

IMPLEMENTASI MANAJEMEN KEAMANAN INFORMASI BERBASIS ISO 27001 PADA SISTEM INFORMASI AKADEMIK

Agnes Intan Mafiana^{1*}, Luthfiah Hanun², Hanifah Mufidatul Ilmi³
, Silvani Febriliani⁴

¹²³⁴⁵Universitas Negeri Surabaya
Jalan Ketintang, Surabaya 60231, Indonesia
agnesintanmafiana@gmail.com

Abstract

The implementation of data security in academic systems is crucial to protect highly sensitive student, faculty, and administrative information. The ISO 27001 standard has become a critical guide in the development and implementation of effective information security measures. This research aims to evaluate the use of ISO 27001 in the context of university) and analyze its impact on data security in the academic environment. The research identified risks relevant to university's academic systems, including cyber threats and physical risks. The results of this study confirm that the implementation of ISO 27001 has had a positive impact on data security at university. The implementation of appropriate security controls and effective risk reduction has assisted in maintaining the integrity of academic data and protecting valuable information assets. As such, university students, lecturers and administrative staff feel more confident that their data is safe and secure. This research provides important insights into the key role played by the ISO 27001 standard in securing academic systems in higher education institutions. It also underscores the importance of continuous risk evaluation, implementation of appropriate controls, and regular security monitoring as part of a successful data security strategy.

Keywords: Information assets; Data security; ISO 27001.

Received: 29 November 2023; Accepted: 15 Desember 2023; Published: 31 Desember 2023

*Corresponding author

E-mail: agnesintanmafiana@gmail.com

To cite this document:

Mafiana, Agnes Intan., Hanun, Luthfiah., Ilmi, Hanifah Mufidatul., Febriliani, Silviani. (2023). Implementasi Manajemen Keamanan Informasi Berbasis ISO 27001 Pada Sistem Informasi Akademik Universitas. *Journal of Digital Business and Innovation Management*

Abstrak

Penerapan keamanan data dalam sistem akademik adalah krusial untuk melindungi data siswa, dosen, dan informasi administratif yang sangat sensitif. Standar ISO 27001 telah menjadi panduan kritis dalam pengembangan dan implementasi langkah-langkah keamanan informasi yang efektif. Penelitian ini bertujuan untuk mengevaluasi penggunaan ISO 27001 dalam konteks Universitas dan menganalisis dampaknya pada keamanan data di lingkungan akademik. Penelitian ini mengidentifikasi risiko yang relevan dengan sistem akademik universitas, termasuk ancaman siber dan risiko fisik. Hasil penelitian ini mengonfirmasi bahwa penerapan ISO 27001 telah memberikan dampak positif pada keamanan data di universitas. Pelaksanaan pengendalian keamanan yang tepat dan pengurangan risiko yang efektif telah membantu dalam menjaga integritas data akademik dan melindungi aset informasi yang berharga. Dengan demikian, siswa, dosen, dan staf administratif universitas merasa lebih yakin bahwa data mereka aman dan terlindungi. Penelitian ini memberikan wawasan penting tentang peran kunci yang dimainkan oleh standar ISO 27001 dalam mengamankan sistem akademik di institusi pendidikan tinggi. Ini juga menggarisbawahi pentingnya evaluasi risiko yang terus-menerus, penerapan pengendalian yang sesuai, dan pemantauan keamanan yang rutin sebagai bagian dari strategi keamanan data yang sukses.

Kata kunci: Aset informasi; Keamanan data; ISO 27001.

PENDAHULUAN

Bagi sebuah lembaga pendidikan adanya keamanan informasi merupakan hal yang sangat penting, khususnya terkait keamanan data pada sistem informasi akademik. Data akademik dapat berisi informasi sensitif seperti data pribadi siswa, nilai, riwayat pendidikan, hingga data para guru (Abdullah et al., 2019). Pengolahan dan Modifikasi data akademik tanpa izin pihak terkait dapat mengakibatkan kerugian finansial, reputasi, dan privasi (Mat et al., 2020). Oleh karena itu, lembaga pendidikan sudah seharusnya melakukan penerapan kontrol keamanan data akademik mereka yang lebih memadai agar dapat melindungi kerahasiaan, integritas, dan ketersediaan data akademik (Rahman et al., 2021). Keamanan data adalah suatu proses dalam melindungi informasi digital dari akses tidak sah atau pencurian data. Beberapa contoh yang dapat kita lihat terkait kontrol keamanan antara lain enkripsi data, otentikasi pengguna, backup data, dan pembatasan akses (Lee & Lee, 2022). Kontrol keamanan tersebut menjadi resiko kecil adanya pencurian data. Sehingga dengan adanya penerapan keamanan informasi yang baik dapat memberikan kepercayaan kepada siswa dan masyarakat terhadap suatu lembaga pendidikan tersebut (Susanto et al., 2020).

Univeristas XYZ adalah universitas yang telah menerapkan sistem informasi dalam penyimpanan data mahasiswa. Penggunaan sistem akademik ini untuk menunjang penyimpanan data digital dan proses pembelajaran digital, termasuk proses perencanaan dan penjadwalan perkuliahan. Sistem ini bertujuan untuk mempercepat proses administrasi akademik universitas dan mengurangi adanya potensi kesalahan. Namun sistem informasi akademik rentan terhadap berbagai ancaman keamanan. Ancaman yang mungkin saja terjadi yaitu serangan siber seperti phishing dan ransomware dapat mengeksploitasi celah pada sistem dan mengakses data tanpa izin (Cheung et al., 2021). Kesalahan konfigurasi server dan jaringan juga dapat membuat data akademik terekspos ke pihak yang tidak berwenang (Wanget al., 2020). Selain itu, kurangnya pelatihan keamanan informasi bagi pengelola IT dan pengguna dapat menyebabkan kerentanan akibat kesalahan manusia (Susanto & Mukhlash, 2021). Ancaman internal seperti staf atau mahasiswa yang menyalahgunakan hak aksesnya juga perlu diperhatikan, perlu adanya batasan diri untuk tidak menyalahgunakan hak akses ke hal yang dapat merugikan mereka sendiri maupun lembaga (Pang et al., 2022). Lembaga pendidikan perlu adanya penilaian risiko secara berkala pada keamanan informasi untuk meminimalisir kerentanan (Mustafa et al., 2019). Selain itu upaya yang dapat dilakukan dalam meminimalisir kerentanan dengan melakukan perbaikan proses bisnis, melakukan sosialisasi kebijakan, pelatihan pengguna, dan peningkatan teknologi keamanan dapat mengurangi risiko insiden keamanan (Khan et al., 2020).

