E-ISSN: 3064-5883
DOI: https://doi.org/10.63217/orbit.v1i2.77

Peran Manajemen Sekuriti Dalam Meningkatkan Kesadaran Keamanan Data Mahasiswa Pada Sistem Informasi Akademik Ubhara Jaya

Salman Hafidzul Haq[1], Achmad Fauzi[2], Djuni Thamrin[3], Panji Maulana[4], Arafanditama Najim Hidayat[5], Syahid Abdullah Muslih[6], Toman Andreas Fernando[7]
[1]Universitas Bhayangkara Jakarta Raya, Bekasi, Indonesia, 202310415260@mhs.ubharajaya.ac.id
[2]Universitas Bhayangkara Jakarta Raya, Bekasi, Indonesia, achmad.fauzi@dsn.ubharajaya.ac.id
[3]Universitas Bhayangkara Jakarta Raya, Bekasi, Indonesia, djuni.thamrin@dsn.ubharajaya.ac.id
[4]Universitas Bhayangkara Jakarta Raya, Bekasi, Indonesia, 202310415289@mhs.ubharajaya.ac.id
[5]Universitas Bhayangkara Jakarta Raya, Bekasi, Indonesia, 202310415137@mhs.ubharajaya.ac.id
[6]Universitas Bhayangkara Jakarta Raya, Bekasi, Indonesia, 202210415103@mhs.ubharajaya.ac.id
[7]Universitas Bhayangkara Jakarta Raya, Bekasi, Indonesia, 202210415137@mhs.ubharajaya.ac.id

Corresponding Author: 202310415260@mhs.ubharajaya.ac.id[1]

Abstract**:** *This research explores the role of security management in increasing students' personal data security awareness in the Academic Information System (AIS) of Bhayangkara University of Greater Jakarta. Based on a literature review, this research identifies the risks of data leakage such as identity theft and data breaches, in addition to mitigation strategies involving education and improved security policies. The findings show that security management plays an important role in educating students through awareness campaigns, by implementing technical measures such as data encryption, and monitoring account activity to protect personal data. The study concludes by emphasizing the importance of collaboration between educational institutions and students to build a more secure system.*

Keyword: *Security Management, Data Security Awareness, Academic Information System, Data Leakage, Digital Privacy.*

Abstrak: Penelitian ini mengeskplorasi peran manajemen keamanan dalam meningkatkan kesadaran keamanan data diri mahasiswa pada Sistem Informasi Akademik (SIA) Universitas Bhayangkara Jakarta Raya. Penelitian ini menggunakan pendekatan kualitatif deskriptif berdasarkan tinjauan literatur, penelitian ini mengidentifikasi risiko dari kebocoran data seperti pencurian identitas dan pelanggaran data, di samping strategi mitigasi yang melibatkan edukasi dan peningkatan kebijakan keamanan. Temuan menunjukkan bahwa manajemen keamanan memainkan peran penting dalam mengedukasi mahasiswa melalui kampanye kesadaran, dengan menerapkan langkah-langkah teknis seperti enkripsi data, dan memantau aktivitas akun untuk melindungi data pribadi. Studi ini menyimpulkan dengan menekankan pentingnya

kolaborasi antara lembaga pendidikan dan mahasiswa untuk membangun sistem yang lebih aman.

Kata Kunci: Manajemen Sekuriti, Kesadaran Keamanan Data, Sistem Informasi Akademik, Kebocoran Data, Privasi Digital.

PENDAHULUAN

Perkembangan teknologi informasi diera sekarang semakin meningkat, dimana sebuah institusi maupun perusahaan berlomba lomba untuk meningkatkan pelayanan mereka agar memberikan kenyamanan dan keamanan serta meningkatkan produktivitas dan efisiensi untuk penggunanya. Termasuk dalam dunia Pendidikan baik Perguruan Tinggi Negri maupun Swasta, keduanya memberikan pelayanan pusat Informasi berbasis teknologi. Sistem Informasi Akademik (SIA) telah menjadi elemen penting dalam pengelolaan data mahasiswa dan penyediaan dukungan informasi akademik di berbagai institusi pendidikan. Dalam konteks pendidikan saat ini, sistem informasi akademik (SIA) tidak hanya berfungsi sebagai sarana untuk menyimpan dan mengelola informasi, tetapi juga sebagai alat yang memfasilitasi komunikasi antara mahasiswa, dosen, dan staf administrasi. Namun, seiring dengan meningkatnya penggunaan teknologi informasi, maka kompleksitas keamanan informasi juga ikut meningkat (Saraswati, 2013).

Meskipun sistem keamanaan akademis memberikan kemudahan komunikasi antara mahasiswa dengan dosen atau staf administrasi dalam mengakses hal-hal yang berhubungan dengan akademik. Namun disamping itu semua, ada permasalah yang perlu diperhatikan (Ariyadi et al., 2023). Salah satunya yaitu keamanan data pribadi mahasiswa, seperti nama, nomor pokok mahasiswa (NPM), nomer induk keluarga (NIK), alamat tempat tinggal, riwayat akademik, dan informasi keuangan, menjadi perhatian utama dalam manajemen sistem informasik akademik (SIA). Saat ini data sudah menjadi hal yang sangat penting, resiko ancaman terhadap data yang kita miliki pun semakin tinggi. Beberapa faktor tersebut disebabkan oleh kecelakaan, atau peristiwa yang tidak disengaja, karena kelalaian pengguna itu sendiri, ataupun orang lain (Setiawan & Yulianto, 2020).

Penyalahgunaan data pribadi dapat terjadi melalui berbagai cara, mulai dari serangan siber, akses tidak sah, hingga kebocoran data. Kebocoran data diri merupakan sebuah ancaman yang serius karena dapat berdampak kepada pemalsuan identitas, penyalahgunaan data, bahkan kerugian finansial(Anggen Suari & Sarjana, 2023).

Insiden-insiden ini tidak hanya berpotensi merugikan individu mahasiswa, tetapi juga dapat mengancam reputasi institusi pendidikan serta integritas sistem akademik secara keseluruhan (Setiawan & Yulianto, 2020).

Sayangnya kesadaran mahasiswa akan pentingnya menjaga keamanan data seringkali masih rendah. Jika data ini jatuh ke tangan yang salah, risiko penyalahgunaan data pribadi semakin meningkat. Kebocoran data pribadi menimbulkan masalah yang cukup signifikan, bukan hanya berdampak pada masalah penyalahgunaan data, tetapi juga, mulai dari pencurian identitas, penipuan, hingga manipulasi data akademik, bahkan secara fisik maupun emosional.

