Universitas Islam Negeri Salatiga
Unit Pelaksana Teknis
Teknologi Informasi dan Pangkalan Data

PEDOMAN KEAMANAN SISTEM INFORMASI

UNIVERSITAS ISLAM NEGERI
SALATIGA

uin saga upt tipd

PEDOMAN
KEAMANAN SISTEM INFORMASI
UIN SALATIGA

UNIVERSITAS ISLAM NEGERI SALATIGA
TAHUN 2023

TIM PENYUSUN

Pengarah	:	Prof. Dr. Zakiyuddin, M.Ag.
Penanggung Jawab	:	Dr. Suwardi M.Pd.
Ketua	:	Bimo Haryo Setyoko, M.Kom.
Anggota	:	1. Naufal Arman Hafidz, S.Kom.
		2. Chamid Bahrul Ulum, S.Kom.
		3. Rio Vindar Prakoso, ST.
		4. Maulana Ayub Dwi Saputra, S.Kom.

DAFTAR ISI

KATA PENGANTAR

Assalamu'alaikum w.w

Alhamdulillah, puji dan syukur kami panjatkan kehadirat Allah S.W.T. atas rahmat dan karunia-Nya sehingga penyusunan Pedoman Keamanan Sistem Informasi Universitas Islam Negeri Salatiga dapat diselesaikan tepat pada waktunya. Penyusunan Pedoman Keamanan Sistem Informasi ini dimaksudkan untuk memberikan pedoman bagi pengelola teknologi informasi dan pengelola layanan yang menggunakan sistem informasi dalam melaksanakan tugas dan fungsi di lingkungan kampus. Pedoman ini merupakan komitmen kami untuk menciptakan keamanan data maupun sistem informasi yang diakses oleh seluruh sivitas akademika UIN salatiga.

Dalam penyusunan pedoman ini, kami melibatkan berbagai pihak, guna memastikan bahwa setiap aspek dari keamanan yang dilakukan sesuai dengan kebutuhan, harapan mereka dan regulasi. Kami berharap pedoman ini dapat menjadi panduan yang berguna bagi semua pengelola teknologi informasi dan pengelola layanan berbasis teknologi informasi dalam mendukung berjalannya roda perguruan tinggi.

Kami juga sampaikan terima kasih kepada semua pihak yang telah berpartisipasi dan memberikan dukungan dalam penyusunan pedoman ini. Untuk itu, kritik dan saran dari berbagai pihak senantiasa diharapkan sebagai bahan penyempurnaan pedoman Keamanan Sistem Informasi ke depan. Semoga pedoman ini bermanfaat bagi semua pihak terkait dan bagi pengembangan keamanan serta pengelolaan teknologi informasi di lingkungan Universitas Islam Negeri Salatiga.

Wassalamu'alaikum w.w.

Salatiga, Mei 2023

Tim Penyusun

BAB I

PENDAHULUAN

A. Latar Belakang

Dalam era digital yang semakin maju, sistem informasi telah menjadi tulang punggung bagi berbagai kegiatan organisasi, baik dalam sektor publik maupun swasta, tidak terkecuali Universitas Islam Negeri (UIN) salatiga. Namun, seiring dengan kemudahan dan kecepatan yang ditawarkan oleh teknologi informasi, juga muncul tantangan besar terkait keamanan data dan informasi.

Keamanan sistem informasi menjadi krusial karena mengamankan data sensitif, menjaga keberlangsungan operasional, serta melindungi reputasi dan kepercayaan publik terhadap suatu entitas. Ancaman terhadap keamanan informasi dapat berasal dari berbagai pihak, termasuk serangan siber, kebocoran data, pencurian identitas, hingga gangguan terhadap infrastruktur IT.

Melindungi informasi tidak hanya menjadi tanggung jawab teknologi informasi semata, tetapi juga merupakan tanggung jawab setiap individu dan departemen dalam suatu organisasi. Kegagalan dalam mengamankan sistem informasi dapat berpotensi merugikan organisasi secara finansial, operasional, dan reputasi.

