Kebijakan Keamanan Sistem Informasi

Modul ini membahas salah satu elemen kunci dari lingkungan pengendalian internal dalam organisasi: kebijakan keamanan sistem informasi (SI). Kebijakan keamanan SI memberikan kerangka kerja tingkat tinggi dimana semua kontrol keamanan terkait SI lainnya berasal.

Tujuan Pembelajaran

Memahami Konsep

Mahasiswa mampu memahami tentang kebijakan keamanan sistem informasi dan penerapannya dalam organisasi

Merancang Kebijakan

Mahasiswa mampu merancang kebijakan keamanan sistem informasi yang efektif dan komprehensif

Implementasi Praktis

Mahasiswa mampu menerapkan standar dan pedoman keamanan dalam lingkungan bisnis nyata

Realitas Mengejutkan: Kondisi Kebijakan Keamanan SI

Survei Datapro Information Services Group tahun 1996 terhadap lebih dari 1.300 organisasi dari Amerika Serikat, Kanada, Amerika Tengah dan Selatan, Eropa, dan Asia mengungkapkan fakta mengejutkan:

54%

Memiliki Kebijakan

Hanya 54% organisasi yang memiliki kebijakan keamanan SI - turun dari 82% pada tahun 1992

62%

Penanggung Jawab

Hanya 62% organisasi yang menetapkan orang tertentu bertanggung jawab terhadap keamanan komputer

<5%

Alokasi Anggaran

Kurang dari 5% anggaran TI dialokasikan untuk keamanan di sebagian besar organisasi

Temuan Survei Global Terkini

Survei Xephon of England England

Mengkonfirmasi temuan Datapro bahwa kurang dari 60% organisasi memiliki kebijakan keamanan SI. Dari yang memiliki kebijakan, hanya satu dari lima yang berdasarkan pada standar eksternal.

Survei Information Security (2000)

22% organisasi tidak memiliki kebijakan keamanan dan 2% responden tidak tahu apakah organisasi mereka memiliki kebijakan.

Survei Internet Week 2000: 25% manajer IT dan keamanan tidak memiliki kebijakan keamanan IT resmi

Mengapa Hasil Ini Mengkhawatirkan?

1

Organisasi Terlena

Banyak organisasi terlena dengan keamanan informasi di era komputer dan sistem informasi berkembang eksponensial

2

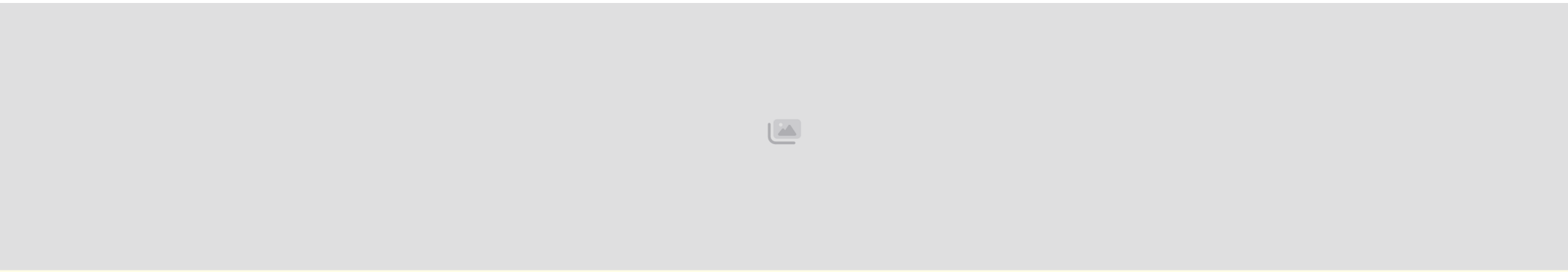
Risiko Kritis Meningkat

Tanpa kebijakan keamanan SI, kelemahan pengendalian internal yang signifikan dapat diidentifikasi

3

Tindakan Segera Diperlukan

Kebijakan keamanan harus dikembangkan dan diimplementasikan sesegera mungkin untuk melindungi aset organisasi



Pentingnya Pembaruan Berkelanjutan

Prosedur harus dilaksanakan untuk memastikan kebijakan dan standar pendukung diperbarui secara berkala. Pembaruan harus mencakup:

- Undang-undang dan peraturan terbaru
- Perubahan dalam praktik teknologi
- Perkembangan praktik bisnis
- Ancaman keamanan baru yang muncul

Kebijakan dan setiap pembaruan harus disampaikan kepada semua karyawan secara teratur (setidaknya setiap tahun), termasuk staf kontingen seperti vendor, konsultan, dan pekerja temporer.