Penerapan standar keamanan informasi ISO 27001 pada sistem akademik diharapkan dapat membantu lembaga pendidikan mengelola risiko keamanan informasi (Susanto et al., 2019). Menurut (Margo Utomo, 2012) ISO 27001 merupakan standar keamanan informasi yang diterbitkan International Organization for Standardization (ISO) pada bulan Oktober 2005 untuk menggantikan standard BS7799-2. Standard ini berisi spesifikasi atau persyaratan yang harus dipenuhi dalam membangun Sistem Manajemen Keamanan Informasi. ISO 27001 merupakan kerangka kerja untuk menerapkan kontrol keamanan yang sesuai berdasarkan penilaian risiko organisasi (Situmorang et al., 2020). Standar ISO 27001 mensyaratkan dalam proses evaluasi dan peningkatan berkelanjutan untuk menjaga efektivitas pengendalian keamanan (Pritasari et al., 2021). Terdapat berbagai klausul yang dapat digunakan salah satunya penelitian ini menggunakan ISO 27001 klausul 16. Beberapa manfaat menerapkan ISO 27001 antara lain membangun budaya keamanan informasi, memenuhi persyaratan kepatuhan, dan meningkatkan kepercayaan pemangku

<https://ejournal.unesa.ac.id/index.php/jdbim>

kepentingan (Fatmawati et al., 2022). Sertifikasi ISO 27001 oleh badan akreditasi juga dapat menjadi bukti komitmen lembaga pendidikan dalam mengelola keamanan informasi (Rozak et al., 2020). Dengan implementasi yang efektif, ISO 27001 dapat membantu lembaga pendidikan memitigasi risiko keamanan dan melindungi integritas data akademik (Permana et al., 2023).

Menyikapi dari adanya suatu potensi kewanitaan data akademik, Melalui implementasi ISO 27001 pada sistem akademik, universitas diharapkan dapat memperoleh manfaat berupa perlindungan data yang lebih baik, pengurangan risiko, kepatuhan terhadap peraturan yang berlaku, serta peningkatan kepercayaan dari pihak-pihak yang terlibat dalam sistem akademik ini. Sehingga universitas dapat memastikan bahwa sistem akademik aman dari ancaman yang mungkin timbul, sehingga dapat memberikan lingkungan yang aman dan terpercaya untuk seluruh pengguna.

Keamanan Data dan Pentingnya Keamanan Data pada Bidang Pendidikan

Keamanan data merupakan suatu kondisi dimana informasi atau data pribadi seseorang dilindungi dari kehilangan, pencurian, korupsi, penyalahgunaan atau pengungkapan yang tidak sah (Malviya & Singh, 2019). Keamanan data bertujuan untuk membuat data tetap aman dari ancaman internal maupun eksternal sehingga integritas, kerahasiaan, dan ketersediaan informasi terjaga (Setiowati & Sunaryono, 2022).

Pentingnya keamanan data yang berkaitan dengan bidang pendidikan khususnya pada sistem informasi akademik telah banyak dibahas dalam berbagai penelitian. Menurut Fatimah dan Ella (2019), keamanan data sangat penting untuk dilaksanakan pada sistem informasi akademik karena terdapat banyak data pribadi mahasiswa seperti nomor induk mahasiswa, alamat, nomor telepon, nilai-nilai, transkrip, hingga riwayat pendidikan. Apabila data tersebut bocor atau diretas oleh pihak tak bertanggung jawab, maka akan menimbulkan kerugian bagi lembaga perguruan tinggi dan mahasiswa seperti hilangnya data pribadi, penggunaan data untuk kepentingan komersial tanpa seizin, hingga penggunaan data untuk kejahatan lainnya (Hidayatullah & Basuki, 2020).

Menurut beberapa penelitian, pentingnya keamanan data pada institusi pendidikan juga bertujuan untuk melindungi integritas perguruan tinggi dan institusi. Apabila terjadi pelanggaran keamanan data yang signifikan, maka dapat merusak reputasi serta kepercayaan masyarakat terhadap lembaga pendidikan tersebut (Rika & Hartati, 2022; Sutedja & Suryani, 2023). Selain itu, keamanan data juga penting untuk melindungi hak kekayaan intelektual milik perguruan tinggi seperti hasil penelitian dosen dan mahasiswa, konten kuliah, hingga dokumen administrasi (Saputra & Rahmadani, 2020; Santoso & Purnomo, 2020). Apabila data tersebut bocor, maka pihak ketiga dapat menggunakan konten tersebut tanpa izin atau melanggar hak cipta.

Beberapa penelitian internasional juga telah membuktikan bagaimana rentannya sistem informasi akademik terhadap ancaman keamanan siber seperti malware, phishing, DDoS attack, hingga ransomware (Kruse & Frederick, 2019; Brodi & Ribeiro-Neto, 2022). Tanpa adanya langkah keamanan data yang memadai, hal tersebut dapat menghambat proses pembelajaran, penelitian dan operasional kampus. Menurut Mishra dan Bhattacharya (2021), keamanan data sudah seharusnya menjadi prioritas utama bagi setiap lembaga pendidikan agar tujuan pendidikan dapat tercapai dengan aman dan lancar.

Pengertian dan Cara Kerja ISO 27001 serta Penerapannya pada Keamanan Data Sistem Informasi Akademik

ISO 27001 merupakan standar internasional untuk manajemen keamanan informasi yang memandu organisasi dalam mengelola risiko keamanan data. Standar ini memberikan panduan untuk melakukan analisis risiko, menerapkan kontrol, serta memantau dan mengevaluasi tanggung jawab organisasi terhadap informasi (Voulimene et al., 2019).

Cara kerja ISO 27001 adalah dengan mengimplementasikan langkah-langkah seperti penentuan ruang lingkup sertifikasi, penilaian risiko, pengembangan kebijakan keamanan, implementasi kontrol, pelatihan karyawan, serta pemantauan dan tinjauan manajemen. Hal ini bertujuan agar organisasi dapat mendefinisikan, menerapkan, dan memelihara kebijakan, prosedur guna mengelola dan meminimalkan risiko informasi (Kamil et al., 2020).

Beberapa penelitian telah mengkaji penerapan ISO 27001 pada sistem informasi akademik untuk memperkuat keamanan data. Menurut Fatimah dan Ella (2019), implementasi standar ini sangat penting untuk melindungi data pribadi mahasiswa serta memelihara integritas lembaga perguruan tinggi. Sedangkan Hidayatullah dan Basuki (2020) menyarankan

penerapan manajemen risiko berdasarkan ISO 27001 guna melindungi data administrasi, penelitian, dan hak kekayaan intelektual milik perguruan tinggi.

Beberapa Universitas juga telah berhasil meraih sertifikasi ISO 27001 atas sistem informasi akademiknya. Penelitian Santoso dan Purnomo (2020) menunjukkan bahwa implementasi standar internasional ini telah membantu meningkatkan keamanan data serta meyakinkan publik akan komitmen perguruan tinggi dalam perlindungan privasi. Namun demikian, penelitian Prasetyo dan Apriyana (2021) menunjukkan bahwa sertifikasi ISO 27001 membutuhkan biaya operasional yang mahal bagi sebagian universitas di Indonesia.

Secara keseluruhan, penerapan ISO 27001 sangat relevan untuk meningkatkan keamanan data pada sistem informasi akademik. Standar internasional ini dapat membantu lembaga pendidikan dalam melindungi aset digital, memenuhi peraturan privasi, serta mempertahankan reputasi institusi. Namun diperlukan upaya khusus agar implementasinya dapat berjalan efektif di berbagai konteks pendidikan tanah air.