Meskipun banyak penelitian telah dilakukan mengenai manajemen keamanan informasi, masih terdapat kekurangan dalam literatur yang membahas secara spesifik tentang sistem informasi akademik (SIA) dan dampaknya terhadap mahasiswa. Dengan memahami manajemen sekuriti sistem informasi akademik dan implikasinya, Maka penelitian ini diharapkan dapat memberikan kontribusi serta pengaruh positif pada pengembang kebijakan. dan praktik yang baik di institusi Pendidikan. Selain itu, kajian ini juga bertujuan untuk mengidentifikasi tantangan, solusi, dan rekomendasi untuk meningkatkan manajemen sekuriti pada sistem informasi akademik (SIA) dengan meningkatkan kesadaran mahasiswa mengenai

pentingnya menjaga keamanan informasi pribadi mereka dalam lingkungan digital yang semakin kompleks, serta dampaknya terhadap mahasiswa sebagai pengguna utama sistem tersebut. Berdasarkan dari latar belakang di atas, maka dapat dirumuskan permasalahan sebagai berikut:

1. Bagaimana peran manajemen sekuriti dalam meningkatkan kesadaran keamanan data pada mahasiswa?
2. Bagaimana dampak dan risiko kebocoran data pada Sistem Informasi Akademik (SIA) bagi Mahasiswa Ubhara Jaya?
3. Strategi apa saja yang perlu diambil oleh mahasiswa dalam meningkatkan perlindungan terhadap data diri mereka pada saat menggunakan SIA Ubhara Jaya ?

METODE

Penelitian ini menggunakan metode penelitian kualitatif deskriptif dengan melakukan pendekatan tinjaun literatur atau *literatur review* dengan mencari dari berbagai sumber buku, jurnal, dan publikasi pustaka lainnya yang relevan (Waruwu, 2022). Dengan pendekatan ini untuk mendalami dan memahami peran manajemen sekuriti dalam meningkatkan kesadaran keamanan data pada mahasiswa serta memahami dampak dan risiko kebocoran data pada sistem informasi akademik bagi mahasiswa.

HASIL DAN PEMBAHASAN

Hasil

Manajemen Sistem Informasi

Manajemen melibatkan serangkaian proses seperti perencanaan, pengorganisasian, pengawasan, pengarahan, dan lainnya dalam sebuah organisasi. Sementara itu, informasi dalam suatu organisasi merupakan hasil pengolahan data sehingga memiliki nilai tertentu (Hariyanto, 2018). Sistem informasi manajemen merupakan gabungan perangkat keras dan perangkat lunak yang dirancang untuk mengolah data menjadi informasi yang bermanfaat (Kurniawan Ritonga & Firdaus, 2024).

Konsep yang terpenting dari manajemen sekuriti informasi ini, yaitu memanajemenkan dan mengawasi serta mengelola aset dengan tujuan yang dapat dimanfaatkan dengan cara terbaik (Emi & Farizy, 2021). Manajemen keamanan informasi merupakan aspek krusial dalam pengawasan dan perlindungan aset digital organisasi maupun data pribadi. Dalam konteks ini, terdapat dua kategori utama aset yang perlu dilindungi yaitu aset fisik dan aset digital. Aset pertama yang bersifat *tangible* (dapat disentuh) seperti perangkat keras, infrastruktur jaringan, media penyimpanan, dan fasilitas fisik memerlukan pengamanan secara fisik. Sementara itu, aset kedua yaitu informasi dan data yang bersifat *intangible* (tidak berwujud) membutuhkan keamanan yang lebih kompleks karena nilai pentingnya terletak pada konten dan strukturnya.

Manajemen Sekuriti

Manajemen sekuriti atau dalam kata lain yaitu manajemen kemanan merupakan sebuah usaha dengan serangkaian bentuk strategi yang berfungsi untuk meningkatkan keamanan serta pencegahan kerugian sehingga tidak terjadi peretasan yang dapat mengakibatkan kerugian, dengan syarat efisien dan efektif (Susanto et al., 2023). Dalam konteks ini, pemahaman mendalam tentang manajemen keamanan menjadi fondasi penting bagi setiap organisasi untuk membangun pertahanan yang efektif terhadap berbagai bentuk ancaman. Pendekatan komprehensif dalam manajemen keamanan tidak hanya mencakup aspek teknologi, tetapi juga melibatkan faktor manusia, proses, dan kebijakan yang saling terintegrasi.

Manajemen sekuriti merupakan pendekatan holistik yang menggabungkan strategi, operasi, prosedur, teknologi, pendidikan, dan pemantauan untuk melindungi aset terpenting organisasi dari berbagai ancaman dan risiko. Hal ini yang memungkinkan organisasi untuk

meningkatkan efisiensi operasional, menjaga reputasi mereka, dan memenuhi kebutuhan pemangku kepentingan.

Keamanan Data

Menurut (Taylor & Bean, 2013) "keamanan" mengacu pada suatu kondisi di mana anggota kelompok atau organisasi memiliki keyakinan relatif bahwa hal-hal yang mereka hargai cukup aman dari ancaman, atau bahwa jika ancaman muncul, ancaman tersebut akan berhasil diatasi (jika tidak dikalahkan) oleh kemampuan adaptasi dan pertahanan kelompok. Sedangkan data merupakan salah satu aset penting dan berharga baik bagi individu maupun organisasi (Wijoyo et al., 2023).

Dalam penelitian (Ujung et al., 2023) menjelaskan bahwa keamanan data merupakan sebuah proses fundamental yang dapat memastikan bahwa data yang tersimpan di dalam basis data selalu terlindungi serta terjaga ketersediaannya. Proses keamanan tersebut melalui beberapa langkah tertentu, sehingga data yang tersedia hanya bisa diakses oleh pengguna terkait tanpa bisa diakses oleh pihak asing. Keamanan data mencakup beberapa aspek yang diantaranya yaitu, kebijakan kemanan, manajemen akses, serta pengawasan (monitoring).

Kebijakan keamanan data mengacu pada peraturan dan ketentuan yang berlaku, dalam memastikan data yang ada tetap ada dan tidak diselewengkan. Manajemen akses, di sisi lain berfungsi untuk membatasi aturan pengguna dalam mengakses sebuah data pada sebuah basis data, agar perizinan akses yang diberikan hanya kepada pengguna sah saja. Terakhir yaitu pengawasan (monitoring) hal ini dilakukan guna memastikan tercatatnya keseluruhan pengaksesan ke basis data, sehingga pengguna dapat dengan cepat mengidentifikasi adanya potensi ancaman sedini mungkin.

Sehingga pada kesimpulannya, keamanan data merupakan aspek penting dalam memastikan data yang ada dan tersimpan selalu aman serta terlindungi sehingga data tersebut tidak dapat diakses oleh pihak yang tidak berwenang. Dengan cara mengimplementasikan serta memastikan sebuah kebijakan keamanan yang tepat, mulai dari segi manajemen akses, dan pengawasan (monitoring) yang dilakukan, maka dengan mengimplementasikan kebijakan keamanan tersebut dapat dipastikan keamanan serta ketersediaan data yang ada pada sebuah organisasi hanya bisa diakses bagi pengguna yang berwenang saja.

