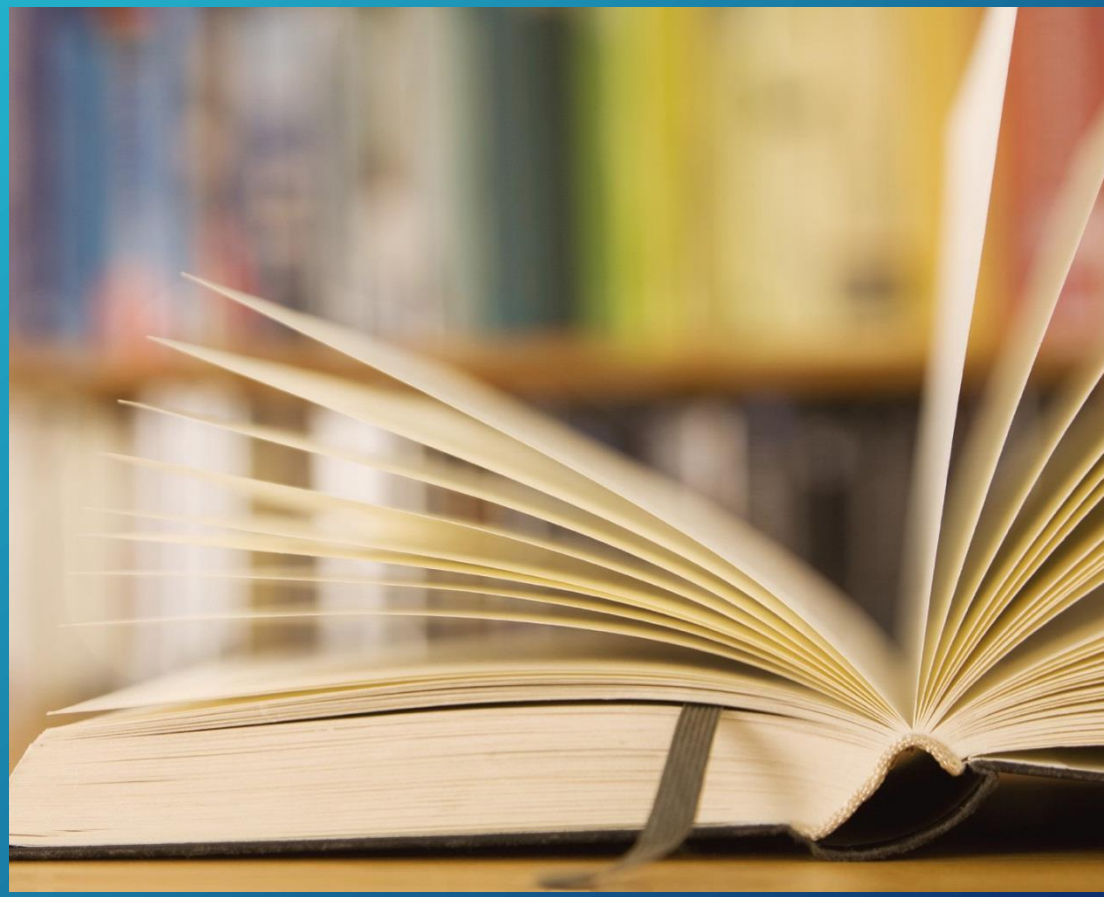
SEKOLAH TINGGI TEKNOLOGI
TERPADU NURUL FIKRI
CHARACTER BUILDING CAMPUS
STT - NF

KEBIJAKAN DAN TANGGUNG JAWAB KEAMANAN KOMPUTER

Keamanan Sistem Informasi – Aditya Putra, ST., MT.