METODE PENELITIAN

Dalam penelitian ini akan melakukan sebuah audit di mana lokasi permasalahanyang dipilih adalah sebuah masalah yang ada di instansi salah satu universitas PTN di Indonesia, mengenai masalah kemanan pada sistem informasi akademik dan akan diselesaikan melalui aturan dari standar ISO 27001 yang dilakukan secara bertahap. Hasil dari sebuah metode tersebut berupa temuan yang nantinya akan dianalisis untuk dicarikan sebuah solusi berupa rekomendasi yang bersifat deskripsi atau gambaran untuk melakukan perbaikan.

Teknik Pengumpulan Data

Dalam melakukan audit harus ada lembar kerja sebagai panduan untuk melakukan wawancara atau pemeriksaan kemudian memverifikasinya. Perolehan data dalam audit ini berdasarkan wawancara dan pengisian kuesioner. Teknik pengumpulan data dilakukan dengan melakukan wawancara dan kuesioner, serta hasil wawancara akan dianalisis. Wawancara yang akan dilakukan adalah wawancara personal kepada *auditee* dimana *auditee* adalah orang yang bertanggung jawab terhadap pekerjaannya. Wawancara dilakukan dengan tatap muka dan tempat wawancara dilakukan di universitas. Pemilihan responden atau bertindak sebagai *auditee* harus mempunyai informasi yang diinginkan oleh peneliti dalam hal ini disebut auditor atau pewawancara. *Auditee* harus mau bekerja sama untuk memberikan informasi yang dibutuhkan oleh auditor atau pihak

pewawancara. Sedangkan pada pengisian kuesioner dilakukan dengan penyebarankuesioner kepada auditee lain yang kurang bisa dijangkau untuk diwawancarai secara langsung. Penyebaran kuesioner dilakukan melalui media sosial yang dimiliki oleh auditor atau pewawancara.

Penelitian ini menggunakan penelitian kuantitatif, menggunakan instrumen kuesioner dengan butir-butir pertanyaan sesuai dengan ISO 27001. Teknik pengumpulan data pada penelitian ini ditujukan kepada *auditee* dengan kriteria sivitas akademika universitas yang bisa mengakses sistem akademik. Target jumlah populasi sampel adalah 100 responden. Adapun populasi responden pada penelitian ini sebanyak 4 orang dengan keterangan pada table berikut.

NO.	Jabatan
1.	Koordinator Program Studi
2.	Dosen
3.	Admin/Sistem data
4.	Mahasiswa

Tahapan Penelitian

Menjelaskan tahapan dan prosedur dalam merancang sistem manajemen keamanan informasi mengacu pada panduan standar ISO 27001 yang disesuaikan dengan kebutuhan penelitian, adapun langkah dan prosedur dapat dijabarkan sebagai berikut:

1. Tahapan Identifikasi Masalah

Tahap identifikasi masalah berfungsi untuk mengidentifikasi beberapamasalah yang ada di perguruan tinggi. Pada penelitian ini berfokus identifikasi permasalahan terkait keamanan data pada sistem akademik meliputi pertahanan integritas, kerahasiaan, dan ketersediaan data yang dikelola, serta mengurangi risiko terhadap ancaman keamanan informasi.

2. Studi Literatur

Studi literatur yang dilakukan pada penelitian ini berdasarkan referensi dari jurnaldan artikel tentang analisa keamanan data menggunakan ISO 27001.secara berkelanjutan kerahasiaan, dan integritas atas informasi yang dimilikinya. ISO 27001 memiliki 16 klausul kontrol keamanan (security control), 39 objektif control (control objectives) dan 133 kontrol keamanan/control (controls). Delapan belas klausul keamanannya adalah sebagai berikut :

- 1) Klausul A.5 *Information Security Policies*
- 2) Klausul A.6. *Internal Organization*
- 3) Klausul A.7 *Human Resource Security*

<https://ejournal.unesa.ac.id/index.php/jdbim>

4) Klausul A.8 *Asset Management*

5) Klausul A.9 *Acces Control*

6) Klausul A.10 *Cryptography*

7) Klausul A.11 *Physical and Enviroment Security*

Klausul A.12 *Operations Security*

8) Klausul A.13 *Communications Security*

9) Klausul A.14 *System Acquisition, Development and Maintenance*

10)Klausul A.15 *Supplier Relationship*

11)Klausal A.16 *Information Security incident Management*

12)Klausal A.17 *Information Security Aspects of Bussiness ContinuityManagement)*

13)Klausal A.18 *Compliance*

3. Pengumpulan Data

Pada tahap pengumpulan data menggunakan teknik wawancara survei kuesioner dengan instrumen kuesioner sesuai ISO 27001 dengan klausul 16 yang dapat diisi oleh koordinator program studi, dosen, admin sitem, dan mahasiswa. Kuesioner ini berkaitan tentang keamanan data pada website akademik SSO universitas. Selain itu, kuesioner ini berupa sebuah pernyataan yang dapat dijawab dengan beberapa pilihan jawaban, yaitu:

- a) Sangat Tidak Setuju
- b) Tidak Setuju
- c) Kurang Setuju
- d) Setuju
- e) Sangat Setuju

Berikut beberapa pernyataan kuesioner mengenai kemanan data informasi yang diajukan untuk koordinator program studi, dosen, admin sistem/data, dan mahasiswa.

a) Pernyataan Koordinator Program Studi

Pernyataan		Klausul Iso 27001:2013
1.	Pimpinan prodi telah menerima prosedur dalam perencanaan dan persiapan tanggap insiden dari pihak SSO universitas dan secara resmi telah digunakan	A.16.1.1 A.16.1.4
2.	Pimpinan prodi telah mengikuti sosialisasi mengenai prosedur pencegahan dan penanganan terhadap ancaman data pada SSO universitas	A.16.1. 1

3.	Pihak SSO telah memberikan umpan balik kepada pelapor mengenai laporan ancamandata/informasi setelah dilakukan penanganan	A.16.1. 1
4	Pimpinan prodi dapat melaporkan segala tindakan terkait keamanan melalui fitur SSO	A.16.1. 2
5	Pemilik akun email akan mendapatkan notifikasi keamanan terkait login email	A.16.1. 2
6	Pimpinan prodi pernah mendapatkan keluhan mengenai sistem akademik	A.16.1. 2
7	Pimpinan prodi telah membuat penanggung jawab dalam manajemen risiko dan eskalasi pelaporan status pengelolaan risiko keamanan informasi sampai ke tingkat pengelola SSO universitas?	A.16.1. 3
8.	Pimpinan prodi telah menyusun langkah-langkah mitigasi dan penanggulangan risiko terkait keamanan data pada mahasiswa	A.16.1. 5
9.	Pimpinan prodi terdampak dengan adanya insiden pengalihan nama sistem akademik	A.16.1. 6
10.	Keluhan mengenai Sistem Akademik telah dikaji secara berkala untuk memastikan dan meningkatkan efektifitas	A.16.1. 6
11.	Pimpinan prodi memepertimbangkn keamanan melakukan backup atau penyimpanan dokumen selain di sistem akademik	A.16.1. 7
12.	Pimpinan Prodi menyimpan segala informasi data diri mahasiswa melalui SSO universitas	A.16.1. 7

b) Pernyataan Dosen

Pernyataan		Klausal Iso 27001:2013
1.	Tugas mahasiswa aman dan tersimpan di dalam sistem	A.16.1.7
2.	Tersedia <i>back up</i> data terkait penelitian, pengabdian, dan pengajaran yang memadai	A.16.1.7