Memahami Perbedaan Istilah Kunci

Kebijakan (Policy)

Pernyataan tingkat tinggi yang menggambarkan tujuan umum organisasi berkaitan dengan kontrol dan keamanan sistem informasi

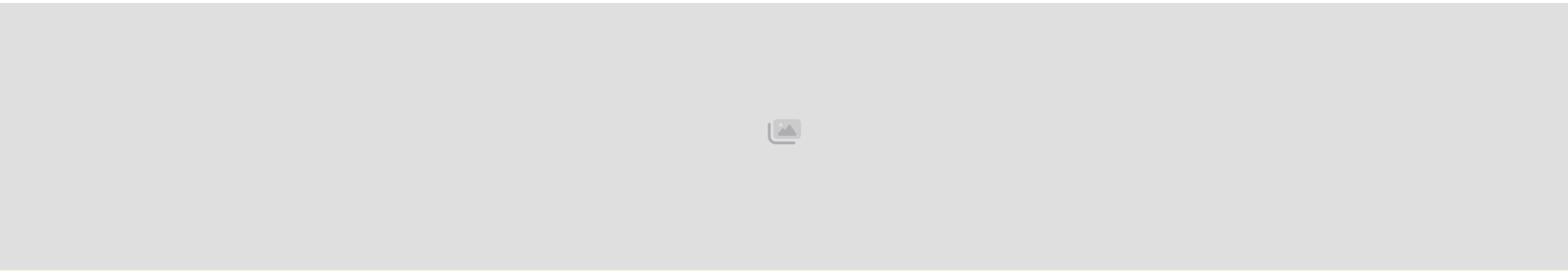
Standar (Standards)

Kriteria minimum, aturan dan prosedur rinci yang harus dilaksanakan untuk mencapai kebijakan keamanan SI

Pedoman (Guidelines)

Rekomendasi yang membantu implementasi tetapi tidak selalu diwajibkan oleh manajemen

Istilah-istilah ini sering digunakan secara bergantian, namun perbedaannya penting untuk dipahami sebelum mengevaluasi kecukupan keamanan SI dalam organisasi.



Kebijakan Keamanan Sistem Informasi

Definisi dan Karakteristik

Kebijakan keamanan sistem informasi adalah pernyataan keseluruhan tingkat tinggi yang menggambarkan tujuan umum organisasi berkaitan dengan kontrol dan keamanan atas sistem informasi.

Dibuat oleh Manajemen

Kebijakan biasanya dibuat oleh manajemen dan disetujui oleh Dewan Direksi

Menentukan Tanggung Jawab

Harus menentukan siapa yang bertanggung jawab untuk implementasinya

Tidak Terlalu Spesifik

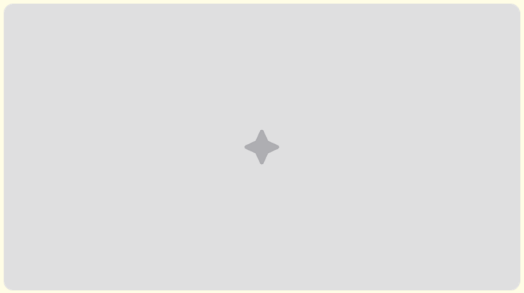
Harus cukup umum untuk menghindari perubahan konstan yang memerlukan persetujuan Dewan

Mengapa Kebijakan Tidak Boleh Terlalu Spesifik?

Proses Persetujuan Lambat

Dewan Direksi biasanya bertemu hanya setiap bulan. Perubahan kebijakan dapat memakan waktu beberapa bulan untuk menjadi resmi.

Perubahan signifikan mungkin memerlukan informasi tambahan atau penelitian sebelum voting.



Contoh Praktis: Kebijakan harus mensyaratkan "kontrol keamanan fisik dan logis yang memadai" bukan "password minimal 8 karakter" - detail seperti ini lebih tepat dalam standar

Contoh Kebijakan Keamanan SI

Kebijakan keamanan SI yang efektif biasanya terbagi menjadi lima bagian utama:

01

Tujuan dan Tanggung Jawab

Mendefinisikan tujuan keseluruhan dan siapa yang bertanggung jawab

02

Sistem Pengadaan dan Pembangunan Pembangunan

Mengatur proses pengembangan dan implementasi sistem baru

03

Akses Terminal

Mengatur hak akses dan penggunaan terminal sistem

04

Keamanan Peralatan dan Informasi

Melindungi aset fisik dan data organisasi

05

Program Biro Jasa

Mengatur hubungan dengan penyedia layanan eksternal

Bagian 1: Tujuan dan Tanggung Jawab

Definisi Sistem

Istilah "sistem" mengacu pada semua operasi komputer (mainframe, mini, mikro, komputer pribadi dan telekomunikasi) dan setiap area fungsional lainnya dimana data ditransmisikan melalui media elektronik atau telekomunikasi.