Aspek-aspek Terhadap Keamanan Data

Keamanan data bagi suatu perusahaan atau organisasi sangatlah penting untuk dijaga kerahasiannya, maka dari itu suatu Perusahaan atau Organisasi perlu memerhatikan aspek yang terkait didalamnya, berikut aspeknya menurut (Chalifa, 2015) :

1) Kerahasiaan (*Confidentiality)*
   Merupakan aspek yang memastikan data atau informasi tetap bersifat rahasia, sehingga hanya dapat diakses oleh pihak yang memiliki otoritas, sekaligus menjaga kerahasiaan data selama proses pengiriman, penerimaan, dan penyimpanan.
2) Integritas (*Integrity)*
   Aspek ini bertujuan untuk menjamin bahwa data yang tersimpan pada sebuah basis data tidak dapat diakses oleh pihak asing, sehingga tidak ada pengambilan atau perubahan data tanpa izin dari pengguna sah.
3) Ketersediaan (*Availability)*
   Merupakan aspek yang memastikan data selalu tersedia saat dibutuhkan, sehingga pengguna yang memiliki hak akses dapat memanfaatkan informasi dan perangkat terkait sesuai kebutuhan.

Ancaman terhadap Keamanan Data

Ancaman terhadap keamanan data semakin meningkat seiring dengan berkembangnya teknologi informasi. Di antara berbagai ancaman, seperti spamming, scamming, phishing, malware propagation, dan spoofing, penting untuk memahami bagaimana masing-masing dapat memengaruhi keamanan email mahasiswa (Wahyu Hidayat M et al., 2023). Spamming, misalnya, tidak hanya mengganggu komunikasi sehari-hari tetapi juga dapat menjadi pintu masuk bagi penjahat siber untuk mengakses informasi pribadi. Ketika email penuh dengan spam, risiko mengabaikan pesan penting yang berkaitan dengan keamanan atau informasi akademik juga meningkat, menciptakan celah bagi potensi penyalahgunaan data.

Dampak Kebocoran Data

Pelanggaran data pelanggan dapat mengakibatkan kerugian yang signifikan, seperti risiko pencurian identitas, penipuan keuangan, atau bahkan pemanfaatan data untuk aktivitas ilegal. Selain itu, insiden semacam ini juga dapat berdampak negatif pada reputasi perusahaan atau organisasi yang mengelola data tersebut, karena pelanggan cenderung kehilangan kepercayaan terhadap pihak yang gagal menjaga keamanan informasi mereka. (Milafebina et al., 2023).

Kesadaran keamanan Data

Kesadaran terhadap keamanan informasi mencerminkan sejauh mana masyarakat dan individu memahami pentingnya melindungi data, disertai tanggung jawab untuk bertindak sesuai dengan pemahaman tersebut.

Menurut (Budi & Tarigan, 2018) kesadaran keamanan informasi merujuk pada tingkat pengetahuan pengguna mengenai konsep ini, kepatuhan mereka terhadap aturan keamanan, serta parameter lain yang telah ditetapkan oleh organisasi.

Dengan adanya kesadaran terhadap keamanan memungkinkan individu untuk lebih memperhatikan berbagai masalah atau potensi ancaman yang dapat terjadi. Keamanan bukan sekadar alat, melainkan sebuah sistem terpadu yang melibatkan aspek manusia, proses, dan teknologi. Oleh karena itu, diperlukan pemahaman yang mendalam untuk menjalankan proses perlindungan informasi dengan memanfaatkan teknologi secara cermat dan bijak (Islami et al., 2016). Kesadaran keamanan informasi memiliki tujuan dalam meningkatkan keamanan dengan menerapkan hal berikut:

1) Para pengguna dan pengelola informasi paham akan memperhatikan sistem keamanan informasi dan mengajarkan kepada mereka cara untuk melakukan pengamanan yang baik sehingga mereka dapat meningkatkan kinerja mereka dan lebih sadar akan sistem keamanan informasi.
2) Mengembangkan kemampuan serta wawasan agar para pengguna dan pengelola informasi mampu menjalankan tugas mereka dengan lebih efisien.
3) Mengembangkan pemahaman mendalam tentang pengetahuan yang diperlukan untuk mengelola, menerapkan, atau menjalankan program kesadaran keamanan informasi di dalam sebuah organisasi.

Sistem Informasi Akademik

Sistem Informasi Akademik (SIA) adalah sebuah sistem yang dirancang untuk mengelola data akademik, baik melalui perangkat lunak maupun perangkat keras, guna memastikan kelancaran kegiatan akademik serta menghasilkan informasi yang bermanfaat bagi pengelolaan perguruan tinggi. Sistem ini juga berfungsi sebagai alat bantu dalam pengambilan keputusan bagi pihak eksekutif. Tujuan utama dari sistem ini adalah mendukung Pelaksanaan pendidikan sehingga institusi perguruan tinggi mampu menyajikan layanan informasi yang efektif dan maksimal dengan memanfaatkan jaringan internet. (Damayanti et al., 2021).

Sistem Informasi Akademik (SIA) juga berperan dalam mengorganisasi dan menyampaikan data akademik yang melibatkan interaksi antara siswa, dosen, administrasi akademik, hasil penilaian, serta berbagai atribut lainnya. Sistem ini mendukung kegiatan administratif akademik, termasuk pengelolaan transaksi belajar mengajar, kelengkapan dokumen, dan pengelolaan biaya yang terkait dengan proses registrasi maupun operasional harian administrasi akademik. (Anam, 2018).

Dalam perguruan tinggi, sistem informasi akademik (SIA) memegang peranan penting dalam meningkatkan efektivitas dan efesiensi lembaga pendidikan. Sistem ini dirancang untuk mengelola dan menyajikan data- data akademik, seperti kartu hasil studi (KHS), kartu rencana studi (KHS), rekap hasil studi, mata kuliah, jadwal, kehadiran dan banyak lainnya. Sistem ini juga memberikan kemudahan dan keringanan kepada mahasiswa dan dosen agar dapat mengakses informasi akademik tanpa harus mendatangi kampus. Sehingga, kendala-kendala selama ini terjadi menjadi terbantu (Homaidi, 2015).

Penelitian Terdahulu

Tabel 1. Penelitian Terdahulu Yang Relevan

No	Author (Tahun)	Judul Penelitian	Tujuan Penelitian	Hasil dan Kesimpulan
1.	(Maulana et al., 2023)	Manfaat manajemen keamanan informasi terhadap keamanan data pribadi mahasiswa prodi akuntasi universitas trunojoyo madura	Tujuan penelitian ini untuk meningkatkan kesadaran mahasiswa dalam mengelola data diri, mengevaluasi praktik keamanan informasi dan mengidentifikasi masalah yang beresiko terhadap keamanan data, serta menawarkan strategi keamanan efektif yang dapat diterapkan.	Penelitian ini mengidentifikasi adanya resiko-resiko yang berpotensi ancaman terhadap keamanan data diri. Penulis meyimpulkan adanya peranan manajemen sekuri dalam menigkatkan kesadaran mahasiswa mengenai praktik keamanan data diri yang efektif
2.	(Sharipuddin, 2014)	Pembangunan sistem manajemen keamanan pada sistem informasi akademik (Studi kasus pada STIKOM dinamika bangsa)	Fokus penelitian ini pada peningkatan keamanan pada sistem informasi akademik melalui peningkatan yang komprehensif pada sistem manajemen keamanan.	Peneltian ini menjelaskan bahwa pentingnya struktur sistem manajeman keamanan yang baik dapat meningkatkan keamanan dan efektivitas serta pengalaman bagi pengguna.
3.	(Mewengkang et al., 2021)	Implementasi Kebijakan Sistem Informasi Manajemen Akademik Di Universitas Negeri Manado	Tujuan penelitian ini menganalisis implementasi secara komprehensif pada sistem informasi manajemen dalam lingkungan akademik Universitas Negeri Manado serta mengidentifikasi tantangan, mengevaluasi sistem dan rekomendasi perbaikan yang dapat ditindak lanjukan	Sistem informasi manajemen menjadi bagian penting untuk manajamen akademik dalam memberikan persiapan bagi pengguna serta meningkatkan langkah-langkah keamanan

