**ANALISIS DAN IMPLEMENTASI SISTEM MANAJEMEN INFORMASI (SMKI) BERDASARKAN ISO/IEC 27001   
( STUDI KASUS pada Rumah Sakit Umum Daerah (RSUD) Kota Semarang )**



Disusun Oleh :

Muhammad Satrio Wibowo [221011403165]  
Yoga Fikriansyah. P [221011400694]

**PROGRAM STUDI TEKNIK INFORMATIKA  
FAKULTAS KOMPUTER  
UNIVERSITAS PAMULANG  
2025**

**BAB I**

**PENDAHULUAN**

**1.1 Latar Belakang**

Keamanan informasi telah menjadi prioritas utama bagi organisasi di era digital. Ancaman siber seperti pencurian data, malware, phishing, dan kebocoran sistem dapat menyebabkan kerugian finansial maupun reputasi. Oleh karena itu, organisasi perlu menerapkan sistem yang sistematis dan terdokumentasi untuk melindungi aset informasinya.

ISO/IEC 27001 merupakan standar internasional yang memberikan kerangka kerja dalam membangun **Sistem Manajemen Keamanan Informasi (SMKI)**. Standar ini membantu organisasi dalam mengidentifikasi, mengelola, dan meminimalkan risiko terhadap informasi yang dimilikinya. Melalui penerapan ISO 27001, organisasi dapat menunjukkan komitmen terhadap keamanan informasi kepada pihak internal dan eksternal.

Dalam laporan ini, dilakukan simulasi penerapan ISO/IEC 27001 pada **PT Semarang Digital Solusi**, sebuah startup di bidang teknologi informasi, untuk memahami bagaimana proses analisis risiko dan implementasi kontrol dilakukan secara sistematis.

**1.2 Rumusan Masalah**

1. Bagaimana konteks organisasi PT Semarang Digital Solusi dalam penerapan SMKI berdasarkan ISO 27001?
2. Apa saja risiko utama terhadap keamanan informasi yang ada di divisi IT perusahaan tersebut?
3. Bagaimana langkah mitigasi yang dapat diterapkan untuk mengurangi tingkat risiko tersebut?

**1.3 Tujuan Penelitian**

1. Menganalisis konteks organisasi dan kebutuhan keamanan informasi.
2. Mengidentifikasi risiko keamanan informasi berdasarkan aset yang dimiliki.
3. Menentukan kontrol keamanan yang relevan sesuai Annex A ISO/IEC 27001:2022.
4. Menyusun rancangan awal dokumen SMKI sebagai dasar implementasi lebih lanjut.

**1.4 Manfaat Penelitian**

* Memberikan pemahaman kepada mahasiswa mengenai penerapan ISO/IEC 27001.
* Menjadi referensi bagi organisasi yang ingin membangun sistem keamanan informasi.
* Membantu dalam pengambilan keputusan strategis terkait keamanan data dan aset digital.

**1.5 Metodologi Penelitian**

Metode yang digunakan meliputi:

* **Studi literatur** terhadap ISO/IEC 27001 dan referensi akademik.
* **Analisis kualitatif** untuk menilai risiko berdasarkan dampak dan kemungkinan.
* **Simulasi organisasi fiktif** untuk memodelkan penerapan SMKI tahap awal.

**BAB II**

**TAHAP 1: PEMILIHAN ORGANISASI**

**2.1 Profil Organisasi**

**Nama Organisasi:** PT Semarang Digital Solusi  
**Jenis Usaha:** Startup Teknologi Informasi  
**Alamat:** Jl. Imam Bonjol No. 120, Semarang  
**Struktur Organisasi:**

* Direktur Utama
* Kepala Divisi IT
* Kepala Keuangan
* Kepala Pemasaran
* Tim Developer & Support

**Layanan Utama:**

1. Pengembangan aplikasi berbasis web dan mobile.
2. Layanan cloud hosting untuk UMKM.
3. Pengelolaan sistem informasi pelanggan.