3.	Pihak universitas mengadakan sosialisasi kepadadosen tentang prosedur pencegahan terhadap ancaman keamanan data	A.16.1.1
4.	Pihak universitas mengadakan sosialisasi kepada dosen tentang prosedur penangananterhadapancaman keamanan data	A.16.1.1
5.	Pengubahan <i>password</i> dilakukan secara berkala untuk meminimalisir terjadinya insiden kebocoran informasi	A.16.1.6
6.	Dosen dapat membuat laporan jika ada kendala layanan informasi	A.16.1.2
7.	Melalui dashboard SSO, dosen dapat mengetahui melalui notifikasi pada SSO bahwa terdapat penambahan layanan informasi maupun modifikasi layanan informasi yang sudah ada	A.16.1.1
8.	Terdapat pelatihan khusus yang disediakan oleh Universitas untuk meningkatkan kualitas dosen dalam memahami pengoperasian sistem	A.16.1.1
9.	Dosen dapat membuat layanan penilaian kepuasan di dalam sistem untuk mahasiswa terhadap keamanan jawaban dari tugas yang telah diberikan	A.16.1.7
10.	Dosen dapat membuat layanan penilaian kepuasan di dalam sistem untuk mahasiswa terhadap keamanan jawaban dari tugas yang telah diberikan	A.16.1.1

c) Pernyataan Mahasiswa

Pernyataan		Klausal Iso 27001:2013
1.	Saya mengetahui bahwa keamanan informasimerupakan aspek penting dalam sistem sistem akademik Universitas	A.16.1.1

2.	Saya memahami prinsip-prinsip dasar keamanan informasi	A.16.1. 1
3.	Saya sangat puas dengan tingkat keamanan sistem akademik dalam melindungi data pribadi	A.16.1. 1
4.	Saya merasa Universitas perlu meningkatkan kesadaran tentang keamanan informasi di kalangan mahasiswa	A.16.1. 2
5.	Saya memiliki pemahaman yang memadai tentang pentingnya keamanan informasi dalam sistem akademik	A.16.1. 3
6.	Apakah Anda merasa Universitas perlu terus mengembangkan dan meningkatkan keamanan informasi dalam sistem akademiknya	A.16.1. 6
7.	Saya merasa puas dengan tingkat keamanan sistem akademik dalam melindungi data pribadi dan akademisi	A.16.1. 6
8.	Saya mengetahui bagaimana cara mengakses dan mengelola data pribadi saya dalam Sistem Akademik	A.16.1. 1
9.	Saya yakin bahwa hanya pihak yang berhak memiliki akses ke data akademik dan pribadisaya di sistem akademik	A.16.1. 3
10.	Saya pernah mengalami atau mengetahui kejadian dimana keamanan dalam Sistem Akademik, seperti pelanggaran data	A.16.1. 2

HASIL DAN PEMBAHASAN

Hasil Kuisisioner

a. Dosen

No	Pernyataan	Jawaban
1.	Tugas mahasiswa aman dan tersimpan di dalam sistem	Setuju
2.	Tersedia back up data terkait penelitian, pengabdian, dan pengajaran yang memadai	Setuju
3.	Pihak universitas mengadakan sosialisasi kepada dosen tentang prosedur pencegahan terhadap ancaman keamanan data	Setuju

4.	Pihak universitas mengadakan sosialisasi kepada dosen tentang prosedur penanganan terhadap ancaman keamanan data	Setuju
5.	Pengubahan password dilakukan secara berkala untuk meminimalisir terjadinya insiden kebocoran informasi	Tidak Setuju
6.	Dosen dapat membuat laporan jika ada kendala layanan informasi	Setuju
7.	Melalui dashboard SSO, dosen dapat mengetahui melalui notifikasi pada SSO bahwa terdapat penambahan layanan informasi maupun modifikasi layanan informasi yang sudah ada	Tidak Setuju
8.	Terdapat pelatihan khusus yang disediakan oleh Universitas untuk meningkatkan kualitas dosen dalam memahami pengoperasian sistem	Tidak Setuju
9.	Dosen dapat membuat layanan penilaian kepuasan di dalam sistem untuk mahasiswa terhadap keamanan jawaban dari tugas yang telah diberikan	Setuju
10.	Dosen bekerja sama dengan admin SSO untuk meningkatkan keamanan informasi baik dari materi, tugas, dan penilaian mahasiswa	Setuju

b. Pimpinan Program studi

No	Pernyataan	
1.	Pimpinan prodi telah menerima prosedur dalam perencanaan dan persiapan tanggap insiden dari pihak SSO universitas dan secara resmi telah digunakan	Setuju
2.	Pimpinan prodi telah mengikuti sosialisasi mengenai prosedur pencegahan dan penanganan terhadap ancaman data pada SSO Universitas	Tidak Setuju
3.	Pihak SSO telah memberikan umpan balik kepada pelapor mengenai laporan ancaman data/informasi setelah dilakukan penanganan	Setuju
4.	Pimpinan prodi dapat melaporkan segala tindakan terkait keamanan melalui fitur SSO	Setuju
5.	Pemilik akun email akan mendapatkan notifikasi keamanan terkait login email	Setuju

6.	Pimpinan prodi pernah mendapatkan keluhan mengenai sistem akademik	Setuju
7.	Pimpinan prodi telah membuat penanggung jawab dalam manajemen risiko dan eskalasi pelaporan status pengelolaan risiko keamanan informasi sampai ke tingkat pengelola SSO Universitas	Setuju
8.	Pimpinan prodi telah menyusun langkah-langkah mitigasi dan penanggulangan risiko terkait keamanan data pada mahasiswa	Setuju
9.	Pimpinan prodi terdampak dengan adanya insiden pengalihan nama sistem akademik	Tidak Setuju
10.	Keluhan mengenai sistem akademik telah dikaji secara berkala untuk memastikan dan meningkatkan efektifitas	Setuju
11.	Pimpinan prodi memepertimbangakn keamanan	Setuju
	melakukan backup atau penyimpanan dokumen selain di sistem akademik	
12.	Pimpinan Prodi menyimpan segala informasi data diri mahasiswa melalui SSO universitas	Setuju

c. Mahasiswa

No	Pernyataan	Jawaban
1.	Saya mengetahui bahwa keamanan informasi merupakan aspek penting dalam sistem sistem akademik universitas	Sangat Setuju
2.	Saya memahami prinsip-prinsip dasar keamanan informasi	Setuju
3.	Saya sangat puas dengan tingkat keamanan Sistem akademik dalam melindungi data pribadi	Setuju
4.	Saya merasa Universitas perlu meningkatkan kesadaran tentang keamanan informasi di kalangan mahasiswa	Sangat Setuju
5.	Saya memiliki pemahaman yang memadai Tentang pentingnya keamanan informasi dalam sistem akademik	Setuju

