# MAKALAH

# STANDAR KEAMANAN INFORMASI

## Mata Kuliah : Keamanan Data dan Informasi


DISUSUN OLEH

**Cindy Ramanda(230103003)**
**Dimas Wiranda(230103007)**
**Farah Audina(240103001)**
**Gema Yusuf Farhan(230103026)**
**Indah Riyadini Putri (230103017)**
**Lina Sulinawati (230103020)**
**Putri Raudah(230103028)**
**Tiara Pardila Putri Asmara(230103034)**

**PROGRAM STUDI TEKNIK INFORMATIKA**
**FAKULTAS ILMU KOMPUTER**
**UNIVERSITAS DUMAI**

**TP. 2025**

# KATA PENGANTAR

Puji syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa atas limpahan rahmat dan karunia-Nya sehingga makalah yang berjudul **"Standar Keamanan Informasi"** ini dapat diselesaikan dengan baik dan tepat waktu. Makalah ini disusun sebagai salah satu bentuk tugas dalam rangka memperdalam pemahaman mengenai pentingnya perlindungan informasi, terutama dalam menghadapi tantangan dunia digital yang terus berkembang.

Dalam penyusunan makalah ini, kami mengacu pada berbagai sumber terpercaya, baik dari buku, jurnal, maupun artikel ilmiah yang relevan dengan topik keamanan informasi. Kami juga berusaha menyusun isi makalah ini secara sistematis agar mudah dipahami oleh pembaca.

Kami menyadari bahwa penyusunan makalah ini masih jauh dari kata sempurna. Oleh karena itu, kami sangat mengharapkan kritik dan saran yang bersifat membangun untuk perbaikan di masa yang akan datang.

Akhir kata, semoga makalah ini dapat memberikan manfaat bagi pembaca dan dapat menambah wawasan khususnya dalam memahami standar keamanan informasi dan penerapannya di dunia nyata.

Dumai, 03 Juli 2025

Kelompok 3

# DAFTAR ISI

# BAB I

# PENDAHULUAN

## 1.1 Latar Belakang

Di era digital saat ini, informasi menjadi aset yang sangat penting bagi individu, organisasi, maupun perusahaan. Informasi yang bocor, rusak, atau tidak tersedia ketika dibutuhkan bisa menyebabkan kerugian besar. Oleh karena itu, perlindungan terhadap informasi sangat krusial dan perlu dilakukan secara sistematis. Salah satu cara untuk melindungi informasi adalah dengan menerapkan standar keamanan informasi. Standar ini dirancang untuk mengatur dan mengontrol bagaimana informasi disimpan, diakses, dan dijaga keamanannya agar tidak disalahgunakan.

## 1.2 Rumusan Masalah

1. Apa yang dimaksud dengan keamanan informasi?
2. Apa saja standar keamanan informasi yang ada?
3. Bagaimana implementasi standar keamanan informasi dalam organisasi?

## 1.3 Tujuan Penulisan

1. Menjelaskan pengertian keamanan informasi.
2. Mengidentifikasi berbagai standar keamanan informasi yang umum digunakan.
3. Menjelaskan cara penerapan standar keamanan informasi dalam organisasi.

## 1.4 Manfaat Penulisan

Makalah ini diharapkan dapat memberikan pemahaman yang lebih luas tentang pentingnya standar keamanan informasi, membantu pembaca mengenal jenis-jenis standar yang ada, serta mendorong kesadaran akan perlunya perlindungan data dalam berbagai aktivitas, khususnya di era digital saat ini.

# BAB II

# TINJAUAN PUSTAKA

## 2.1 Pengertian Keamanan Informasi

Keamanan informasi adalah praktik yang bertujuan untuk melindungi informasi dari berbagai ancaman seperti akses yang tidak sah, penggunaan yang tidak semestinya, pengungkapan, gangguan, perubahan, atau perusakan. Tujuan utamanya adalah menjaga agar informasi tetap terlindungi dari sisi kerahasiaan, integritas, dan ketersediaannya, baik dalam bentuk digital maupun non-digital.