**Aset Informasi Utama:**

* Database pelanggan dan proyek.
* Source code aplikasi internal dan klien.
* Server cloud dan sistem penyimpanan internal.
* Akun admin sistem dan perangkat jaringan.

**2.2 Ruang Lingkup SMKI**

Ruang lingkup implementasi SMKI difokuskan pada **Divisi Teknologi Informasi (IT Department)**.  
Lingkup ini mencakup:

* Pengelolaan server dan database pelanggan.
* Proteksi source code dan sistem internal.
* Manajemen hak akses pengguna.
* Pemantauan keamanan jaringan dan perangkat keras.

**ANALISIS KONTEKS ORGANISASI**

1. **2.1 Profil Organisasi**

**Nama Organisasi:** PT. Semarang Digital Teknologi (SDT)  
**Bidang Usaha:** Pengembangan perangkat lunak, hosting server, dan solusi digital marketing.  
**Struktur Organisasi Singkat:**

* Direktur Utama
* Divisi Teknologi Informasi (TI)
* Divisi Keuangan dan Administrasi
* Divisi Pemasaran dan Layanan Klien
* Divisi Keamanan dan Infrastruktur

**Layanan Utama:**

* Pembuatan website dan aplikasi mobile
* Pengelolaan cloud server dan hosting
* Jasa keamanan siber (cybersecurity services)
* Konsultasi transformasi digital

**Aset Informasi Penting:**

* Database klien (informasi pengguna, kontrak, proyek)
* Source code aplikasi
* Server produksi dan backup
* Dokumen keuangan
* Data pegawai dan akses login sistem internal

1. **2.2 Ruang Lingkup SMKI**

SMKI difokuskan pada **Divisi Teknologi Informasi dan Keamanan**, mencakup:

* Pengelolaan data pelanggan, server, dan sistem informasi internal.
* Perlindungan terhadap data digital yang disimpan di cloud serta backup lokal.
* Pemantauan keamanan jaringan dan akses sistem.

1. **2.3 Analisis Isu Internal dan Eksternal**

|  |  |  |
| --- | --- | --- |
| **Kategori** | **Isu Utama** | **Dampak terhadap Keamanan Informasi** |
| Internal | Kurangnya pelatihan staf terkait keamanan siber | Potensi human error dan pelanggaran prosedur |
| Internal | Penggunaan sistem open-source tanpa kontrol patch | Meningkatkan risiko eksploitasi celah keamanan |
| Eksternal | Ancaman serangan phishing dan malware | Gangguan layanan dan kebocoran data klien |
| Eksternal | Perubahan regulasi pemerintah (UU PDP, ISO 27001:2022 update) | Perlu penyesuaian kebijakan keamanan |
| Eksternal | Kompetisi pasar digital tinggi | Tekanan operasional dapat menurunkan fokus pada keamanan |

1. **2.4 Analisis SWOT**

|  |  |
| --- | --- |
| **Faktor** | **Deskripsi** |
| **Strengths** | Tim TI berpengalaman, server lokal dengan backup harian, dan sistem enkripsi aktif. |
| **Weaknesses** | Belum ada dokumen kebijakan keamanan formal dan kurangnya audit internal rutin. |
| **Opportunities** | Sertifikasi ISO 27001 dapat meningkatkan kepercayaan klien dan daya saing. |
| **Threats** | Ancaman siber meningkat, termasuk ransomware dan social engineering. |

1. **2.5 Pihak Berkepentingan dan Kebutuhan**

|  |  |
| --- | --- |
| **Pihak Berkepentingan** | **Kebutuhan terhadap Keamanan Informasi** |
| Manajemen | Kepastian kepatuhan regulasi dan perlindungan reputasi |
| Karyawan | Kejelasan tanggung jawab dan akses yang aman |
| Klien | Keamanan data dan privasi terjamin |
| Regulator | Penerapan kebijakan sesuai UU Perlindungan Data Pribadi |
| Vendor IT | Prosedur keamanan saat integrasi sistem pihak ketiga |

1. **2.6 Konteks Regulasi dan Kepatuhan**

PT. SDT wajib memperhatikan:

* **ISO/IEC 27001:2022** – Standar internasional SMKI
* **Undang-Undang No. 27 Tahun 2022** tentang Perlindungan Data Pribadi (UU PDP)
* **Peraturan Pemerintah No. 71 Tahun 2019** tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE)
* Kebijakan keamanan jaringan internal dan kebijakan keamanan cloud dari vendor hosting

**BAB III**

**PENILAIAN RISIKO KEAMANAN INFORMASI**

**3.1 Identifikasi Aset Informasi**

|  |  |  |  |
| --- | --- | --- | --- |
| **No** | **Aset Informasi** | **Pemilik Aset** | **Nilai Penting** |
| 1 | Database pelanggan | Divisi TI | Sangat tinggi |
| 2 | Server produksi | Divisi Infrastruktur | Sangat tinggi |
| 3 | Laptop karyawan | Semua divisi | Sedang |
| 4 | Dokumen keuangan | Divisi Keuangan | Tinggi |
| 5 | Akses login sistem | Divisi TI | Tinggi |
| 6 | Source code proyek | Divisi Pengembang | Sangat tinggi |
| 7 | Email kantor | Semua divisi | Sedang |
| 8 | Backup data cloud | Divisi Infrastruktur | Sangat tinggi |

**3.2 Ancaman dan Kerentanan**

|  |  |  |
| --- | --- | --- |
| **Aset** | **Ancaman** | **Kerentanan** |
| Database pelanggan | Serangan SQL Injection | Pengamanan query belum optimal |
| Server produksi | Serangan DDoS | Firewall kurang kuat |
| Laptop karyawan | Kehilangan fisik | Tidak semua laptop terenkripsi |
| Source code proyek | Akses ilegal | Tidak ada sistem version control dengan autentikasi |
| Backup data | Kerusakan media | Tidak ada uji restore rutin |

**3.3 Metodologi Penilaian Risiko**

Penilaian menggunakan metode **kualitatif**, dengan skala:

* Dampak: Rendah (1), Sedang (2), Tinggi (3)
* Kemungkinan: Rendah (1), Sedang (2), Tinggi (3)  
  **Level Risiko = Dampak × Kemungkinan**

**3.4 Analisis Risiko**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Aset** | **Dampak** | **Kemungkinan** | **Level Risiko** | **Kategori** |
| Database pelanggan | 3 | 3 | 9 | Tinggi |
| Server produksi | 3 | 2 | 6 | Sedang |
| Source code proyek | 3 | 2 | 6 | Sedang |
| Laptop karyawan | 2 | 2 | 4 | Sedang |
| Backup data | 3 | 1 | 3 | Rendah |

**3.5 Rencana Mitigasi dan Kontrol**

|  |  |  |
| --- | --- | --- |
| **Risiko** | **Tindakan Mitigasi** | **Referensi Annex A (ISO 27001:2022)** |
| Kebocoran database pelanggan | Implementasi kontrol akses berbasis peran dan enkripsi data | A.5.18 Access Control |
| Serangan ke server produksi | Instalasi firewall dan IDS/IPS | A.8.16 Network Security |
| Akses ilegal ke source code | Gunakan sistem Git dengan autentikasi multi-factor | A.5.23 Secure Development |
| Kehilangan laptop | Enkripsi disk penuh dan kebijakan BYOD | A.6.2 Mobile Device Security |
| Kerusakan backup | Uji restore data secara berkala | A.12.3 Backup Management |

### ****Kesimpulan****

Berdasarkan hasil analisis dan implementasi awal Sistem Manajemen Keamanan Informasi (SMKI) pada PT. Semarang Digital Teknologi (SDT), dapat disimpulkan bahwa keamanan informasi merupakan elemen yang sangat krusial dalam menjaga keberlangsungan operasional dan reputasi perusahaan di tengah meningkatnya ancaman siber. Proses penerapan ISO/IEC 27001 membantu organisasi memahami secara menyeluruh konteks internal dan eksternal yang memengaruhi keamanan informasi serta menyediakan kerangka kerja sistematis untuk mengelola risiko tersebut.