6.	Apakah Anda merasa Universitas perlu terus mengembangkan dan meningkatkan keamanan informasi dalam sistem akademiknya	Sangat Setuju
7.	Saya merasa puas dengan tingkat kemanan sistem akademik dalam melindungi data pribadi dan akademi	Setuju
8.	Saya mengetahui bagaimana cara mengakses dan mengelola data pribadi saya dalam Sistem Akademik	Setuju
9.	Saya yakin bahwa hanya pihak yang berhak memiliki akses ke data akademik dan pribadi saya di sistem akademik	Setuju
10.	Saya pernah mengalami atau mengetahui kejadian dimana keamanan dalam Sistem Akademik, seperti pelanggaran data	Tidak Setuju & Setuju

Tabel Hasil Analisis Menggunakan Maturity Level

a. Pimpinan Program Studi

Analisis A.16.1.1 & A.16.1.4
Pimpinan prodi telah menerima prosedur dalam perencanaan dan persiapan tanggap insiden dari pihak SSO universitas dan secara resmi telah digunakan
Analisis A.16.1.1
Pimpinan prodi telah mengikuti sosialisasi mengenai prosedur pencegahan dan penanganan terhadap ancaman data pada SSO universitas
Analisis A.16.1.1
Pihak SSO telah memberikan umpan balik kepada pelapor mengenai laporan ancaman data/informasi setelah dilakukan penanganan
Analisis A.16.1.2
Pimpinan prodi dapat melaporkan segala tindakan terkait keamanan melalui fitur SSO
Analisis A.16.1.2
Pemilik akun email akan mendapatkan notifikasi keamanan terkait login email
Analisis A.16.1.2

Pemilik akun email akan mendapatkan notifikasi keamanan terkait login email
Analisis A.16.1.2
Pimpinan prodi pernah mendapatkan keluhan mengenai sistem akademik
Analisis A.16.1.3
Pimpinan prodi telah membuat penanggung jawab dalam manajemen risiko dan eskalasi pelaporan status pengelolaan risiko keamanan informasi sampai ke tingkat pengelola SSO universitas?
Analisis A.16.1.5
Pimpinan prodi telah menyusun langkah-langkah mitigasi dan penanggulangan risiko terkait keamanan data pada mahasiswa
Analisis A.16.1.6
Pimpinan prodi terdampak dengan adanya insiden pengalihan nama Sistem akademik
Analisis A.16.1.6
Keluhan mengenai sistem akademik telah dikaji secara berkala untuk memastikan dan meningkatkan efektifitas
Analisis A.16.1.7
Pimpinan prodi mempertimbangkan keamanan melakukan backup atau penyimpanan dokumen selain di sistem akademik
Analisis A.16.1.7
Pimpinan Prodi menyimpan segala informasi data diri mahasiswa melalui SSO universitas
Nilai kepuasan :
Jumlah total yang sesuai = 4
Jumlah total pertanyaan = 12
$4/12 \times 100 = 33,3\%$

Kesimpulan

Setelah survey melalui penyebaran kuisioner tentang kewanaman data pada sistem akademik di Universitas , maka didapatkan kesimpulan :

1. Tingkat penggunaan dan pengelolaan data pada sistem akademik mendapatkan nilai 33,3 %
2. Pimpinan prodi telah menerima prosedur dalam perencanaan dan persiapan tanggap insiden dari pihak SSO universitas dan secara resmi
3. Pimpinan prodi banyak yang mendapatkan keluhan mengenai sistem akademik
4. Pimpinan prodi banyak yang terdampak dengan adanya insiden pengalihan nama sistem akademik

b. Dosen

Analisis A.16.1.7

Tugas mahasiswa aman dan tersimpan di dalam sistem
Analisis A.16.1.7
Tersedia <i>back up</i> data terkait penelitian, pengabdian, dan pengajaran yang memadai
Analisis A.16.1.1
Pihak universitas mengadakan sosialisasi kepada dosen tentang prosedur pencegahan terhadap ancaman keamanan data
Analisis A.16.1.1
Pihak universitas mengadakan sosialisasi kepada dosen tentang prosedur penanganan terhadap ancaman keamanan data
Analisis A.16.1.6
Pengubahan <i>password</i> dilakukan secara berkala untuk meminimalisir terjadinya insiden kebocoran informasi
Analisis A.16.1.2
Dosen dapat membuat laporan jika ada kendala layanan informasi
Analisis A.16.1.1
Melalui dashboard SSO, dosen dapat mengetahui melalui notifikasi pada SSO bahwa terdapat penambahan layanan informasi maupun modifikasi layanan informasi yang sudah ada
Analisis A.16.1.1
Terdapat pelatihan khusus yang disediakan oleh Universitas untuk meningkatkan kualitas dosen dalam memahami pengoperasian sistem
Analisis A.16.1.7
Dosen dapat membuat layanan penilaian kepuasan di dalam sistem untuk mahasiswa terhadap keamanan jawaban dari tugas yang telah diberikan
Analisis A.16.1.1
Dosen dapat membuat layanan penilaian kepuasan di dalam sistem untuk mahasiswa terhadap keamanan jawaban dari tugas yang telah diberikan
Nilai kepuasan :
Jumlah total yang sesuai = 4 dan 3
Jumlah total pertanyaan = 10
$4/10 \times 100 = 40\%$
$3/10 \times 100 = 30\%$

Kesimpulan

Setelah survey melalui penyebaran kuisisioner tentang kemanan data pada sistem akademik di Universitas , maka didapatkan kesimpulan :

1. Tingkat penggunaan dan pengelolaan data pada sistem akademik mendapatkan nilai 40% dan 30%
2. Dosen telah menerima sosialisasi tentang penanganan terhadap ancaman data
3. Tingkat kemanan universitas sudah cukup terjaga

dengan sering mengubah password

c. Mahasiswa

Analisis A.16.1.1
Saya mengetahui bahwa keamanan informasi merupakan aspek penting dalam sistem sistem akademik Universitas
Analisis A1.6.1.1
Saya memahami prinsip-prinsip dasar keamanan informasi
Analisis A.16.1.1
Saya sangat puas dengan tingkat keamanan sistem akademik dalam melindungi data pribadi
Analisis A.16.1.2
Saya merasa Universitas perlu meningkatkan kesadaran tentang keamanan informasi di kalangan mahasiswa
Analisis A.16.1.3
Saya memiliki pemahaman yang memadai tentang pentingnya keamanan informasi dalam sistem akademik
Analisis A.16.1.6
Apakah Anda merasa Universitas perlu terus mengembangkan dan meningkatkan keamanan informasi dalam sistem akademiknya
Analisis A16.1.6
Saya merasa puas dengan tingkat kemanan Sistem Akademik dalam melindungi data pribadi dan akademi
Analisis A.16.1.6
Saya mengetahui bagaimana cara mengakses dan mengelola data pribadi saya dalam Sistem Akademik
Analisis A.16.1.3
Saya yakin bahwa hanya pihak yang berhak memiliki akses ke data akademik dan pribadi saya di sistem akademik
Analisis A.16.1.2
Saya pernah mengalami atau mengetahui kejadian dimana keamanan dalam Sistem Akademik, seperti pelanggaran data
Nilai kepuasan :
Jumlah total yang sesuai = 4
Jumlah total pertanyaan = 10
$4/10 \times 100 = 40\%$