## 2.2 Tujuan dan Ruang Lingkup Keamanan Informasi

Tujuan utama dari keamanan informasi adalah untuk menjaga tiga aspek utama yang dikenal sebagai CIA Triad:

- Kerahasiaan (Confidentiality): Menjamin bahwa informasi hanya diakses oleh pihak yang memiliki otoritas.
- Integritas (Integrity): Memastikan bahwa informasi tetap akurat, utuh, dan tidak diubah oleh pihak yang tidak berwenang.
- Ketersediaan (Availability): Menjaga agar informasi dapat diakses kapan saja oleh pengguna yang berwenang ketika dibutuhkan.

Ruang lingkup keamanan informasi mencakup seluruh siklus hidup data, mulai dari penciptaan, penyimpanan, penggunaan, hingga pemusnahan informasi.

## 2.3 Ancaman dan Risiko terhadap Informasi

Beberapa ancaman dan risiko yang umum terhadap keamanan informasi meliputi:

- Serangan siber: seperti peretasan (hacking), virus, malware, ransomware, dan phishing yang dapat mencuri atau merusak data.

- Kesalahan manusia: seperti kelalaian dalam mengatur hak akses, salah mengirim file, atau penggunaan kata sandi yang lemah.
- Kegagalan sistem: termasuk kerusakan perangkat keras, kegagalan perangkat lunak, atau gangguan jaringan.

Bencana alam: seperti gempa bumi, banjir, atau kebakaran yang dapat menyebabkan hilangnya data atau kerusakan infrastruktur informasi.

## 2.4 Standar Keamanan Informasi

Standar keamanan informasi adalah seperangkat pedoman, kebijakan, dan praktik terbaik yang dirancang untuk melindungi informasi dari ancaman dan risiko. Standar ini membantu organisasi dalam mengelola keamanan data secara sistematis dan profesional. Beberapa standar yang umum digunakan antara lain:

- ISO/IEC 27001: Standar internasional untuk sistem manajemen keamanan informasi (ISMS).
- NIST: Kerangka kerja yang dikembangkan di Amerika Serikat untuk mengelola risiko keamanan informasi.
- COBIT: Framework yang digunakan untuk tata kelola dan manajemen teknologi informasi.
- ITIL: Berfokus pada manajemen layanan TI, termasuk pengelolaan keamanan informasi.

Dengan memahami standar-standar ini, organisasi dapat menyusun kebijakan, prosedur, dan kontrol yang sesuai untuk menjaga informasi tetap aman dan terpercaya.

# BAB III

# STANDAR KEAMANAN INFORMASI

## 3.1 Pengertian Standar Keamanan Informasi

Standar keamanan informasi adalah seperangkat kebijakan, prosedur, dan pedoman teknis yang dirancang untuk membantu organisasi menjaga keamanan informasi dari berbagai ancaman. Standar ini memberikan kerangka kerja yang sistematis dalam mengelola risiko, mengatur akses, serta menjaga kerahasiaan, integritas, dan ketersediaan data.

## 3.2 Jenis-Jenis Standar Keamanan Informasi

### 1.4.1 ISO/IEC 27001

ISO/IEC 27001 merupakan standar internasional yang paling dikenal dalam sistem manajemen keamanan informasi (ISMS). Standar ini menyediakan kerangka kerja untuk mengelola keamanan informasi secara berkelanjutan, termasuk pengelolaan risiko, kontrol keamanan, audit, dan peningkatan sistem. Sertifikasi ISO 27001 juga sering menjadi syarat kepercayaan dalam kerja sama antar perusahaan.