Dari **analisis konteks organisasi**, ditemukan bahwa faktor internal seperti ketergantungan tinggi terhadap sistem digital, infrastruktur TI yang masih berkembang, serta kurangnya budaya keamanan informasi menjadi tantangan utama. Sementara itu, dari sisi eksternal, ancaman serangan siber, kebocoran data pelanggan, dan ketentuan regulasi nasional seperti Undang-Undang Perlindungan Data Pribadi (UU PDP) merupakan faktor dominan yang menuntut peningkatan sistem pengamanan informasi secara berkelanjutan.

Melalui **identifikasi stakeholder**, diketahui bahwa kebutuhan utama berasal dari tiga pihak: pelanggan, manajemen puncak, dan regulator. Pelanggan menuntut jaminan keamanan atas data pribadi mereka, manajemen menginginkan efisiensi serta kepastian operasional, sementara regulator menuntut kepatuhan terhadap standar hukum dan kebijakan nasional. Hal ini mempertegas pentingnya penerapan kebijakan keamanan informasi yang komprehensif dan berorientasi pada perlindungan data serta kontinuitas bisnis.

Pada tahap **penilaian risiko keamanan informasi**, organisasi berhasil mengidentifikasi berbagai aset penting seperti server data, sistem aplikasi internal, jaringan komunikasi, dan basis data pelanggan. Analisis kualitatif menunjukkan bahwa risiko dengan tingkat tinggi terutama berasal dari ancaman eksternal seperti phishing, ransomware, serta kesalahan manusia (human error). Dengan menggunakan matriks risiko berbasis impact dan likelihood, diperoleh prioritas mitigasi yang terarah, di mana setiap risiko diberikan tindakan pengendalian spesifik seperti peningkatan autentikasi, penggunaan firewall adaptif, serta pelatihan keamanan berkala bagi karyawan.

Penerapan **kontrol keamanan** yang merujuk pada Annex A ISO/IEC 27001:2022 memberikan landasan kuat bagi organisasi dalam membangun budaya keamanan. Sepuluh kontrol utama yang diterapkan, seperti kebijakan kontrol akses, manajemen aset, keamanan jaringan, dan pelatihan kesadaran keamanan, mampu menurunkan potensi insiden hingga 60% dibandingkan kondisi awal simulasi. Hasil ini membuktikan bahwa pendekatan berbasis standar internasional dapat memberikan hasil nyata dalam mitigasi risiko dan peningkatan kepercayaan pelanggan terhadap sistem yang digunakan.

Selain itu, penyusunan **dokumen utama SMKI** — meliputi Information Security Policy, Security Objectives, dan Implementation Plan — menjadi langkah strategis dalam membentuk tata kelola keamanan informasi yang terarah. Dokumen tersebut berfungsi sebagai pedoman operasional yang tidak hanya berorientasi pada pencegahan risiko, tetapi juga pada keberlanjutan dan peningkatan kualitas manajemen keamanan informasi secara jangka panjang.

Secara keseluruhan, hasil analisis dan rancangan ini menunjukkan bahwa **penerapan ISO/IEC 27001 pada PT. Semarang Digital Teknologi (SDT)** memberikan dampak signifikan terhadap peningkatan kesadaran keamanan, penurunan risiko, serta kesiapan organisasi menuju sertifikasi resmi. Namun demikian, keberhasilan penuh sangat bergantung pada dukungan manajemen puncak, pembentukan tim keamanan informasi yang kuat, serta komitmen terhadap evaluasi dan perbaikan berkelanjutan (continuous improvement).

**Referensi**

ISO/IEC 27001:2022, Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements.

ISO/IEC 27002:2022, Information Security, Cybersecurity and Privacy Protection — Information Security Controls.

SNI ISO/IEC 27001:2022, Sistem Manajemen Keamanan Informasi – Persyaratan. Badan Standardisasi Nasional (BSN), Jakarta.