4.	(Ariyadi et al., 2023)	Analisis Kerentanan Keamanan Sistem Informasi Akademik Universitas Bina Darma Menggunakan OWASP	Memastikan bahwa keamanan sistem informasi akademik baik, mengetahui celah terbuka yang beresiko dan memberikan solusi agar terhindar dari serangan *hacker*	Dengan menggunakan pemindaian otomatis menggunakan OWASO ZAP mendapatkan berbagai celah kerentanan pada keamanan sistem. Penelitian ini juga memberikan rekomendasi yang bertujuan untuk meminimalkan resiko serangan dengan mengidentifikasi masalah.
5.	(Mahameru et al., 2023).	IMPLEMENTASI UU PERLINDUNGAN DATA PRIBADI TERHADAP KEAMANAN INFORMASI IDENTITAS DI INDONESIA	Penelitian ini bertujuan untuk menganalisis implikasi undang-udang perlindungan data indonesia terhadap keamanan informasi, mengidentifikasi tantangan dalam implementasinya, dan mengusulkan solusi untuk meningkatkan perlindungan data pribadi di era digital.	Penerapan UU perlindungan data pribadi menjadi langkah yang maju dan signifikan dalam melindungi dan menjaga data pribadi di Indonesia. Implementasi yang berhasil tergantung pada penanganan tantangan yang ada, peningkatan kesadaran publik, dan memastikan bahwa suatu organisasi menerapkan dan mematuhi peraturan yang baru
6.	(Ramayani & Oktarina, 2022)	Analisa Manajemen Resiko Keamanan Pada Sistem Informasi Akademik (Simak) Uin Raden Fatah Palembang Menggunakan Metode Failure Mode And Effect Analysis (FMEA)	Mengimplementasikan strategi manajemen resiko untuk menganalisis dan meminimalkan resiko pada penggunaan sistem informasi akademik (SIMAK)	Penelitian ini menemukan dan mengkategorikan resiko-resiko yang berhubungan dengan sistem SIMAK dengan menerapkan metode FMEA untuk mengedepankan resiko ini, dan meyimpulkan bahwa strategi manajemen risiko yang efektif sangat penting untuk meningkatkan keamanan dan fungsionalitas sistem
7.	(Cahyono et al., 2024)	Pentingnya Edukasi dalam Mengatasi Keamanan Data Mobile Banking di Indonesia	Penelitian ini menyidiki perluasan edukasi pengguna dan keamanan di mobile banking serta mengidentifikasi masalah dan memberikan solusi yang dapat diterapkan untuk meningkatkan keamanan dan keamanan pengguna	Penelitian ini menyimpulkan bahwa edukasi menjadi solusi yang sangat penting untuk meningkatkan keamanan data di mobile banking, efektivitasnya yang sangat meningkat ketika dipasangkan dengan inisiatif pendidikan pada pengguna. Hal ini dilakukan untuk menciptakan lingkungan perbankan digital yang lebih aman dan lebih dapat dipercaya di Indonesia
8.	(Destrianto et al., 2017)	Manajemen Risiko Ancaman pada Aplikasi Website Sistem Informasi Akademik Politeknik Negeri Batam Menggunakan Metode OCTAVE	Penelitian ini bertujuan untuk melakukan penilaian terhadap keamanan dan manajemen resiko yang terjadi pada sistem informasi akademik di Politeknik Negeri Batam serta mengidentifikasi dan mengelola resiko terhadap informasi didalamnya dan memberikan panduan sistematis untuk manajemen risiko	Metode OCTAVE merupakan pendekatan sistematis untuk mengelola risiko yang dilakukan dengan membagi proses identifikasi ancaman ke dalam tiga tahapan, yaitu identifikasi risiko, penilaian risiko, dan pengelolaan risiko. Penelitian ini mengungkapkan adanya empat jenis ancaman yang dapat memengaruhi sistem informasi akademik, yaitu ancaman terkait autentikasi seperti *sniffing* dan *cookie replay*, ancaman pada kriptografi seperti *encryption*

			menggunakan metode OCTAVE .	*cracking*, ancaman dalam manajemen sesi seperti *session hijacking, session replay*, dan serangan *man-in-the-middle*, serta ancaman pada manajemen konfigurasi seperti kerentanan terhadap *clickjacking*.
9.	(Zahwani & Nasution, 2024)	Analisis Kesadaran Masyarakat Terhadap Perlindungan Data Pribadi di Era Digital	Tujuan penelitian ini adalah untuk menganalisis kesadaran publik tentang perlindungan data pribadi, memberikan rekomendasi untuk perbaikan, dan berkontribusi pada lanskap digital yang lebih aman melalui peningkatan pemahaman dan pendidikan.	Penelitian ini menjelaskan wawasan signifikan tentang kesadaran publik tentang perlindungan data pribadi, mengidentifikasi faktor-faktor utama yang mempengaruhi, dan menekankan perlunya inisiatif pendidikan untuk mengurangi risiko dan meningkatkan privasi di era digital.
10	(Silvia et al., 2024)	Analisis Keamanan Data Pribadi pada Pengguna BPJS Kesehatan: Ancaman, Risiko, Strategi Kemanan (Literature Review)	Penelitian ini bertujuan untuk menganalisis keadaan keamanan data bagi pengguna BPJS Kesehatan, mengidentifikasi kerentanan, dan mengusulkan strategi efektif untuk meningkatkan perlindungan data pribadi terhadap berbagai ancaman.	Penelitian ini menunjukan analisis komprehensif tentang lanskap keamanan data pribadi di BPJS Kesehatan. Ini mengidentifikasi ancaman utama, menekankan pentingnya pendidikan pengguna dan keamanan jaringan, dan menganjurkan audit keamanan reguler dan kepatuhan terhadap peraturan sebagai strategi penting untuk melindungi informasi sensitif.
11	(Intan Mafiana et al., 2023)	IMPLEMENTASI MANAJEMEN KEAMANAN INFORMASI BERBASIS ISO 27001 PADA SISTEM INFORMASI AKADEMIK	Penelitian ini bertujuan untuk rekomendasi meningkatkan kesadaran dan pemahaman tentang keamanan informasi di kalangan sivitas akademika.	Penelitian ini mengonfirmasi bahwa standar ini memberikan pedoman yang komprehensif untuk mengidentifikasi dan mengelola risiko keamanan informasi, Penelitian juga menekankan pentingnya upaya berkelanjutan dalam memperbaiki dan meningkatkan keamanan sistem akademik seiring dengan perkembangan ancaman siber yang terus berubah.
12	(Fachrudin et al., 2024)	Peranan Penting Manajemen Sekuriti di Era Digitalisasi	Mempelajari keamanan informasi teknologi dari ancaman cyber, peningkatan keamanan dari ancaman cyber dan juga evaluasi dari tantangan cyber baru yang muncul	Keamanan data sangat penting untuk sebuah perusahaan maupun organisasi untuk mendapatkan kepercayaan pelanggan, selain itu implementasi manajemen dan keamanan yang integritas termasuk upaya melindungi teknologi dan informasi yang dimiliki
13	(Irawan et al., 2024)	Pengaruh Efektifitas Manajemen Sekuriti Dalam keamanan Perusahaan	Mengeksplorasi bagaimana efektivitas manajemen sekuriti disebuah perusahaan sangat berpengaruh dari serangan cyber, dan mengidentifikasi tantangan baru untuk meningkatkan	Manajemen sekuritas yang efektif dapat memiliki efek positif bagi keseluruhan operasi perusahaan, perlindungan aset dan data serta menjaga keberlanjutan operasional perusahaan. Serta penerapan kepada karyawan agar lebih mengikuti praktik keamanan yang baik