### 1.4.2 NIST (National Institute of Standards and Technology)

NIST adalah badan standar asal Amerika Serikat yang merilis berbagai pedoman keamanan informasi. Salah satu yang terkenal adalah NIST Cybersecurity Framework, yang membantu organisasi mengidentifikasi, melindungi, mendeteksi, merespons, dan memulihkan aset informasi dari ancaman.

### 1.4.3 COBIT (Control Objectives for Information and Related Technology)

COBIT adalah kerangka kerja untuk tata kelola dan manajemen TI yang mencakup kontrol terhadap keamanan informasi. COBIT banyak digunakan oleh

organisasi yang ingin memastikan bahwa TI mendukung tujuan bisnis secara optimal dan aman.

### 1.4.4 ITIL (Information Technology Infrastructure Library)

ITIL adalah kumpulan praktik terbaik dalam manajemen layanan TI. Meskipun tidak secara spesifik berfokus pada keamanan informasi, ITIL mencakup aspek-aspek pengelolaan insiden, manajemen risiko, dan ketersediaan layanan yang mendukung keamanan sistem secara keseluruhan.

## 3.3 Penerapan ISO/IEC 27001 dalam Organisasi

Implementasi ISO/IEC 27001 dalam organisasi umumnya melalui tahapan:

- Menyusun kebijakan keamanan informasi
- Mengidentifikasi aset dan risiko
- Menentukan kontrol dan tindakan mitigasi
- Menerapkan sistem dan prosedur keamanan
- Melakukan audit internal dan evaluasi berkala
- Menerapkan perbaikan berkelanjutan

Penerapan ini dapat membantu organisasi mencegah pelanggaran data, meningkatkan kepercayaan pelanggan, dan memenuhi persyaratan hukum.

## 3.4 Contoh Implementasi Standar

Sebagai contoh, perusahaan perbankan menerapkan ISO 27001 untuk memastikan data nasabah tersimpan secara aman, terutama dalam sistem digital yang terhubung dengan layanan online. Perusahaan e-commerce juga menggunakan standar keamanan seperti NIST atau ISO untuk melindungi data transaksi pelanggan dan menjaga reputasi bisnis.

# BAB IV

# PEMBAHASAN DAN ANALISIS

## 4.1 Perbandingan Antar Standar Keamanan Informasi

Setiap standar keamanan informasi memiliki fokus dan keunggulan yang berbeda, tergantung pada kebutuhan dan karakter organisasi. Berikut perbandingan singkat antara standar yang umum digunakan:

- **ISO/IEC 27001** merupakan standar internasional yang fokus pada sistem manajemen keamanan informasi. Kelebihannya adalah cocok untuk semua jenis organisasi karena bersifat umum dan terstruktur. Namun, proses sertifikasinya cukup kompleks dan membutuhkan biaya serta waktu yang tidak sedikit.
- **NIST** adalah kerangka kerja keamanan informasi yang dikembangkan di Amerika Serikat. Standar ini sangat teknis dan detail, serta tersedia secara gratis, sehingga banyak digunakan oleh instansi pemerintahan maupun sektor swasta. Meskipun begitu, implementasinya bisa terasa rumit, terutama untuk organisasi kecil atau yang belum memiliki infrastruktur TI yang matang.
- **COBIT** lebih fokus pada tata kelola dan kontrol internal di bidang teknologi informasi. Kelebihan COBIT adalah kemampuannya menyelaraskan antara TI dan tujuan bisnis organisasi. Namun, jika dibandingkan dengan NIST atau ISO, COBIT kurang detail dalam aspek teknis keamanan informasi.
- **ITIL** berfokus pada manajemen layanan TI secara menyeluruh. Standar ini mendukung keamanan informasi dari sisi operasional dan pengelolaan insiden. Kelemahannya, ITIL tidak secara khusus membahas keamanan informasi secara mendalam seperti standar lainnya.