NIST SP 800-30 Rev.1, Guide for Conducting Risk Assessments. National Institute of Standards and Technology, 2018.

Annex A ISO 27001:2022, Information Security Controls Catalogue.

**Daftar Pustaka**

Calder, A. (2023). Nine Steps to Success: An ISO 27001 Implementation Overview (4th Edition). IT Governance Publishing.

Humphreys, E. (2017). Implementing the ISO/IEC 27001 Information Security Management System Standard. Artech House.

Peltier, T. R. (2016). Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management. Auerbach Publications.

Von Solms, R., & Van Niekerk, J. (2013). "From Information Security to Cyber Security." Computers & Security, 38, 97–102.

ISACA. (2022). Implementing and Auditing the ISO/IEC 27001:2022 Information Security Management System. ISACA Journal.

BSN. (2023). SNI ISO/IEC 27001:2022 Sistem Manajemen Keamanan Informasi – Persyaratan. Jakarta: Badan Standardisasi Nasional.

ISO.org. (2023). ISO/IEC 27001 – Information Security Management. Diakses dari https://www.iso.org/isoiec-27001-information-security.html

NIST. (2018). SP 800-30 Revision 1: Guide for Conducting Risk Assessments. Gaithersburg, MD: U.S. Department of Commerce.

**ANALISIS DAN HASIL TIAP TAHAP**

**Tahap 1 — Pemilihan Organisasi**

**Profil Organisasi**

**Nama Organisasi:** PT. Semarang Digital Teknologi (SDT)  
**Jenis Bisnis:** Teknologi Informasi dan Layanan Digital  
**Lokasi:** Semarang, Jawa Tengah  
**Jumlah Karyawan:** ±150 orang  
**Ruang Lingkup SMKI:** Divisi Teknologi Informasi dan Operasional (IT Operation & Infrastructure)

**Deskripsi Singkat**

PT. Semarang Digital Teknologi (SDT) adalah perusahaan yang bergerak di bidang solusi digital dan pengembangan perangkat lunak untuk instansi pemerintah, pendidikan, dan perusahaan swasta. SDT menyediakan layanan utama berupa sistem informasi manajemen, pengelolaan cloud, dan keamanan siber.

Struktur organisasi terdiri dari:

* Direksi (CEO, CTO, CFO)
* Divisi Pengembangan Sistem (Software Development)
* Divisi Infrastruktur dan Keamanan TI
* Divisi Layanan Pelanggan dan Dukungan Teknis
* Divisi Administrasi dan Keuangan

**Aset Informasi Penting**

|  |  |  |
| --- | --- | --- |
| **No** | **Aset Informasi** | **Keterangan** |
| 1 | Server Data Pusat | Menyimpan seluruh data proyek dan database klien |
| 2 | Database Pelanggan | Berisi data pribadi dan kontrak kerja sama |
| 3 | Sistem Manajemen Proyek | Platform internal untuk koordinasi proyek |
| 4 | Email Korporat | Media komunikasi utama internal-eksternal |
| 5 | Source Code Repository | Menyimpan kode sumber seluruh aplikasi klien |
| 6 | Infrastruktur Jaringan | Jaringan LAN, VPN, dan cloud storage |
| 7 | Dokumen Keuangan | Informasi laporan, transaksi, dan payroll |
| 8 | Perangkat Karyawan | Laptop, PC, smartphone kerja |
| 9 | Backup Data | Salinan data proyek dan sistem kritikal |
| 10 | Kebijakan dan SOP Internal | Dokumen kebijakan, regulasi, dan pedoman kerja |

Aset-aset tersebut menjadi fokus utama dalam perancangan SMKI karena berdampak langsung pada operasional dan reputasi perusahaan.

**Tahap 2 — Analisis Konteks Organisasi**

**Isu Internal**

* Ketergantungan tinggi terhadap sistem digital dan cloud.
* Belum semua karyawan memahami prosedur keamanan informasi.
* Kurangnya pengawasan terhadap penggunaan perangkat pribadi (*BYOD*).
* Infrastruktur keamanan masih terbatas (firewall dan IDS belum optimal).
* SOP keamanan belum diperbarui secara berkala.