Pedoman ini disusun untuk memberikan arahan yang jelas dalam mengimplementasikan praktik keamanan yang efektif dan terstruktur. Dengan mengikuti pedoman ini, diharapkan UIN Salatiga dapat:

- Memahami dan mengelola risiko keamanan informasi yang relevan dengan kegiatan UIN salatiga.
- Mengembangkan kebijakan dan prosedur yang sesuai untuk melindungi aset informasi yang berharga.
- Menerapkan kontrol akses yang memadai untuk melindungi data sensitif dari akses yang tidak sah.
- Melakukan pemantauan dan evaluasi secara teratur untuk mendeteksi potensi ancaman dan insiden keamanan.
- Merespons dengan cepat dan tepat terhadap insiden keamanan yang terjadi.

Pedoman ini bukan hanya merupakan panduan praktis, tetapi juga merupakan langkah strategis dalam menjaga keamanan dan integritas sistem informasi pada UIN Salatiga dalam menghadapi tantangan dan perkembangan teknologi yang terus berubah.

B. Dasar Hukum

Keamanan sistem informasi merupakan hal yang diatur secara ketat oleh berbagai undang-undang, peraturan pemerintah, dan standar internasional untuk memastikan perlindungan data sensitif dan operasional yang aman dari ancaman yang ada. Berikut ini adalah beberapa dasar hukum dan peraturan terkait keamanan sistem informasi:

1. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE)
2. Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP 82/2012)
3. Undang-Undang Nomor 19 Tahun 2016 tentang Penanganan Informasi dan Transaksi Elektronik (UU PITE)
4. Standar ISO/IEC 27001:2013 tentang Sistem Manajemen Keamanan Informasi (ISMS)

Pedoman keamanan sistem informasi haruslah sesuai dengan ketentuan-ketentuan diatas untuk memastikan bahwa setiap langkah yang diambil dalam menjaga keamanan informasi tidak hanya efektif tetapi juga mematuhi hukum yang berlaku. UIN Salatiga diharapkan untuk selalu mengikuti perkembangan regulasi terbaru dan menyesuaikan praktik keamanan mereka sesuai dengan standar yang ditetapkan oleh berbagai regulasi di atas.

C. Pengertian

Keamanan sistem informasi merupakan disiplin yang mencakup berbagai strategi, teknik, dan alat yang digunakan untuk melindungi sistem informasi dari ancaman, baik dari dalam maupun dari luar organisasi. Tujuannya adalah untuk menjaga kerahasiaan, integritas, dan ketersediaan data dan system.

Selain itu, keamanan sistem informasi juga mencakup penanganan ancaman dari malware, serangan siber, dan kesalahan manusia. Upaya ini melibatkan penerapan perangkat lunak keamanan, firewall, deteksi intrusi, serta pelatihan karyawan tentang praktik keamanan terbaik. Secara keseluruhan, keamanan sistem informasi merupakan elemen penting dalam melindungi aset digital organisasi dari berbagai ancaman yang terus berkembang, memastikan operasi bisnis berjalan lancar, dan menjaga kepercayaan pengguna serta pemangku kepentingan.

D. Tujuan

Pedoman ini disusun dengan tujuan untuk membantu perguruan tinggi dalam memberikan kerangka kerja yang sistematis dan terstruktur dalam melindungi aset informasi organisasi dari berbagai ancaman. Pedoman ini bertujuan untuk:

1. Melindungi Kerahasiaan Informasi: Memastikan bahwa informasi hanya diakses oleh pihak-pihak yang berwenang, sehingga data sensitif dan pribadi tetap aman dari akses yang tidak sah.
2. Menjaga Integritas Data: Mencegah modifikasi atau manipulasi data oleh pihak yang tidak berwenang, sehingga informasi tetap akurat dan dapat dipercaya.
3. Menjamin Ketersediaan Sistem dan Data: Memastikan bahwa sistem informasi dan data tersedia untuk pengguna yang berwenang kapan saja diperlukan, serta mencegah gangguan layanan seperti serangan denial-of-service.
4. Mencegah dan Mengelola Risiko: Mengidentifikasi potensi ancaman dan kerentanan, serta mengimplementasikan langkah-langkah untuk mengurangi risiko yang dapat merugikan UIN Salatiga.
5. Mematuhi Regulasi dan Standar: Memastikan bahwa UIN Salatiga mematuhi berbagai peraturan, standar, dan kebijakan terkait keamanan informasi yang berlaku, seperti GDPR, HIPAA, atau ISO 27001.
6. Meningkatkan Kepercayaan dan Reputasi: Melindungi informasi pelanggan, mitra, dan pemangku kepentingan lainnya untuk mempertahankan dan meningkatkan kepercayaan serta reputasi organisasi.
7. Menjaga Keberlangsungan Operasi: Memastikan bahwa operasi bisnis dapat terus berjalan meskipun terjadi insiden keamanan, melalui rencana pemulihan bencana dan strategi kontinuitas bisnis.
8. Mendorong Kesadaran dan Pendidikan: Meningkatkan kesadaran dan pemahaman karyawan tentang pentingnya keamanan informasi melalui pelatihan dan sosialisasi, sehingga mereka dapat berperan aktif dalam menjaga keamanan sistem.
9. Mengidentifikasi dan Menanggapi Insiden: Memberikan pedoman untuk mendeteksi, melaporkan, dan merespons insiden keamanan dengan cepat dan efektif, sehingga dampaknya dapat diminimalkan.

Dengan memiliki pedoman keamanan sistem informasi yang komprehensif, UIN Salatiga dapat lebih efektif dalam melindungi aset informasinya dan menjaga keberlanjutan serta keberhasilan operasionalnya dalam jangka panjang.

BAB II

DEFINISI DAN JENIS

A. Definisi Keamanan Sistem Informasi

Keamanan sistem informasi adalah disiplin yang mencakup berbagai strategi, teknik, dan alat yang digunakan untuk melindungi sistem informasi dari ancaman, baik dari dalam maupun dari luar organisasi. Tujuannya dari keamanan sistem informasi adalah untuk menjaga kerahasiaan, integritas, dan ketersediaan data dan sistem.

1. Kerahasiaan, merujuk pada perlindungan informasi agar hanya dapat diakses oleh pihak-pihak yang berwenang. Hal ini melibatkan penerapan kontrol akses, enkripsi data, dan kebijakan privasi yang ketat.
2. Integritas memastikan bahwa data tidak dapat diubah atau dimanipulasi oleh pihak yang tidak berwenang. Ini memerlukan mekanisme untuk mendeteksi perubahan yang tidak sah dan mengembalikan data ke keadaan aslinya.
3. Ketersediaan berarti memastikan bahwa sistem informasi dan data dapat diakses dan digunakan oleh pengguna yang berwenang kapan pun dibutuhkan. Ini melibatkan penerapan langkah-langkah untuk mencegah gangguan layanan seperti serangan denial-of-service dan menjaga infrastruktur teknologi yang andal.

Selain itu, keamanan sistem informasi juga mencakup penanganan ancaman dari malware, serangan siber, dan kesalahan manusia. Upaya ini melibatkan penerapan perangkat lunak keamanan, firewall, deteksi intrusi, serta pelatihan karyawan tentang praktik keamanan terbaik. Secara keseluruhan, keamanan sistem informasi adalah elemen penting dalam melindungi aset digital organisasi dari berbagai ancaman yang terus berkembang, memastikan operasi bisnis berjalan lancar, dan menjaga kepercayaan pengguna serta pemangku kepentingan.