Agenda

Mahasiswa diharapkan dapat memahami

- Kebijakan Keamanan Informasi
- Urgensi dari Aturan Keamanan Informasi
- Hirarki Aturan Keamanan Informasi
- Beberapa Aturan Keamanan Informasi di Level Organisasi
  - Password Policy
  - Email Security Policy
  - Data Classification
- Pelatihan Kesadaaran Aturan Keamanan
- Apa aturan yang umum berlaku terkait keamanan informasi

Kebijakan Keamanan Informasi

Kebijakan Keamanan Informasi adalah kumpulan rencana, proses, prosedur, standar dan pedoman yang dibutuhkan untuk membangun lingkungan keamanan informasi yang ideal bagi organisasi

Kebijakan adalah hal yang wajib dalam manajemen keamanan informasi

Kebutuhan Kebijakan Keamanan Informasi:

- Menjamin penerapan prinsip keamanan yang konsisten
- Membatasi keterbukaan data internal terhadap ancaman eksternal
- Untuk menekankan komitmen manajemen dalam menciptakan lingkungan yang aman
- Menyediakan perlindungan hukum
- Memberikan respon insiden secara tanggap
- Menurunkan dampak insiden
- Meminimalisir kebocoran data
- Meningkatkan keamanan data dan jaringan

Hirarki Kebijakan Keamanan Informasi

Hukum	Aturan tertinggi yang diikuti semua orang
Regulasi	Kumpulan pedoman yang disahkan oleh Hukum
Kebijakan	Aturan legal dan bersifat internal yang mengatur tentang keamanan informasi
Standar	Nilai-nilai yang disusun untuk memastikan kebijakan diikuti dan tidak dilanggar
Prosedur, Pedoman	Prosedur: aturan teknis step-by-step Pedoman: saran-saran untuk menjaga keamanan

Password dan Email Security Policy

- Aturan Password menyediakan rangkaian aturan untuk menggunakan password yang kuat pada asset informasi organisasi
- Konsideran dalam mendesain aturan Password:
  - Panjang dan formasi
  - Kompleksitas
  - Blacklist Password
  - Kapan Password harus diganti

- Aturan Email mengatur penggunaan email organisasi yang seharusnya
- Konsideran dalam mendesain aturan keamanan Email :
  - Tentukan peruntukan email organisasi, terlebih jika diizinkan untuk penggunaan personal
  - Pengguna email harus diberitahu bahwa emailnya direview atau disimpan
  - Tipe email apa saja yang perlu disimpan dan untuk berapa lama
  - Kapan harus mengencrypt email
  - Konsekuensi dari pelanggaran aturan keamanan email

Data Classification Policy

- Aturan Klasifikasi Data adalah sebuah framework untuk mengklasifikasikan seluruh data organisasi berdasarkan level sensitivitasnya, nilai, dan seberapa penting data tersebut dalam domain aturan keamanan informasi organisasi

- Pada umumnya data organisasi diklasifikasikan menjadi tiga kategori:
  - Restricted / Classified → Hanya bisa dibuka oleh kalangan yang sangat terbatas
  - Private → Hanya untuk kalangan internal organisasi
  - Public → Bisa dibuka kepada masyarakat luas

- 5 Langkah Efektif Klasifikasi Data
  - Identifikasi → Daftarkan semua asset informasi
  - Temukan Lokasi dan Akesibilitas
  - Klasifikasi → Data Labelling
  - Amankan secara teknis → by technology
  - Monitoring, Evaluasi, dan Reimplementasi

Pelatihan Kesadaran Keamanan Informasi

- Pelatihan Keamanan Informasi mengajarkan pada peserta/pegawai bagaimana melakukan tugasnya agar sesuai dengan ketentuan aturan keamanan
- Pelatihan diperlukan sebagai syarat sebelum seseorang diberikan akses ke dalam jaringan organisasi

Pentingnya Pelatihan

- Implementasi aturan keamanan menjadi lebih efektif
- Peserta yang mengerti manfaat aturan akan lebih mudah menjalankan sehingga tidak merasa dipaksa
- Membangun kesadaran pada isu keamanan terkait
- Membantu organisasi untuk meningkatkan keamanan jaringan informasinya