Tujuan Kebijakan

Memberikan pedoman penting untuk memproses transaksi elektronik yang efisien, pelaporan jasa, sistem informasi manajemen, dan kemampuan informasi yang tepat bagi manajemen dan Direksi.

Tanggung Jawab

Presiden atau individu yang ditunjuknya dan Komite Manajemen Senior bertanggung jawab mengelola sistem komputer dan telekomunikasi perusahaan, termasuk melakukan studi kelayakan dan mengarahkan implementasi sistem.

Rekomendasi Perbaikan: Definisi Definisi Sistem

Definisi sistem dalam kebijakan sering kali tertinggal zaman. Berikut adalah definisi yang lebih universal dan komprehensif:

> "Untuk tujuan kebijakan ini, istilah sistem menunjuk pada semua operasi komputer dalam perusahaan, termasuk namun tidak terbatas pada: mainframe, midranges, mini, jaringan lokal dan wide area, desktop pribadi dan komputer laptop, telekomunikasi, setiap teknologi baru yang sedang dikembangkan, dan komputer khusus lainnya di bidang fungsional dimana data ditransmisikan atau diproses melalui elektronik, telekomunikasi, satelit, microwave, atau media lain."

Bagian 2: Sistem Pengadaan dan Pembangunan

Pengadaan, pengembangan dan pengoperasian sistem pengolahan data harus dikelola melalui langkah-langkah evaluasi siklus hidup sistem:

Definisi Lingkup

Gambaran masalah yang perlu diatasi

Definisi Persyaratan

Gambaran persyaratan pengguna akhir dan tujuan pembangunan

Review Solusi Alternatif

Evaluasi berbagai opsi solusi

Desain Sistem

Perancangan arsitektur dan komponen sistem

Pengembangan Sistem

Pembangunan dan konfigurasi sistem

Pengujian Sistem

Verifikasi dan validasi fungsionalitas

Pemantauan Sistem

Monitoring kinerja dan keamanan berkelanjutan

Langkah Penting yang Hilang: Implementasi Sistem

Antara pengujian sistem dan pemantauan sistem, harus ada langkah krusial yang disebut **Implementasi Sistem**.

Mengapa Penting?

- Puncak dari semua perencanaan dan tahap pengembangan sebelumnya
- Sistem baru ditempatkan ke dalam produksi
- Tim mengetahui seberapa baik sistem bekerja dengan beban data langsung
- Implementasi utama sering dilakukan saat akhir pekan

Pertimbangan Implementasi

- Dapat berlangsung beberapa minggu atau bulan
- Sistem lama sering beroperasi paralel dengan yang baru
- Memberikan jaminan tambahan sistem baru mampu memproses data tanpa masalah

Bagian 4: Keamanan Peralatan dan Informasi

Pembentukan dan pemeliharaan program keamanan lengkap adalah tanggung jawab Presiden atau individu yang ditunjuknya. Kontrol dan keamanan meliputi:

1	2	3
Peralatan dan Ketahanan Lingkungan	**Keamanan Informasi dan Komunikasi**	**Kontingensi dan Pemulihan**
Keamanan fisik untuk sistem komputer dan telekomunikasi, termasuk catu daya tak terputus, perlindungan dari api, asap dan air, serta sistem HVAC yang memadai	Kontrol akses logis, klasifikasi sumber daya informasi, keamanan jaringan, retensi dan pembuangan informasi, serta sistem pelaporan insiden	Rencana pemulihan bencana, identifikasi aplikasi penting, dokumentasi backup, pengujian tahunan, dan penyimpanan data cadangan di luar lokasi

Perbaikan Keamanan Logis dan Jaringan

Dalam kebijakan asli, terdapat kebingungan antara kontrol akses logis dan keamanan jaringan. Keduanya sebenarnya bagian dari lingkungan keamanan logis yang sama.