			manajemen sekuritas serta menerapkannnya	
14	(Hutapea et al., 2024)	Peran Manajemen Sekuriti Dalam Mencegah Resiko Kerugian Terhadap Keuangan Digital	Mengeksplorasi peran manajemen keamanan dalam mencegah risiko kerugian terhadap keuangan digital. Serta memberi wawasan untuk membantu melindungi dana digital yang dapat merugikan finansial	Manajemen Keamanan yang baik dapat melindungi dana digital dari potensi kerugian dengan mengikuti prosedur keamanan yang baik. Termasuk kemitraan multipihak (bank,pemerintah, pengguna, pembuat) memerlukan kerjasama untuk menghadapi ancaman yang terus berkembang. Serta inovasi teknologi yang harus dikembangkan agar meningkatkan kepercayaan pengguna
15	(Azhari et al., 2024)	Penerapan Manajemen Sekuriti Dalam Meningkatkan Keamanan Pengguna Pada Transaksi E-wallet	Mengidentifikasi ancaman keamanan yang muncul dikalangan e-wallet seperti identifikasi identitas dan juga keamanan akun agar penyedia layanan (pembuat) dapat membuat pencegahan yang tepat dan membuat strategi mitigas seperti enskripsi data, otentikasi multifaktor, pemantauan transaksi yang tepat yang dapat dipertanggung jawabkan untuk mengurangi risiko yang dihadapi pengguna e-wallet	Penerapan manajemen keamanan sangat penting untuk menjaga integritas, kerahasiaan, dan ketersediaan data pengguna dengan prosedur yang holistik. Selain masalah teknis, edukasi untuk pengguna juga menjadi bagian yang terpenting dari manajemen keamanan untuk keamanan dan privasi saat bertransaksi secara digital
16	(Sugiartono et al., 2024)	Peran Manajemen Sekuriti Dalam Dunia Digital: Pendekatan Dan Kendala Dalam Perlindungan Data Bisnis	Memahami peran penting manajemen keamanan dalam melindungi data diera digital. Mengidentifikasi tantangan keamanan yang semakin kompleks.	Teknologi digital dapat meningkatkan efektivitas manajemen keamanan. Menerapkan strategi perlindungan data seperti enskripsi data, manajemen hak akses yang ketat yang dapat menjaga integritas karahasiaan informasi
17	(Andini & Anisa, 2022)	Analisis Penilaian Risiko Keamanan Sistem Informasi Akademik Di Universitas Aisyah Pringsewu	penelitian ini bertujuan untuk menilai risiko keamanan pada Sistem Informasi Akademik (SIAKAD) di Universitas Aisyah Pringsewu. Hal ini dilakukan karena universitas tersebut belum melakukan penilaian risiko terhadap SIAKAD, yang dapat menimbulkan permasalahan pada data, informasi, dan gangguan teknis .	Penilaian risiko berfungsi untuk mengidentifikasi ancaman yang dapat memengaruhi aset penting serta menentukan langkah-langkah pencegahan terhadap potensi ancaman tersebut. Klausul dalam ISO 27002 yang berkaitan dengan penilaian risiko mencakup aspek keamanan sumber daya manusia, keamanan fisik dan lingkungan, pengendalian akses, serta akuisisi, pengembangan, dan pemeliharaan sistem informasi.
18	(Siagian &	Analisis dan Perancangan Sistem Informasi	Menganalisis dan merancang sistem informasi akademik yang	Penilaian risiko berperan dalam menggambarkan potensi ancaman terhadap aset-aset vital serta

	Effiyaldi, 2018)	Akademik pada STIKES Prima Jambi	dapat mengatasi berbagai kendala yang dihadapi STIKes Prima Jambi.	merumuskan langkah pencegahan untuk mengantisipasi ancaman yang mungkin terjadi. Klausul yang terdapat dalam ISO 27002 terkait penilaian risiko mencakup aspek keamanan sumber daya manusia, perlindungan fisik dan lingkungan, pengelolaan akses, serta akuisisi, pengembangan, dan pemeliharaan sistem informasi.
19	(Harion o et al., 2019)	*Web-based Academic Information System Security*	Penelitian ini bertujuan untuk mengidentifikasi kelemahan dalam sistem login yang ada, seperti penggunaan password default dan kurangnya enkripsi data, serta untuk merancang solusi yang dapat memperbaiki kelemahan tersebut agar sistem menjadi lebih aman dari potensi ancaman dan penyusupan	Penelitian ini menekankan pentingnya meningkatkan langkah-langkah keamanan SIA untuk melindungi data akademik yang sensitif. Dengan mengatasi kelemahan yang teridentifikasi dan menerapkan solusi yang diusulkan, sistem dapat secara signifikan meningkatkan postur keamanannya dan melindungi informasi pengguna
20	(Yel & Nasution, 2022)	Keamanan Informasi Data Pribadi Pada Media Sosial	Penelitian ini bertujuan untuk mengatasi masalah kritis terkait keamanannn data pribadi di media sosial, menilai resiko, kesadaran, dan perilaku pengguna serta merekomendasi langkah langkah yang lebih kuat dalam hal menyimpan informasi informasi pribadi secara online.	Penelitian ini menekankan pentingnya memahami privasi, kebutuhan kesaaran pengguna, dan perlunya langkah-langkah peraturan untuk melindungi data pribadi di platform media sosial. Studi menunjukkan bahwa menggabungkan teknologi dengan praktik pengguna yang terinformasi dapat menghasilkan peningkatan signifikan dalam keamanan data .

Pembahasan

Peran manajemen sekuriti dalam meningkatkan kesadaran keamanan data pada mahasiswa

Manajemen sekuriti memiliki peranan penting dalam meningkatkan kesadaran keamanan data pribadi mahasiswa. Data pribadi mencakup segala informasi yang dapat digunakan untuk mengidentifikasi seseorang, baik secara langsung maupun tidak langsung. Informasi tersebut meliputi nama, alamat, nomor telepon, alamat email, tanggal lahir, nomor identifikasi, data keuangan, hingga informasi medis.