ISO/IEC 27001:2013 ISMS

ISO/IEC 27001:2013 adalah standar keamanan yang telah digunakan secara internasional dan merupakan *best practice* untuk Sistem Manajemen Keamanan Informasi (ISMS)

ISO 27001 merinci persyaratan untuk membangun, mengimplementasikan, merawat, dan mengembangkan ISMS pada sebuah organisasi

ISO 27001 dibagi menjadi 10 chapter:

1. Scope of the Standard
2. Document Reference
3. Term dan Definitions
4. Organizational Context
5. Leadership Support to the ISMS
6. Planning an ISMS
7. Required Support for an ISMS
8. Operating ISMS
9. Evaluation
10. Further Improvement

ISO/IEC 27001:2013

Terdapat total 114 Kontrol Annex A yang dibagi menjadi 14 Kategori

- A.5 – Information Security Policies (2 Control)
- A.6 – Organisation of Information Security (7 Controls)
- A.7 - Human resource security (6 controls)
- A.8 - Asset management (10 controls)
- A.9 – Access control (14 controls)
- A.10 – Cryptography (2 controls)
- A.11 – Physical and environmental security (15 controls)

ISO/IEC 27001:2013

Terdapat total 114 Kontrol Annex A yang dibagi menjadi 14 Kategori (lanjutan)

- A.12 - Operations security (14 controls)
- A.13 – Communications security (7 controls)
- A.14 – System acquisition, development and maintenance (13 controls)
- A.15 – Supplier relationships (5 controls)
- A.16 - Information security incident management (7 controls)
- A.17 – Information security aspects of business continuity management (4 controls)
- A.18 - Compliance (8 controls)

PCI-DSS

- **Payment Card Industry Data Security Standard (PCI-DSS)** adalah standar keamanan informasi yang diperuntukann bagi perusahaan yang mengelola informasi pemegang kartu transaksi seperti Kartu Debit, Kredit, e-Money, dll
- Aturan **PCI-DSS** berlaku untuk semua stakeholder yang terlibat dengan penggunaan kartu transaksi tersebut termasuk, pemilik toko, penerbit, penyedia layanan, dan entitas lain yang terlibat dalam menyimpan, memproses dan metransmisikan data pemilik kartu
- Requirement **PCI-DSS** dikembangkan dan dievaluasi oleh Payment Card Industry (PCI) Security Standard Council

HIPAA

Health Insurance Portability and Accountability Act (HIPAA) adalah legislasi AS yang menyediakan privasi data dan ketentuan keamanan untuk menjaga informasi Kesehatan.

Legislasi ini menjadi semakin penting untuk dibuat dengan semakin banyaknya serangan siber dan ransomware yang menyerang rumah sakit dan institusi Kesehatan lainnnya

Ada 2 tujuan HIPAA yaitu menyediakan asuransi Kesehatan bagi pekerja yang kehilangan atau ganti pekerjaan dan mengurangi biaya Kesehatan dengan melakukan standarisasi transmisi elektronik untuk administrasi dan transaksi elektronik

5 Komponen utama HIPAA

- Title I: HIPAA Health Insurance reform

  Proteksi asuransi pribadi bagi warga yang pindah atau kehilangan pekerjaan

- Title II: HIPAA Administrative Simplification

  Pembuatan standar nasional untuk pemrosesan transaksi Kesehatan elektronik. Pada komponen ini juga meminta penyedia layanan Kesehatan untuk menggunakan akses elektronik yang aman terhadap data Kesehatan dan tetap *comply* dengan regulasi privasi yang diatur oleh Departemen Kesehatan AS

- Title III: HIPAA Tax-Related Healtd Provision

  Ketentuan dan Pedoman Kesehatan yang terkait dengan pajak

- Title IV: Application and Enforcement of Group Health Plan Requirements

  Reformasi Asuransi Kesehatan

- Title V: Revenue Offset

  Ketentuan terhadap asuransi jiwa yang dimiliki oleh perusahaan dan penanganan terhadap warga yang kehilangan kewarganegaraannya