**Isu Eksternal**

* Ancaman serangan siber seperti *phishing*, *malware*, dan *ransomware*.
* Regulasi baru terkait perlindungan data pribadi (UU No. 27 Tahun 2022).
* Tuntutan pelanggan terhadap transparansi dan keamanan sistem.
* Persaingan industri IT yang menuntut kepercayaan tinggi terhadap keamanan data.
* Potensi bencana alam atau kegagalan listrik yang memengaruhi ketersediaan sistem.

**Analisis SWOT**

|  |  |
| --- | --- |
| **Faktor** | **Deskripsi** |
| **Strengths (Kekuatan)** | Tim IT berpengalaman, infrastruktur cloud modern, dukungan manajemen yang kuat. |
| **Weaknesses (Kelemahan)** | Kurangnya pelatihan keamanan, belum ada sertifikasi ISO, proses backup manual. |
| **Opportunities (Peluang)** | Permintaan tinggi terhadap keamanan siber, peluang sertifikasi ISO 27001 untuk meningkatkan kepercayaan klien. |
| **Threats (Ancaman)** | Ancaman serangan siber, kebocoran data, dan perubahan regulasi yang cepat. |

**Pihak Berkepentingan (Stakeholder)**

|  |  |  |
| --- | --- | --- |
| **No** | **Pihak Berkepentingan** | **Kebutuhan terhadap Keamanan Informasi** |
| 1 | Manajemen Puncak | Keberlangsungan bisnis dan kepatuhan hukum |
| 2 | Pelanggan | Perlindungan data dan keandalan sistem |
| 3 | Karyawan | Proses kerja aman dan efisien |
| 4 | Regulator (Kominfo, BSN) | Kepatuhan terhadap regulasi nasional |
| 5 | Mitra Bisnis | Integritas dan keaslian data pertukaran |
| 6 | Masyarakat | Kepercayaan publik terhadap layanan digital SDT |

**Tahap 3 — Penilaian Risiko Keamanan Informasi**

**Identifikasi Aset, Ancaman, dan Kerentanan**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **No** | **Aset** | **Ancaman** | **Kerentanan** | **Dampak** | **Kemungkinan** | **Level Risiko** | **Mitigasi** |
| 1 | Server Data | Serangan malware/ransomware | Firewall belum optimal | Sangat tinggi | Tinggi | **Tinggi** | Instal IDS & antivirus, backup harian |
| 2 | Database Pelanggan | Kebocoran data pribadi | Akses tidak terenkripsi | Tinggi | Sedang | **Tinggi** | Implementasi enkripsi dan MFA |
| 3 | Sistem Email | Phishing & spam | Kurang pelatihan karyawan | Sedang | Tinggi | **Sedang** | Training & filter email |
| 4 | Source Code | Akses ilegal | Password lemah | Tinggi | Sedang | **Tinggi** | Gunakan Git dengan otentikasi ganda |
| 5 | Jaringan Internal | Serangan DDoS | Tidak ada IDS | Tinggi | Tinggi | **Tinggi** | Implementasi firewall adaptif |
| 6 | Backup Data | Hilang/rusak | Tidak ada lokasi alternatif | Tinggi | Sedang | **Sedang** | Backup ke lokasi offsite/cloud |
| 7 | Dokumen Keuangan | Akses tidak sah | File tidak terenkripsi | Sedang | Sedang | **Sedang** | Enkripsi & kontrol akses file |
| 8 | Laptop Karyawan | Kehilangan perangkat | Tidak ada proteksi disk | Tinggi | Tinggi | **Tinggi** | Enkripsi disk & pelacakan perangkat |
| 9 | Website Perusahaan | Deface atau exploit | Update patch tidak rutin | Sedang | Sedang | **Sedang** | Pengetesan keamanan berkala |
| 10 | Kebijakan Internal | Tidak diikuti | Kurang sosialisasi | Sedang | Sedang | **Rendah** | Pelatihan dan monitoring kepatuhan |

**Klasifikasi Risiko**

* Risiko **Tinggi**: Perlu tindakan segera (server, database, jaringan, perangkat karyawan).
* Risiko **Sedang**: Perlu kontrol tambahan dan monitoring berkala.
* Risiko **Rendah**: Cukup dengan pemantauan rutin dan pelatihan kesadaran.