B. Jenis Keamanan Sistem Informasi

Keamanan sistem informasi melibatkan berbagai mekanisme dan strategi untuk melindungi informasi dan sistem dari ancaman. Berikut adalah beberapa jenis utama keamanan sistem informasi:

1. Keamanan Fisik: Melindungi perangkat keras dan infrastruktur fisik dari kerusakan atau akses tidak sah, seperti penggunaan kunci fisik, sistem alarm, pengawasan CCTV, dan kontrol akses biometrik.

2. Keamanan Jaringan: Melindungi integritas, kerahasiaan, dan ketersediaan data yang dikirim melalui jaringan, seperti Firewall, sistem deteksi intrusi (IDS), sistem pencegahan intrusi (IPS), VPN, dan enkripsi data.
3. Keamanan Aplikasi: Melindungi aplikasi perangkat lunak dari ancaman seperti malware, hacking, dan kerentanan lainnya, seperti pengembangan perangkat lunak yang aman (secure coding), pengujian penetrasi, dan penggunaan WAF (Web Application Firewall).
4. Keamanan Informasi: Melindungi data dan informasi dari akses, penggunaan, pengungkapan, atau modifikasi yang tidak sah, sepert Enkripsi data, kontrol akses berbasis peran (RBAC), dan manajemen identitas dan akses (IAM).
5. Keamanan Operasional: Mengelola dan melindungi operasi sehari-hari sistem informasi, seperti Kebijakan keamanan, prosedur operasi standar, dan pelatihan karyawan.
6. Keamanan Endpoint: Melindungi perangkat pengguna akhir seperti komputer, ponsel, dan tablet dari ancaman, seperti penggunaan Antivirus, anti-malware, dan solusi manajemen perangkat mobile (MDM).
7. Keamanan Awan (Cloud Security): Melindungi data, aplikasi, dan layanan yang di-hosting di lingkungan cloud.
8. Keamanan Identitas dan Akses: Mengelola dan mengontrol siapa yang dapat mengakses informasi dan sumber daya tertentu, seperti penggunaan Sistem manajemen identitas (IDM), otentikasi dua faktor (2FA), dan single sign-on (SSO).
9. Keamanan Data: Melindungi data dari ancaman seperti pencurian, penghapusan, atau modifikasi yang tidak sah, seperti backup data, enkripsi data, dan kebijakan retensi data.
10. Manajemen Risiko: Mengidentifikasi, menilai, dan mengelola risiko yang dapat mempengaruhi keamanan informasi, seperti penilaian risiko, analisis dampak bisnis, dan penerapan kontrol mitigasi.
11. Keamanan Pengguna: Meningkatkan kesadaran dan perilaku pengguna terkait dengan keamanan informasi, seperti pelatihan keamanan, kampanye kesadaran keamanan, dan simulasi phishing.

BAB III

STRATEGI KEAMANAN

Agar keamanan system informasi dapat terjamin dan terselnggara dengan baik, maka perlu adanya strategi-strategi dalam menjelankan keamanan sistem informasi. Strategi keamanan sistem informasi melibatkan pendekatan yang komprehensif dan berlapis untuk melindungi informasi dan sistem dari ancaman yang mungkin muncul. Berikut adalah beberapa strategi utama yang dapat diterapkan:

1. Pendekatan Berlapis (Defense in Depth): Menerapkan beberapa lapisan pertahanan untuk melindungi aset informasi. Antara lain menggabungkan firewall, antivirus, deteksi intrusi, enkripsi, dan kontrol akses.
2. Penilaian Risiko: Mengidentifikasi dan mengevaluasi risiko yang dapat mempengaruhi sistem informasi. Melakukan analisis risiko secara berkala, mengidentifikasi kerentanan, dan menentukan dampak serta probabilitas ancaman.
3. Pengelolaan Identitas dan Akses (Identity and Access Management - IAM): Mengontrol siapa yang dapat mengakses informasi dan sumber daya tertentu. Implementasi single sign-on (SSO).
4. Enkripsi: Melindungi data selama transit dan penyimpanan agar tidak dapat dibaca oleh pihak yang tidak berwenang. Menggunakan SSL/TLS untuk enkripsi data saat transit dan enkripsi disk untuk data yang disimpan.
5. Keamanan Jaringan: Melindungi jaringan dari ancaman eksternal dan internal. Menggunakan firewall, sistem deteksi dan pencegahan intrusi (IDS/IPS), dan segmentasi jaringan.
6. Keamanan Aplikasi: Melindungi aplikasi dari ancaman yang mungkin terjadi selama pengembangan dan penggunaan.
7. Backup dan Pemulihan Data: Memastikan data dapat dipulihkan setelah insiden keamanan atau kegagalan sistem. Melakukan backup data secara rutin, menyimpan backup di lokasi yang terpisah, dan menguji prosedur pemulihan data.
8. Pelatihan dan Kesadaran Keaman: Meningkatkan kesadaran karyawan tentang praktik keamanan terbaik dan ancaman potensial. Mengadakan pelatihan keamanan berkala, kampanye kesadaran, dan simulasi phishing.
9. Kebijakan Keamanan dan Prosedur: Menerapkan aturan dan prosedur yang jelas untuk mengelola dan melindungi sistem informasi.
10. Pemantauan dan Audit: Memantau aktivitas sistem dan jaringan untuk mendeteksi dan merespons ancaman secara real-time.

Dengan menerapkan strategi-strategi ini, organisasi dapat membangun pertahanan yang kuat dan komprehensif untuk melindungi sistem informasi dari berbagai ancaman dan risiko yang mungkin terjadi.

BAB IV

PENUTUP

Membangun kampus yang modern di era transformasi digital ini adalah menjadi sebuah keharusan karena adanya perubahan teknologi yang menjadikannya suatu keharusan dalam rangka meningkatkan layanan. Sistem informasi berbasis teknologi sudah tidak lagi menjadi kebutuhan dalam memberikan layanan, akan tetapi sudah menjadi suatu keharusan.

Keamanan sistem informasi adalah aspek krusial yang menentukan keberlanjutan dan keberhasilan operasional organisasi di era digital ini. Pedoman ini telah dirancang untuk memberikan panduan komprehensif dalam melindungi aset informasi kita dari berbagai ancaman yang terus berkembang. Dengan menerapkan strategi dan praktik terbaik yang telah diuraikan, kita berkomitmen untuk menjaga kerahasiaan, integritas, dan ketersediaan informasi yang menjadi tulang punggung kegiatan kita.

Pedoman ini adalah petunjuk teknis, tentang bagaimana kita mengelola system informasi dengan baik dan benar sesuai dengan standar. Implementasi dan kepatuhan terhadap pedoman ini bukan hanya tanggung jawab tim keamanan informasi, tetapi merupakan tanggung jawab bersama setiap individu dalam organisasi. Setiap karyawan memiliki peran penting dalam menjaga keamanan informasi dengan mematuhi kebijakan, prosedur, dan praktik yang telah ditetapkan. Melalui kesadaran dan kerja sama seluruh anggota organisasi, kita dapat menciptakan lingkungan yang aman dan terlindungi dari ancaman siber.

Melalui pedoman ini diharpkan dapat mendorong setiap pengelola di UIN Salatiga untuk terus memperbarui pengetahuan mereka tentang keamanan informasi dan berpartisipasi aktif dalam pelatihan serta kegiatan kesadaran keamanan. Dengan demikian, kita dapat bersama-sama mengatasi tantangan keamanan informasi dan memastikan bahwa aset berharga kita tetap aman. Setiap SDM di UIN Salatiga diharpkan dapat terus berinovasi dan beradaptasi dengan perubahan teknologi sambil mempertahankan komitmen kita terhadap keamanan informasi. Dengan semangat kerja sama dan kepatuhan terhadap pedoman ini, UIN Salatiga dapat mencapai tujuan bersama dalam menciptakan ekosistem digital yang aman dan andal.

upt
tipd

UNIVERSITAS ISLAM NEGERI
SALATIGA