## 4.2 Tantangan dalam Implementasi Standar Keamanan

Meskipun bermanfaat, penerapan standar keamanan informasi menghadapi beberapa tantangan, antara lain:

- Biaya dan waktu implementasi: Standar seperti ISO/IEC 27001 membutuhkan audit, dokumentasi, dan pelatihan yang menyita sumber daya.
- Kurangnya kesadaran dan komitmen: Tidak semua karyawan atau manajemen memahami pentingnya keamanan informasi.
- Kesulitan teknis: Implementasi kontrol teknis bisa kompleks jika organisasi belum memiliki infrastruktur TI yang matang.
- Kekurangan SDM yang kompeten: Diperlukan tenaga ahli yang memahami standar serta cara mengelolanya.

### 4.3 Solusi dan Strategi Penerapan

Untuk mengatasi tantangan di atas, organisasi dapat mengambil langkah-langkah berikut:

- Pelatihan dan sosialisasi rutin untuk seluruh karyawan terkait keamanan informasi.
- Penerapan secara bertahap, dimulai dari identifikasi risiko dan kebijakan dasar keamanan.
- Menggunakan jasa konsultan atau pihak ketiga untuk mendampingi proses sertifikasi dan implementasi.
- Melibatkan manajemen puncak dalam setiap tahap penerapan agar kebijakan berjalan efektif.

### 4.4 Dampak Penerapan Standar Keamanan Informasi

Penerapan standar keamanan informasi membawa berbagai dampak positif, seperti:

- Meningkatkan kepercayaan pengguna atau pelanggan terhadap organisasi.
- Mengurangi risiko kebocoran dan kehilangan data.
- Meningkatkan efisiensi dan kontrol internal.
- Memenuhi kewajiban hukum dan regulasi, seperti UU Perlindungan Data Pribadi (PDP) atau GDPR.
- Menjadi keunggulan kompetitif, terutama untuk perusahaan yang bergerak di bidang layanan digital.

# BAB V

# PENUTUP

## 5.1 Kesimpulan

Keamanan informasi merupakan aspek yang sangat penting dalam menghadapi perkembangan teknologi digital saat ini. Perlindungan terhadap informasi tidak hanya menjadi kebutuhan teknis, tetapi juga menjadi bagian dari tanggung jawab organisasi dalam menjaga kepercayaan dan integritas data. Berbagai standar keamanan informasi seperti ISO/IEC 27001, NIST, COBIT, dan ITIL telah dikembangkan untuk memberikan pedoman dan kerangka kerja dalam mengelola risiko dan melindungi informasi dari ancaman.

Masing-masing standar memiliki keunggulan dan kelemahannya sendiri, tergantung pada kebutuhan dan skala organisasi. Penerapan standar ini, meskipun menantang, terbukti mampu meningkatkan perlindungan data, efisiensi pengelolaan sistem, serta kepatuhan terhadap regulasi.

## 5.2 Saran

Organisasi disarankan untuk mulai menerapkan standar keamanan informasi secara bertahap, dimulai dari pemetaan risiko dan penyusunan kebijakan dasar keamanan. Pelatihan dan peningkatan kesadaran karyawan juga perlu dilakukan secara rutin agar keamanan informasi menjadi bagian dari budaya kerja. Selain itu, dukungan dari manajemen puncak sangat penting agar implementasi dapat berjalan dengan efektif dan berkelanjutan.

# DAFTAR PUSTAKA

ISO. (2013). ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements. International Organization for Standardization.

NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity Version 1.1. National Institute of Standards and Technology. Retrieved from https://www.nist.gov

ISACA. (2012). COBIT 5: A Business Framework for the Governance and Management of Enterprise IT. ISACA.

Axelos. (2019). ITIL Foundation: ITIL 4 Edition. TSO (The Stationery Office), United Kingdom.

Setiawan, D. (2020). Keamanan Sistem Informasi. Yogyakarta: Andi Offset.

Siregar, R. (2021). Manajemen Keamanan Informasi. Bandung: Informatika.