Kesimpulan

Setelah survey melalui penyebaran kuisisioner tentang kemanan data pada sistem akademik di Universitas, maka didapatkan kesimpulan :

1. Tingkat pemahaman data penerapan kontrol keamanan yang telah dilakukan cukup baik untuk keamanan komunikasi mendapat nilai 40 %.
2. Perlu adanya peningkatan kesadaran tentang keamanan informasi

di kalangan mahasiswa

- Universitas perlu mengembangkan dan meningkatkan keamanan informasi dalam sistem akademiknya

Hasil Analisis Data Menggunakan Excel

Tabel 1. Hasil Kuisisioner Kepala Prodi

No	Nama	Item Jawaban												Skor	Nilai
		1	2	3	4	5	6	7	8	9	10	11	1 2		
1	Responden 1	1	1	4	4	2	5	1	5	5	5	2	5	40	66,66667
2	Responden 2	4	1	1	4	5	4	4	2	5	1	1	5	37	61,66667
3	Responden 3	3	2	3	5	3	4	2	2	4	4	2	3	37	61,66667
4	Responden 4	4	5	4	3	5	2	3	4	2	4	4	5	45	75
Rata - rata														39,75	66,25

Tabel 2. Hasil Kuisisioner Dosen

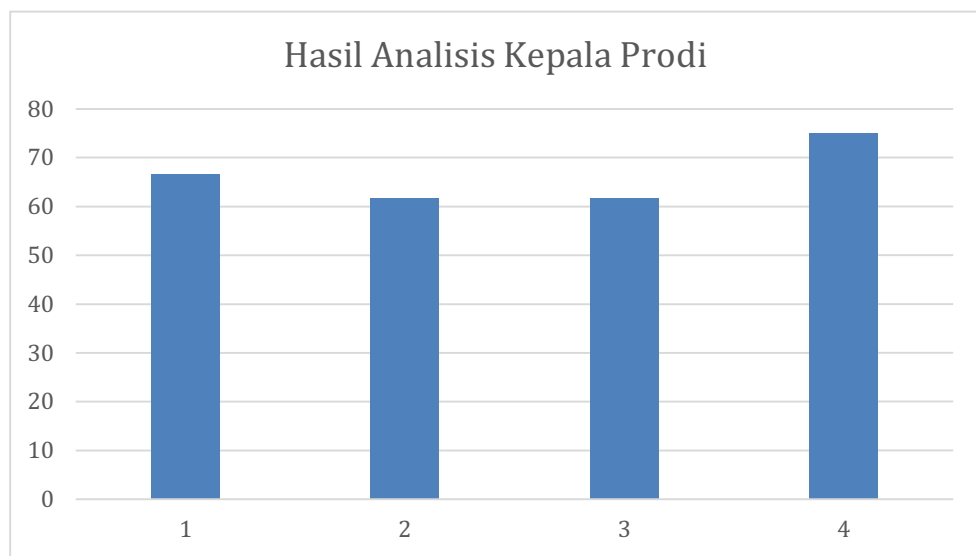
No	Nama	Item Jawaban										Skor	Nilai
		1	2	3	4	5	6	7	8	9	10		
1	Responden 1	4	4	4	4	3	5	5	5	5	4	43	86
2	Responden 2	4	3	3	2	3	2	4	4	1	3	29	58
3	Responden 3	4	4	4	5	5	5	4	4	4	5	44	88
4	Responden 4	2	4	2	2	2	4	4	4	2	3	29	58
5	Responden 5	5	4	3	3	3	5	5	5	5	3	41	82
6	Responden 6	5	5	5	5	1	5	5	5	1	1	38	76
7	Responden 7	5	5	5	5	3	5	5	5	2	1	41	82
8	Responden 8	4	3	2	2	2	3	4	4	3	3	30	60
9	Responden 9	3	5	3	3	5	5	3	4	3	4	38	76
10	Responden 10	4	4	4	3	4	4	4	4	4	4	39	78
11	Responden 11	4	4	3	3	3	3	4	4	4	3	35	70
Rata - rata												37	74

Tabel 3. Hasil Kuisisioner Mahasiswa

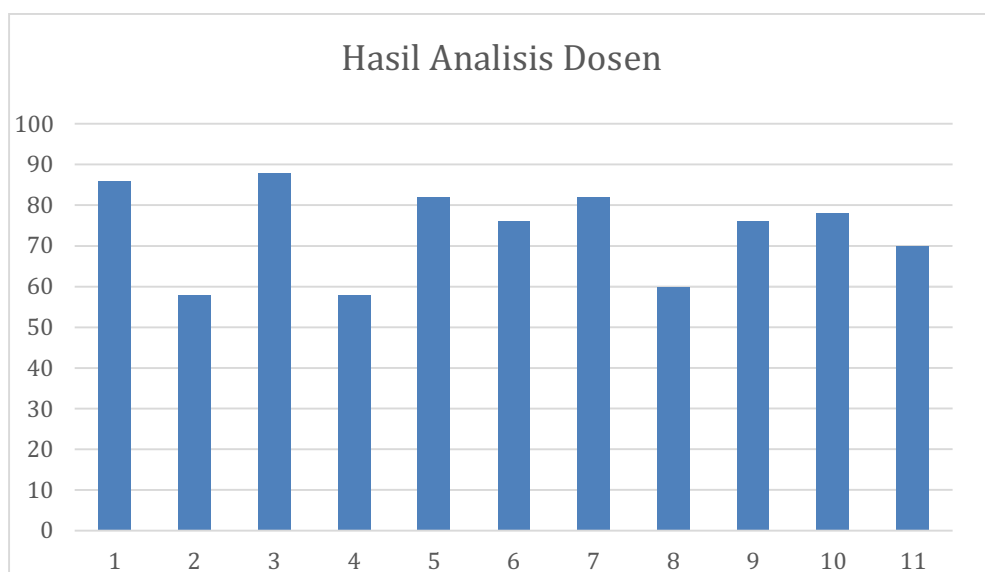
No	Nama	Item Jawaban										Skor	nilai
		1	2	3	4	5	6	7	8	9	10		
1	Responden 1	4	4	3	4	3	3	3	3	3	3	33	66
2	Responden 2	4	4	3	5	5	5	5	4	4	4	43	86
3	Responden 3	5	3	4	4	4	4	4	4	4	3	39	78
4	Responden 4	5	4	3	3	4	3	3	3	4	2	34	68
5	Responden 5	4	3	3	5	3	5	4	4	4	2	37	74
6	Responden 6	5	5	5	5	4	5	5	5	5	3	47	94
7	Responden 7	4	4	4	5	5	4	4	4	5	4	43	86
8	Responden 8	4	4	4	4	4	5	4	4	4	2	39	78