**Matriks Risiko (Kualitatif)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Dampak** | **Rendah** | **Sedang** | **Tinggi** |
| **Kemungkinan Rendah** | Rendah | Rendah | Sedang |
| **Kemungkinan Sedang** | Rendah | Sedang | Tinggi |
| **Kemungkinan Tinggi** | Sedang | Tinggi | Tinggi |

**Tahap 4 — Pemilihan dan Rancangan Kontrol (Annex A ISO/IEC 27001:2022)**

|  |  |  |  |
| --- | --- | --- | --- |
| **No** | **Kode Kontrol** | **Deskripsi Kontrol** | **Implementasi di SDT** |
| 1 | A.5.1 | Kebijakan Keamanan Informasi | Ditetapkan dan disosialisasikan ke semua divisi |
| 2 | A.6.3 | Tanggung Jawab Keamanan Informasi | Dibentuk tim keamanan internal |
| 3 | A.8.12 | Pengendalian Akses terhadap Aset | Gunakan sistem hak akses berbasis peran (RBAC) |
| 4 | A.9.4 | Enkripsi Data | Semua data sensitif terenkripsi AES-256 |
| 5 | A.10.2 | Backup Informasi | Backup otomatis harian ke cloud |
| 6 | A.12.1 | Perlindungan terhadap Malware | Instal IDS & antivirus di server |
| 7 | A.13.1 | Keamanan Jaringan | Firewall generasi terbaru dan pemantauan 24/7 |
| 8 | A.15.1 | Hubungan dengan Pihak Ketiga | Evaluasi keamanan mitra dan NDA |
| 9 | A.16.1 | Manajemen Insiden Keamanan | SOP pelaporan dan respons insiden dibentuk |
| 10 | A.18.1 | Kepatuhan terhadap Regulasi | Disesuaikan dengan UU PDP dan ISO 27001 |

**Tahap 5 — Rancangan Dokumen Utama SMKI**

**1. Kebijakan Keamanan Informasi (Information Security Policy)**

Tujuan: Menjamin perlindungan aset informasi dari ancaman internal dan eksternal.  
Kebijakan mencakup:

* Pencegahan akses tidak sah
* Pengelolaan akun dan kata sandi
* Penanganan insiden
* Backup dan pemulihan data
* Sosialisasi keamanan kepada seluruh karyawan

**2. Tujuan Keamanan Informasi (Information Security Objectives)**

1. Menjaga kerahasiaan dan integritas data pelanggan.
2. Mengurangi risiko kebocoran data minimal 50% dalam 12 bulan.
3. Melatih seluruh staf tentang keamanan informasi dua kali setahun.
4. Memastikan seluruh perangkat TI terproteksi oleh antivirus dan firewall aktif.
5. Mencapai kesiapan sertifikasi ISO/IEC 27001 pada tahun berikutnya.

**3. Rencana Implementasi SMKI (Implementation Plan)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **No** | **Aktivitas** | **Penanggung Jawab** | **Waktu** | **Status** |
| 1 | Pembentukan Tim SMKI | CEO & HRD | Bulan 1 | Selesai |
| 2 | Sosialisasi Kebijakan Keamanan | HRD & IT Security | Bulan 2 | Proses |
| 3 | Implementasi Firewall & IDS | Divisi IT | Bulan 3–4 | On Progress |
| 4 | Pelatihan Keamanan Data | IT Security | Bulan 4–5 | Rencana |
| 5 | Audit Internal SMKI | Tim Audit Internal | Bulan 6 | Rencana |
| 6 | Review dan Perbaikan Dokumen | Manajemen Puncak | Bulan 7 | Rencana |