Rekomendasi Perbaikan

Gabungkan kedua pernyataan kontrol menjadi frase tunggal yang menyeluruh:

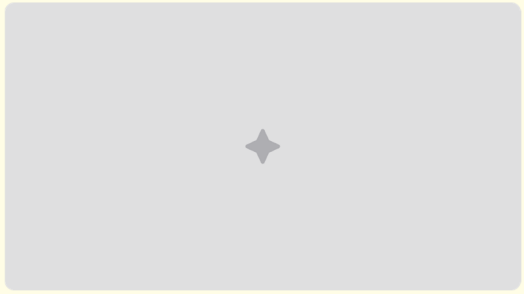
> "Kontrol akses logis dalam sistem operasi, sistem manajemen database, dan aplikasi dari semua sistem komputasi dan telekomunikasi perusahaan."

Definisi ini lebih jelas dan mencakup semua jenis sistem tanpa redundansi atau kebingungan.

Bagian 5: Program Biro Jasa

Persyaratan Utama

- Perjanjian harus mendetail tingkat dukungan yang disediakan
- Monitoring ketepatan waktu respons biro jasa
- Verifikasi sistem perangkat lunak baru sebelum konversi
- Dokumentasi rinci untuk operasi dan prosedur



Risiko Penting yang Sering Diabaikan: Disposisi kode sumber aplikasi jika biro jasa berhenti beroperasi atau gagal memenuhi kontrak

Perlindungan Kode Sumber: Escrow Agreement

Apa itu Escrow?

Kode sumber aplikasi versi terkini disimpan oleh pihak ketiga independen yang akan melepaskan kode ke organisasi klien jika aspek tertentu kontrak tidak terpenuhi

Mengapa Penting?

Mengurangi risiko gangguan bisnis jika biro jasa atau vendor perangkat lunak berhenti operasi. Organisasi dapat terus memelihara dan memodifikasi kode sampai pengganti cocok ditemukan

Rekomendasi Tambahan

Persyaratan escrow juga harus diterapkan dalam kontrak dengan vendor perangkat lunak yang memasok dan memelihara program tetapi bukan biro jasa

Ringkasan: Item dalam Kebijakan Keamanan SI

- **Pernyataan tujuan dan tanggung jawab**
- **Sistem pengadaan dan pendekatan pengembangan**
- **Peralatan dan ketahanan lingkungan (keamanan fisik)**
- **Keamanan informasi dan komunikasi (keamanan logis)**
- **Kontingensi dan pemulihan**
- **Program biro jasa (jika diterapkan)**
- **Vendor program perangkat lunak (jika diterapkan)**

Kebijakan harus diperiksa untuk memastikan mengandung setidaknya konsep-konsep ini, dengan penyesuaian sesuai sifat dan kompleksitas organisasi.

Standar Keamanan Sistem Informasi

Definisi

Standar keamanan sistem informasi adalah kriteria minimum, aturan dan prosedur yang ditetapkan oleh manajemen senior yang harus dilaksanakan untuk membantu memastikan pencapaian kebijakan keamanan SI.

Karakteristik Standar

- Menentukan persyaratan rinci masing-masing kontrol SI
- Tidak spesifik untuk platform komputer tertentu
- Cukup umum untuk semua sistem yang ada dan diusulkan
- Dapat diubah tanpa persetujuan Dewan Direksi

Contoh Standar Rinci

- Panjang password minimal 8 karakter
- Masa kadaluarsa password 30 hari
- Password terdiri dari minimal 2 karakter alfa dan 2 numerik

Contoh Standar Keamanan SI (Bagian 1)

Berikut adalah standar keamanan SI minimum yang telah disetujui manajemen senior:

Standar 1-3: Administrator Keamanan

- Password pertama diubah setelah instalasi awal
- Administrator keamanan cadangan harus ditunjuk dan dilatih
- Parameter password minimal 8 karakter alfa-numerik

Standar 4-6: Perlindungan Password Password

- Password tersamar pada layar saat dimasukkan
- File password dienkripsi dengan algoritma aman
- Password otomatis berakhir dalam 60 hari atau kurang

Standar 7-9: Kontrol Akses

- ID dibatalkan setelah 3 kali gagal login berturut-turut
- Sesi berakhir setelah 5 menit tanpa aktivitas
- Pengguna tidak boleh login pada sesi bersamaan

Contoh Standar Keamanan SI (Bagian 2)

1

Penghapusan ID Pengguna

Administrator keamanan harus menghapus ID pengguna yang dihentikan atau dialihkan segera setelah pemberitahuan dari manajer departemen dan/atau SDM