9	Responden 9	4	5	5	4	5	5	5	3	5	5	46	92
10	Responden 10	4	4	4	5	5	5	5	5	5	5	47	94
11	Responden 11	5	4	1	5	5	5	1	5	3	5	39	78
12	Responden 12	5	4	3	4	3	4	3	4	3	3	36	72
13	Responden 13	5	5	5	4	4	5	5	4	5	2	44	88
14	Responden 14	5	3	4	5	4	5	3	4	4	1	38	76
15	Responden 15	5	4	4	3	4	3	3	2	4	4	36	72
16	Responden 16	5	3	3	4	3	5	2	2	2	3	32	64
17	Responden 17	4	3	4	5	4	5	3	5	4	3	40	80
18	Responden 18	4	3	4	4	4	5	4	4	4	2	38	76
19	Responden 19	4	4	3	3	3	4	4	3	4	3	35	70
20	Responden 20	5	2	4	4	4	4	4	3	4	2	36	72
21	Responden 21	4	3	3	4	4	3	4	4	4	2	35	70
22	Responden 22	5	4	5	3	4	5	5	4	4	2	41	82
23	Responden 23	5	4	5	5	4	5	5	5	5	1	44	88
24	Responden 24	5	4	1	5	4	5	1	4	2	5	36	72
25	Responden 25	3	3	3	3	3	3	3	3	3	3	30	60
26	Responden 26	1	2	2	1	2	1	2	2	2	3	18	36
27	Responden 27	4	3	3	5	3	5	3	4	3	1	34	68
28	Responden 28	5	5	5	5	5	5	5	5	5	1	46	92
29	Responden 29	4	3	3	5	4	4	4	4	4	3	38	76
30	Responden 30	5	4	5	3	4	5	4	4	4	3	41	82
31	Responden 31	5	5	5	5	5	5	5	5	5	5	50	100
32	Responden 32	5	4	4	5	4	5	4	4	4	4	43	86
33	Responden 33	4	4	3	4	4	5	3	4	4	4	39	78
34	Responden 34	4	4	4	4	4	4	4	4	4	4	40	80
35	Responden 35	5	3	4	5	3	5	4	4	3	2	38	76
36	Responden 36	3	4	3	5	3	5	3	4	4	4	38	76
37	Responden 37	5	5	4	3	4	3	4	4	4	2	38	76
38	Responden 38	5	5	5	5	5	5	5	5	5	5	50	100
39	Responden 39	4	3	4	5	3	5	5	4	4	2	39	78
40	Responden 40	5	5	5	5	5	5	3	5	4	2	44	88
41	Responden 41	5	4	4	5	5	5	4	5	1	3	41	82
42	Responden 42	5	5	5	5	5	4	4	4	4	5	46	92
43	Responden 43	4	4	3	5	4	4	3	2	4	4	37	74
44	Responden 44	5	4	4	5	4	4	4	5	5	4	44	88
45	Responden 45	5	4	4	5	3	5	4	4	5	2	41	82
46	Responden 46	5	4	3	4	4	4	4	5	4	2	39	78
47	Responden 47	4	2	4	3	4	5	5	5	4	4	40	80
48	Responden 48	4	4	4	4	4	4	4	4	4	4	40	80
49	Responden 49	5	5	3	5	5	5	3	5	3	3	42	84
50	Responden 50	5	3	3	5	2	5	3	5	4	1	36	72
51	Responden 51	4	4	4	4	4	4	4	4	4	2	38	76
52	Responden 52	5	4	4	5	5	5	4	5	5	2	44	88

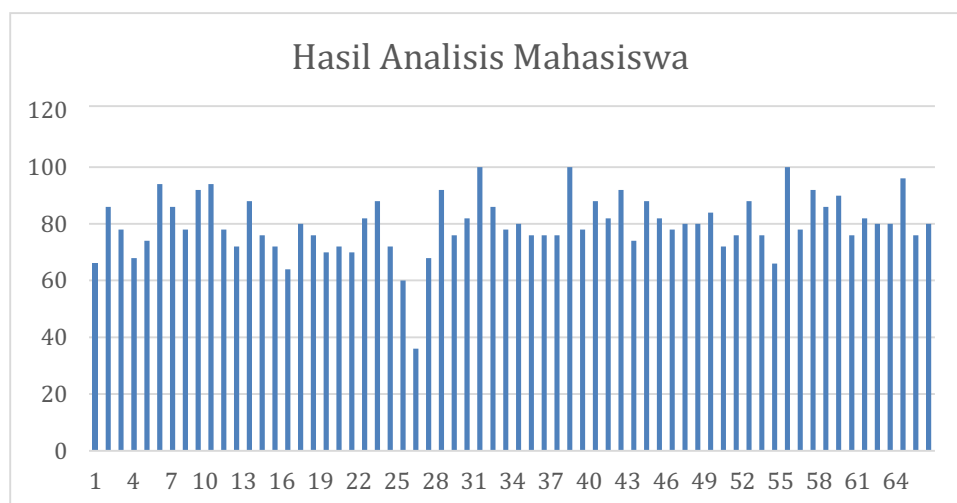
53	Responden 53	5	4	4	5	4	5	4	2	4	1	38	76
54	Responden 54	5	2	3	5	2	5	3	3	3	2	33	66
55	Responden 55	5	5	5	5	5	5	5	5	5	5	50	100
56	Responden 56	5	4	3	4	4	4	4	4	4	3	39	78
57	Responden 57	5	4	5	5	5	5	5	5	5	2	46	92
58	Responden 58	5	4	3	5	4	5	5	4	4	4	43	86
59	Responden 59	5	5	5	5	4	5	4	4	4	4	45	90
60	Responden 60	4	3	4	4	4	4	4	4	3	4	38	76
61	Responden 61	5	3	5	3	4	4	4	5	4	4	41	82
62	Responden 62	4	4	4	4	4	4	4	4	4	4	40	80
63	Responden 63	4	4	4	5	5	4	3	4	3	4	40	80
64	Responden 64	5	5	5	5	4	5	5	4	5	5	48	96
65	Responden 65	5	3	3	4	4	4	3	4	4	4	38	76
66	Responden 66	5	4	4	5	4	5	4	3	5	1	40	80
Rata-rata												39,86364	79,72727



Gambar 1. Hasil Kuisisioner Kepala Prodi



Gambar 2. Hasil Kuisiioner Dosen



Gambar 3. Hasil Kuisiioner mahasiswa

Evaluasi Penggunaan ISO 27001 di Sistem Akademik Universitas

Penelitian ini mengonfirmasi bahwa penerapan ISO 27001 adalah pendekatan yang efektif untuk meningkatkan keamanan data dalam konteks sistem akademik Universitas. Standar ini memberikan pedoman yang komprehensif untuk mengidentifikasi, mengelola, dan mengurangi risiko keamanan informasi. Penggunaan ISO 27001 membantu Universitas dalam memahami aktiva informasi yang perlu dilindungi, mengidentifikasi ancaman dan kerentanannya, dan menyusun rencana aksi yang lebih efektif untuk mengurangi risiko.