Menurut (Maulana et al., 2023) salah satu tujuan utama manajemen sekuriti yaitu mengedukasi mahasiswa tentang risiko yang mucul di era digital ini, seperti ancaman siber yaitu pencurian data dan peretas menjadi hal yang penting untuk dibahas dalam era digital saat ini. Pencurian data pribadi merupakan hal yang berbahaya, oleh karena itu perlu adanya pengetahuan dasar terkait tentang *information security* pada mahasiswa dengan meninjau tiga aspek utama dalam keamanan informasi dasar yaitu *Confidentiality, Integrity*, dan *Avaibility* bertujuan untuk meminimalkan terjadinya pencurian data.

Penerapan manajemen sekuriti juga mencakup langkah-langkah edukasi melalui sosialisasi dan kampanye. Berdasarkan hasil dari studi literatur menerangkan bahwa edukasi

dan kampanye tentang kesadaran diperlukan dalam meningkatkan kesadaran pengguna terhadap keamanan data pribadi. Dalam kajian Wibowo & Pratama dalam (Zahwani & Nasution, 2024) menyarankan bahwa pemerintah, perusahaan teknologi, maupun lembaga pendidikan harus saling bekerja sama dalam membuat penyelenggaraan program edukasi secara penyeluruh tentang keamanan data dan privasi digital. Program ini bisa mencakup Workshop, seminar, materi edukasi di sekolah-sekolah dan kursus online yang dapat dengan mudah diakses (Mahameru et al., 2023). Penelitian (Cahyono et al., 2024) juga menunjukan bahwa kampanye edukasi yang efektif dapat membantu mengurangi risiko serangan siber secara signifikan. Kampanye edukasi pengguna memegang peranan yang krusial dalam meningkatkan kesadaran dan perilaku keamanan. Dengan demikian hal ini bertujuan untuk menambah wawasan bagi mahasiswa dengan pengetahuan mengenai perlindungan data pribadi dan ancaman digital pada Sistem Informasi Akademik (SIA).

Dampak dan risiko kebocoran data pada Sistem Informasi Akademik (SIA) bagi Mahasiswa Ubhara Jaya

Dalam sistem informasi akademik, identitas pribadi pengguna menjadi komponen esensial yang berfungsi menjadi elemen utama dalam mengelola berbagai data dan informasi pengguna maupun aktivitas akademik. Informasi ini mencakup biodata diri mahasiswa seperti nama, nomor pokok mahasiswa (NPM), nomer induk keluarga (NIK), alamat tempat tinggal, riwayat akademik, dan informasi keuangan. Dalam konteks keamanan, pengelolaan identitas pribadi ini harus sangat dijaga mengingat risiko kebocoran data semakin tinggi.

Kebocoran data pada Sistem Informasi Akademik (SIA) menjadi ancaman terhadap keamanan data pribadi mahasiswa dapat menimbulkan dampak dan resiko yang signifikan bagi pengguna dan kepercayaan terhadap lembaga atau organisasi. Menurut (Silvia et al., 2024) ada beberapa ancaman yang mungkin akan terjadi akibat kebocoran terhadap keamanan data pribadi yaitu:

1) Pencurian Identitas: Menjadi ancaman terhadap keamanan data, pencurian identitas dapat mengakibatkan seseorang melakukan tindakan kriminal seperti pinjaman online atas nama orang lain, penipuan kartu kredit, dan kegiatan ilegal lainnya.
2) Penyalahgunaan Informasi Pribadi: Informasi yang bocor dapat membuka peluang bagi pihak tertentu untuk menyalahgunakan data tersebut, sehingga akan merugikan pemiliknya. Seperti pencurian atau perdagangan data pribadi.
3) Hilangnya Kepercayaan: Jika sebuah lembaga atau organisasi terkena serangan pencurian data, maka pengguna akan kehilangan kepercayaan dan berpikir bahwa mereka tidak dapat lagi mempercayakan data mereka pada lembaga atau organisasi tersebut.
4) Dampak Finansial dan Psikologis: Kerugian serta penyalahgunaan informasi pribadi merupakan salah satu contoh dampak dari adanya kebocoran data. Bukan hanya itu, kebocoran data bahkan dapat menyebabkan pengguna merasa stress, menimbulkan rasa cemas dan khawatir tentang penyalahgunaan informasi pribadi mereka.

Upaya yang Dapat Dilakukan Mahasiswa untuk Meningkatkan Perlindungan Data Pribadi saat Menggunakan Sistem Informasi Akademik

Dalam meningkatkan keamanan data pribadi mahasiswa saat menggunakan Sistem Informasi Akademik (SIA), terdapat beberapa langkah yang direkomendasikan, yaitu membuat kata sandi (pasword) yang unik (kombinasi huruf & angka) dan kuat (terdiri dari 12 karakter), menjaga kerahasiaan kata sandi (pasword) dengan tidak sembarang memberikannya kepada orang lain, serta menghindari membagikan data diri pada pihak asing (tidak dikenal). Dengan mengimplementasikan langkah-langkah ini, maka mahasiswa dapat meminimalkan potensi

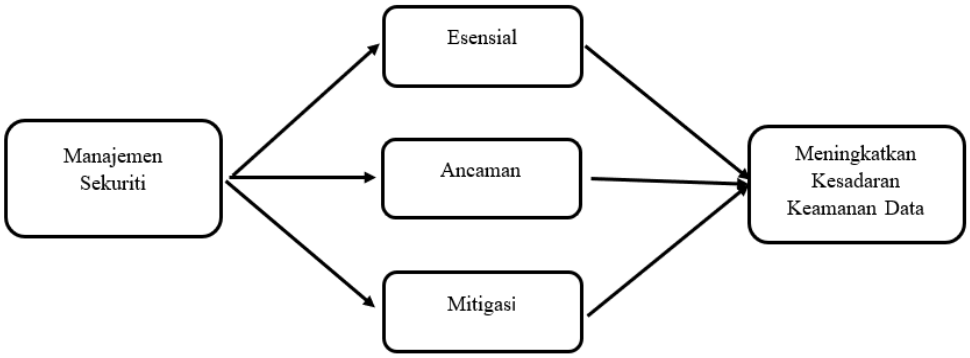
ancaman yang ada pada keamanan siber yang mungkin terjadi saat mengakses SIA. Berikut beberapa langkah yang dapat meningkatkan perlindungan data pribadi mahasiswa saat menggunakan Sistem Informasi Akademik:

1) Manajemen password
   Kata sandi/password yang kuat menjadi peran utama dalam keamanan sebuah sistem. Sehingga sebaiknya sebuah kata sandi dibuat menjadi kompleks dengan minimal 12 karakter, dengan mengombinasikan huruf besar, huruf kecil, angka, dan simbol agar password tersebut sulit untuk ditebak. Selain itu password yang dibuat juga harus bersifat unik, hindari penggunaan tanggal lahir, dan tanggal pernikahan/jadian (Yel & Nasution, 2022).
2) Tidak Menyimpan Password
   Hindari untuk menyimpan password (Password manager) pada sebuah browser, meski fitur ini terlihat memudahkan pengguna dalam mengakses sebuah platform, namun dari sisi keamanan hal ini merupakan suatu ancaman karena jika perangkat kita berada di tangan orang yang tidak bertanggung jawab, ia akan dengan mudah untuk melakukan log in terhadap akun kita karena password yang telah kita simpan sebelumnya.
3) Membiasakan Logout
   Log out akun dari sebuah perangkat merupakan kebiasaan yang mesti dipelihara, karena dengan membiasakan untuk log out akun setelah mengakses sebuah sistem informasi akademik (SIA) dapat meminimalisir ancaman terhadap akun pribadi yang kita miliki (Yel & Nasution, 2022).
4) Menghapus Cookie/Riwayat Pencarian
   Selain memastikan akun kita log out dari sebuah perangkat maka langkah selanjutnya yang dapat diterapkan yaitu menghapus chace data pada sebuah browser, hal ini dilakukan guna memastikan bahwa tidak ada jejak yang tertinggal di sebuah perangkat yang telah kita gunakan (Satoto, 2008).
5) Monitoring Aktivitas Akun
   Memantau aktivitas akun merupakan langkah terakhir dalam meningkatkan kemananan pada Sistem Informasi Akademik, karena dengan melakukan hal tersebut kita dapat mengetahui riwayat login terakhir kali pada akun dan adanya akses asing/aktivitas mencurigakan sedini mungkin. Sehingga jika kita mendapati aktivitas mencurigakan pada akun SIA yang kita miliki kita dapat menindaklanjuti hal tersebut sesegera mungkin.

Dengan menerapkan langkah-langkah tersebut, bukan hanya bertujuan untuk meningkatkan perlindungan data pada Sistem Informasi Akademik, tetapi juga menjadi upaya dalam meningkatkan kesadaran mahasiswa akan pentingnya keamanan data dan penerapannya.

Keerangka Konseptual

Dengan memahami rumusan masalah, kajian pustaka, penelitian terdahulu yang relevan dan pemahaman antar variabel, maka dapat diperoleh kerangka berfikir pada artikel seperti dibawah ini.



Gambar 1. Conceptual Framework

Berdasarkan kerangka pemikiran pada penelitian ini menghasilkan bahwa penerapan manajemen sekuriti di Sistem Informasi Akademik Universitas Bhayangkara Jakarta Raya dapat meningkatkan kesadaran keamanan data diri mahasiswa pada SIA UBHARA JAYA dengan mengetahui tiga aspek penting, yaitu: a) Esensial. b) Ancaman. c) Mitigasi.

KESIMPULAN

Dalam penelitian ini menemukan bahwa manajemen sekuriti berperan penting dalam meningkatkan kesadaran keamanan data mahasiswa di Sistem Informasi Akademik (SIA) Universitas Bhayangkara Jakarta Raya. Dengan pendekatan edukatif melalui kampanye kesadaran dan sosialisasi, mahasiswa dapat lebih memahami pentingnya menjaga keamanan data pribadi dalam era digital yang kompleks. Langkah-langkah seperti penggunaan kata sandi yang kuat, penghapusan cookie, monitoring aktivitas akun, serta edukasi berkelanjutan terbukti efektif dalam meningkatkan perlindungan terhadap ancaman keamanan data.

Dampak kebocoran data, seperti pencurian identitas dan penyalahgunaan informasi, menunjukkan urgensi penerapan manajemen keamanan yang menyeluruh. Dengan demikian, hasil ini diharapkan dapat berkontribusi pada pengembangan teknik perlindungan data dalam sektor pendidikan dan menggarisbawahi pentingnya manajemen sekuriti untuk menjaga integritas dan kepercayaan institusi.

REFERENSI

Anam, K. (2018). Analisa Dan Perancangan Sistem Informasi Akademik Berbasis Web Pada Mi Al-Mursyidiyyah Al-'Asyirotussyafi'Iyyah. *Jurnal Teknik Informatika*, *11*(2), 207–217. https://doi.org/10.15408/jti.v11i2.8867

Andini, D. Y. A., & Anisa, C. (2022). *Analisis Penilaian Resiko Keamanan Sistem Informasi Akademik Security Risk Assessment Analysis Academic Information System*. *1*(1), 1–7.

Anggen Suari, K. R., & Sarjana, I. M. (2023). Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia. *Jurnal Analisis Hukum*, *6*(1), 132–142. https://doi.org/10.38043/jah.v6i1.4484

Ariyadi, T., Widodo, T. L., Apriyanti, N., & Kirana, F. S. (2023). Analisis Kerentanan Keamanan Sistem Informasi Akademik Universitas Bina Darma Menggunakan OWASP. *Techno.Com*, *22*(2), 418–429. https://doi.org/10.33633/tc.v22i2.7562

Azhari, F., Sumarno, S., Fauzi, A., & Pratama, D. R. (2024). *Penerapan Manajemen Sekuriti Dalam Meningkatkan Keamanan Pengguna Pada Transaksi E-wallet*. *2*(2), 138–147.

Budi, D. S., & Tarigan, A. (2018). 1) Jl. Ring Road Utara, Condong Catur, Sleman 55283 2) Jl. Margonda Raya 100. *Tahun*, *2*(1), 53–64.

Cahyono, D., Fahrudin, R., Sinclair, A., Informatika, F. T., Info, A., Data, K., Banking, M., Multifactor, A., & Pengguna, E. (2024). *Pentingnya Edukasi dalam Mengatasi Keamanan Data Mobile Banking di Indonesia*. *3*(1), 81–89.

Chalifa, C. (2015). *Jurnal Informasi Volume VII*. *VII*(1), 58–82. https://informasi.stmik-im.ac.id/wp-content/uploads/2016/05/03-Haryoso-Wicaksono.pdf

Damayanti, S., Elysia, Y. G., Purba, O. A. P., & Prawira, I. F. A. (2021). Pengaruh Penggunaan Sistem Informasi Akademik Di Lingkungan Pendidikan Tinggi. *Jurnal MANAJERIAL*, *20*(1), 43–53. https://doi.org/10.17509/manajerial.v20i1.25095

Destrianto, F. R., Armys, M., & Sitorus, R. (2017). *Manajemen Risiko Ancaman pada Aplikasi Website Sistem Informasi Akademik Politeknik Negeri Batam Menggunakan Metode OCTAVE*. *9*(1), 35–47.

Emi, S. E., & Farizy, S. (2021). Sistem Informasi Manajemen. In *Tangerang Selatan* (Issue 1). www.unpam.ac.id

Fachrudin, R., Respaty, E., Adilah, I. S., & Sinlae, F. (2024). *Multidisciplinary Science Peranan Penting Manajemen Sekuriti di Era Digitalisasi*. *2*(1), 94–102.

