keamanan informasi.

NIST
National Institute of Standards and Technology

Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communication	Improvements
Governance	Data Security	Detection Processes	Analysis	Communication
Risk Assessment	Info Protection Processes and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

Govern

Fungsi ini menekankan bahwa keamanan siber merupakan sumber utama risiko perusahaan dan menjadi pertimbangan bagi pimpinan senior.

Social engineering bypasses all technologies, including firewalls.

ANONYMOUS