Analisis Risiko

Evaluasi risiko merupakan langkah kritis dalam penerapan ISO 27001. Penelitian ini telah mengidentifikasi berbagai jenis risiko yang terkait dengan sistem akademik Universitas, termasuk risiko terhadap data pribadi mahasiswa, data akademik, dan informasi administratif. Risiko tersebut meliputi ancaman siber seperti serangan peretasan, malware, dan phishing, serta risiko fisik seperti kehilangan data akibat bencana alam atau perangkat keras yang rusak.

Penerapan Pengendalian Keamanan

Hasil penelitian ini menunjukkan bahwa Universitas telah mengimplementasikan sejumlah pengendalian keamanan informasi yang sesuai berdasarkan standar ISO 27001. Pengendalian tersebut mencakup enkripsi data, pengaturan akses yang ketat, pemantauan lalu lintas jaringan, otentikasi ganda, dan prosedur penanganan insiden keamanan. Pengendalian ini berkontribusi secara signifikan pada peningkatan keamanan data dalam sistem akademik Universitas.

Dampak pada Keamanan Data

Penerapan ISO 27001 dalam sistem akademik Universitas telah memberikan dampak positif pada keamanan data. Dengan pengurangan risiko yang efektif dan penerapan pengendalian keamanan yang tepat, Universitas telah berhasil mengurangi insiden pelanggaran keamanan dan menjaga integritas data akademik. Hal ini memberikan keyakinan bagi mahasiswa, dosen, dan staf administratif bahwa data mereka dalam lingkungan akademik Universitas aman dan dilindungi.

KESIMPULAN

Hasil dari penelitian sistem akademik dengan ISO 27100 menunjukkan bahwa keamanan akademik merupakan aspek penting dalam pengelolaan sistem akademik. Hasil penelitian ini memberikan pemahaman bahwa perlu untuk selalu meningkatkan keamanan akademik, dan perlu mengimplementasikan standar ISO 27100 sebagai panduan yang dapat membantu meningkatkan keamanan sistem akademik.

Penelitian juga menunjukkan bahwa di lingkungan Universitas (Universitas), upaya untuk menjaga keamanan sistem akademik sudah berjalan dengan baik. Ini menandakan bahwa Universitas telah mengambil langkah-langkah yang cukup efektif dalam melindungi data

akademik dan menjaga integritas sistem akademik mereka.

Namun, perlu dicatat bahwa keamanan siber adalah hal yang terus berubah, dan serangan siber terus berkembang. Oleh karena itu, hasil penelitian ini juga menegaskan bahwa perbaikan dan peningkatan keamanan sistem akademik harus menjadi upaya berkelanjutan. Universitas, serta lembaga pendidikan lainnya, harus tetap memantau tren keamanan siber terbaru, merancang kebijakan keamanan yang sesuai, dan melibatkan staf yang kompeten dalam upaya menjaga integritas dan kerahasiaan data akademik.

Dalam rangka mencapai tujuan ini, implementasi standar ISO 27100 dapat menjadi landasan yang kuat untuk membantu menjaga keamanan sistem akademik, memitigasi risiko, dan meningkatkan resiliensi terhadap potensi ancaman siber di masa depan.

DAFTAR PUSTAKA

- Abdullah, A.N., et al. (2019). Information security practices in Malaysian University medical center. *IJHISI*, 14(2), 44-54. <https://doi.org/10.4018/IJHISI.2019040103>
- Cheung, R. et al. (2021). Phishing and ransomware attacks on Hong Kong universities during the COVID-19 pandemic. *JCS*, 37(6), 753-765. <https://doi.org/10.1108/JCS-05-2020-0090>.
- Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for information security management. *Journal of Information Security*, 4(2).
- Fatmawati, E.D. et al. (2022). Challenges in implementing ISO 27001 in Indonesian universities. *IEEE Access*, 10, 23272-23292. <https://doi.org/10.1109/ACCESS.2022.3152698>
- Haris, L. (2018, August). Risk Assessment on Information Asset an academic Application Using ISO 27001. In *2018 6th International Conference on Cyber and IT Service Management (CITSM)* (pp. 1-4). IEEE.
- Itradat, A., Sultan, S., Al-Junaidi, M., Qaffaf, R., Mashal, F., & Daas, F. (2014). Developing an ISO27001 Information Security Management System for an Educational Institute: Hashemite University as a Case Study. *Jordan Journal of Mechanical & Industrial Engineering*, 8(2).
- Khan, M.S.M. et al. (2020). Information security awareness training for university students. *IJCSNS*, 20(1), 137-145. http://paper.ijcsns.org/07_book/20200101/2020010120.pdf

Lee, J.K., & Lee, W.J. (2022). Blockchain based access control for campus information systems. *Electronics*, 11(3),501. <https://doi.org/10.3390/electronics11030501>.

Mat, S.N.S. et al. (2020). Data breach notification model for Malaysian universities. *F1000Research*, 9,1135. <https://doi.org/10.12688/f1000research.25619.1>

Mustafa, S.A. et al. (2019). Information security governance practices in Malaysian public universities. *IJACSA*, 10(2), 459-465. <https://doi.org/10.14569/IJACSA.2019.0100262>.

Pang, J.S. et al. (2022). Insider threats in universities and mitigation strategies. *SN Computer Science*, 3(2). <https://doi.org/10.1007/s42979-022-01118-9>

Permana, A. et al. (2023). ISO 27001 implementation framework for Indonesia higher education institutions. *Journal of Physics: Conference Series*, 2217(1). <https://doi.org/10.1088/1742-6596/2217/1/012048>.

Pritasari, K. et al. (2021). Readiness and implementation of ISO 27001 on information security management system in Indonesia universities. *CommIT Journal*, 15(1), 19-26. <https://doi.org/10.21512/commit.v15i1.7148>.

Rahman, A. et al. (2021). A review of information security policies and guidelines in higher education institutions. *Heliyon*, 7(3). <https://doi.org/10.1016/j.heliyon.2021.e06467>.

Rozak, F. et al. (2020). Benefits of implementing ISO 27001 in a university: A case study in Indonesia. *2020 International Conference on Information Management and Technology (ICIMTech)*. <https://doi.org/10.1109/ICIMTech50083.2020.9211016>.

Situmorang, M.S. et al. (2020). Information security risk analysis based on ISO27001:2013 in the academic information system. *CommIT Journal*, 14(1), 19- 24. <https://doi.org/10.21512/commit.v14i1.6456>.

Susanto, H., & Mukhlash, I. (2021). Information security awareness level of university students. *Library Hi Tech News*, 38(4), 7-12. <https://doi.org/10.1108/LHTN-10-2020-0098>.

Susanto, H. et al. (2019). Developing information security management system standards for Indonesian university. *ISASE 2019*. <https://doi.org/10.1109/ISASE47356.2019.9106132>.

- Susanto, H. et al. (2020). Information security management system with risk management at higher education. 2020 International Conference on Information Management and Technology (ICIMTech). <https://doi.org/10.1109/ICIMTech50083.2020.9210999>.
- Wang, T. et al. (2020). Security vulnerabilities of campus network and securityreinforcement suggestions. Procedia Computer Science, 166, 597-602. <https://doi.org/10.1016/j.procs.2020.02.085>.