Hariono, T., Iqbal, M., Yaqin, N., & Hilyah, A. (2019). Web-Based Academic Information System. *IOP Conference Series: Materials Science and Engineering*, *662*(2). https://doi.org/10.1088/1757-899X/662/2/022042

Hariyanto, S. (2018). Sistem Informasi Manajemen. *Sistem Informasi Manajemen*, *9*(1), 80–85. https://jurnal-unita.org/index.php/publiciana/article/viewFile/75/69

Homaidi, A. (2015). Tijd van slapen: Verstoring van de biologische klok door nacht-en wisse ldiensten. *Nederlands Tijdschrift Voor Geneeskunde*, *159*(51–52), 17–23.

Hutapea, Y., Fauzi, A., Dwiyanti, A., Alifah, F. A., Andina, N., & Jati, S. M. D. (2024). *Peran Manajemen Sekuriti Dalam Mencegah Resiko Kerugian Terhadap Keuangan Digital*. *2*(2).

Intan Mafiana, A., Hanum, L., Ilmi, H. M., & Febriliani, S. (2023). Implementasi Manajemen Keamanan Informasi Berbasis Iso 27001 Pada Sistem Informasi Akademik. *Journal of Digital Business and Innovation Management*, *2*(2), 139–163. https://doi.org/10.26740/jdbim.v2i2.57580

Irawan, C. R., Fauzi, A., Sanjaya, F., & Ramadhan, A. (2024). *Pengaruh Efektivitas Manajemen Sekuriti Dalam Keamanan Perusahaan*. *3*(1), 59–68.

Islami, D. C., I.H, K. B., & Candiwan, C. (2016). Kesadaran Keamanan Informasi pada Pegawai Bank x di Bandung Indonesia. *Jurnal INKOM*, *10*(1), 19. https://doi.org/10.14203/j.inkom.428

Kurniawan Ritonga, R., & Firdaus, R. (2024). Pentingnya Sistem Informasi Manajemen Dalam Era Digital the Importance of Management Information Systems in the Digital Era. *JICN: Jurnal Intelek Dan Cendikiawan Nusantara* , *1*(3), 4353–4358. https://jicnusantara.com/index.php/jicn

Mahameru, D. E., Nurhalizah, A., Wildan, A., Haikal, M., & Rahmadia, M. H. (2023). *Implementasi Uu Perlindungan Data*. *5*(20), 115–131.

Maulana, G. R., Aqila, S. W., Sakinah, N. H., Wulandari, N. I., & Nurhayati, I. (2023). *PENGAMANAN DATA PRIBADI MAHASISWA PRODI AKUNTANSI UNIVERSITAS TRUNOJOYO MADURA*. *9*(2), 89–96.

Mewengkang, R., Tumbel, G., Mamonto, F., & Joufree, V. N. (2021). *YUME : Journal of Management Implementasi Kebijakan Sistem Informasi Manajemen Akademik Di Universitas Negeri Manado*. *4*(2), 318–339. https://doi.org/10.37531/yume.vxix.234

Milafebina, R., Lesmana, I. P., & Syailendra, M. R. (2023). Perlindungan Data Pribadi terhadap Kebocoran Data Pelanggan E-commerence di Indonesia. *Jurnal Tana Man*, *4*(1), 158–169. https://ojs.staialfurqan.ac.id/jtm/

Ramayani, Y., & Oktarina, T. (2022). *Analisa Manajemen Resiko Keamanan Pada Sistem Informasi Akademik (Simak) Uin Raden Fatah Palembang Menggunakan Metode Failure Mode And Effect Analysis (FMEA)*. 289–296.

Saraswati, E. (2013). Sistem Informasi Akademik Berbasis WEB Pada Sekolah Menengah Pertama N 3 Pringkulu. *Indonesia Jurnal on Networking and Security*, *2*(2), 58–63.

Satoto, K. I. (2008). Analisis Keamanan Sistem Informasi Akademik Berbasis Web Di Fakultas Teknik Universitas Diponegoro Oleh : Ir . Kodrat Iman Satoto , MT Program Studi Sistem Komputer Fakultas Teknik Universitas Diponegoro. *Seminar Nasional Aplikasi Sains Dan Teknologi ISSN:1979-911X*, *13 Desember*, 175–186.

Setiawan, A., & Yulianto, E. (2020). *Keamanan Dalam Media Digital* (Edisi Pert). Informatika Bandung.

Sharipuddin. (2014). *SISTEM INFORMASI AKADEMIK (STUDI KASUS PADA STIKOM DINAMIKA BANGSA)*. *9*(2), 132–140.

Siagian, S. H. T., & Effiyaldi. (2018). *AKADEMIK PADA STIKES PRIMA JAMBI*. *3*(4), 1282–1291.

Silvia, A. F., Saputra, W., Sunaryo, H., Sinlae, F., & Info, A. (2024). *Multidisciplinary Science Analisis Keamanan Data Pribadi pada Pengguna BPJS Kesehatan : Ancaman , Risiko , Strategi*. *2*(1), 201–207.

Sugiartono, A. M., Yasril, A., Sumantry, D. H., Nugraha, D. A., Arif, I. N., Nugroho, P. B., Fauzan, R., & Saepudin, T. H. (2024). *No Title*. *2*(7), 742–747.

Susanto, E., Moses, H., Ramadan, R., & Deanova, S. (2023). Analisis dan Pengembangan Sistem Manajemen Sekuriti pada PT. Denso Manufacturing Indonesia. *Jurnal Ilmiah Wahana Pendidikan*, *9*(13), 225–236.

Taylor, B., & Bean, H. (2013). The handbook of communication history. In *The Handbook of Communication History*. Taylor & Francis. https://doi.org/10.4324/9780203149119

Ujung, A. M., Irwan, M., & Nasution, P. (2023). Pentingnya Sistem Keamanan Database untuk melindungi data pribadi. *JISKA: Jurnal Sistem Informasi Dan Informatika*, *1*(2), 44. http://jurnal.unidha.ac.id/index.php/jteksis

Wahyu Hidayat M, Nurhayi Musdira, Natatsa Rasyid, Miftahul Khairi S, & Muh Juharman. (2023). Analisis Ancaman Terhadap Keamanan Data Pribadi pada Email. *Jurnal Pendidikan Terapan*, *01*, 7–12. https://doi.org/10.61255/jupiter.v1i2.73

Waruwu, M. (2022). Motivasi Belajar Dan Prestasi Belajar Pada Mata Pelajaran Ppkn Di Indonesia: Kajian Analisis Meta. *Bhineka Tunggal Ika: Kajian Teori Dan Praktik Pendidikan PKn*, *9*(2), 99–113. https://doi.org/10.36706/jbti.v9i2.18333

Wijoyo, A., Fatimah, S., Toni, Widianti, Y., & Fadillah, M. (2023). *Keamanan Data dalam Sistem Informasi Manajemen : Risiko dan Strategi Perlindungan*. *1*(2), 1–7.

Yel, M. B., & Nasution, M. K. M. (2022). Keamanan Informasi Data Pribadi Pada Media Sosial. *Jurnal Informatika Kaputama (JIK)*, *6*(1), 92–101. https://doi.org/10.59697/jik.v6i1.144

Zahwani, S. T., & Nasution, M. I. P. (2024). *Analisis Kesadaran Masyarakat Terhadap Perlindungan Data Pribadi di Era Digital*. *2*(2), 105–109.