2

Pelatihan Pengguna

Manajer departemen bertanggung jawab melatih pengguna untuk tidak membagi password, menuliskannya, mempostingnya, atau menyimpannya dalam file elektronik

3

Review Kemampuan Akses

Administrator keamanan meminta manajemen departemen meninjau kemampuan akses pengguna dan menyatakan secara tertulis bahwa akses sesuai kebutuhan, setidaknya setiap tahun

4

Pencatatan Kejadian Keamanan

Kejadian keamanan logis dicatat dan dipantau terus-menerus oleh administrator keamanan untuk mendeteksi potensi akses tidak sah

Standar Keamanan SI: Backup dan Asuransi

Standar 14: Rencana Pemulihan Bisnis

Prosedur pemulihan bisnis harus sepenuhnya dikembangkan, diuji, dan didokumentasikan. Rencana harus mencakup:

- Backup sistem lengkap secara mingguan
- Backup data lengkap setiap hari
- Rotasi media cadangan ke fasilitas luar yang aman
- Siklus rotasi tiga generasi atau lebih

Standar 15: Cakupan Asuransi

Asuransi memadai harus mencakup:

- Perangkat keras dengan biaya penggantian
- Sistem operasi dan aplikasi dengan biaya penciptaan kembali
- Data dengan biaya penciptaan kembali
- Pendapatan yang hilang akibat kegagalan sistem

Standar Opsional Berdasarkan Risiko Risiko

Standar berikut bersifat opsional dan diterapkan jika dibenarkan oleh risiko dan jika sistem mampu:

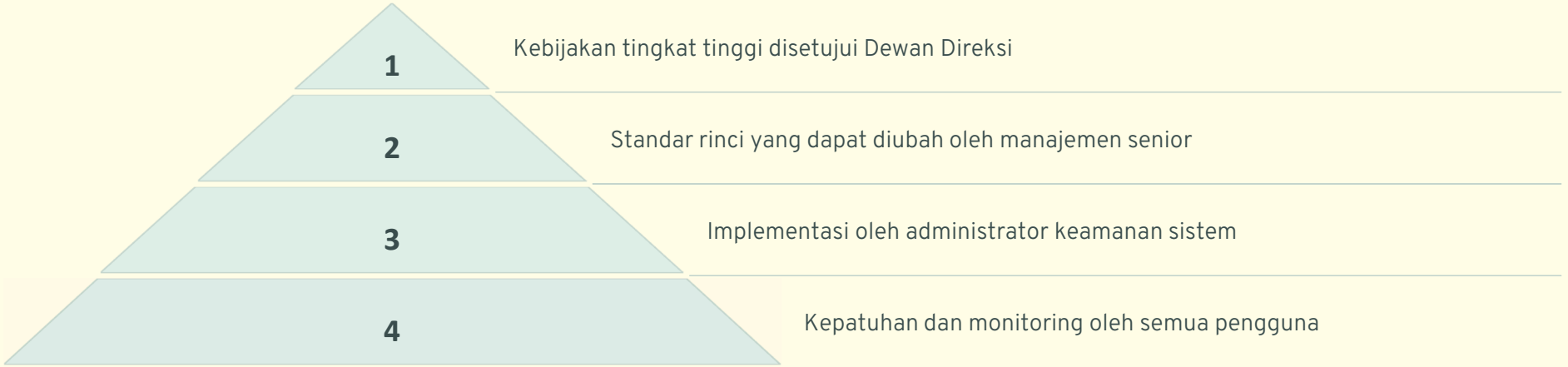
Standar 20: Pembatasan Waktu Akses

Akses pengguna dibatasi untuk jam dan hari kerja normal (misalnya 6 pagi hingga 6 sore, Senin sampai Jumat). Akses malam dan akhir pekan memerlukan persetujuan tertulis tambahan dari manajemen

Standar 21: Pembatasan Lokasi Akses

Akses pengguna dibatasi untuk tempat kerja tertentu yang diidentifikasi dengan nomor titik unik untuk meningkatkan keamanan dan kontrol

Kesimpulan: Pentingnya Kebijakan dan Standar Terintegrasi Terintegrasi



Kebijakan, standar dan pedoman keamanan sistem informasi harus dirancang bersama untuk memastikan kontinuitas dan konsistensi dalam aplikasi mereka untuk semua sistem informasi di seluruh perusahaan. Dokumen harus tersedia untuk semua karyawan, diperbarui setidaknya setahun sekali, dan dikomunikasikan secara teratur kepada seluruh staf.