ANALISIS KEPATUHAN KEBIJAKAN KEAMANAN INFORMASI BERDASARKAN TREN KEAMANAN DAN PRIVASI DENGAN *PROTECTION MOTIVATION THEORY*

TUGAS AKHIR

Diajukan Sebagai Salah Satu Syarat
untuk Memperoleh Gelar Sarjana Komputer pada
Program Studi Sistem Informasi

Oleh:

RAHMAT AFRIYANTO
12250314432

UIN SUSKA RIAU

FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI SULTAN SYARIF KASIM RIAU
PEKANBARU
2026

LEMBAR PERSETUJUAN

ANALISIS KEPATUHAN KEBIJAKAN KEAMANAN INFORMASI BERDASARKAN TREN KEAMANAN DAN PRIVASI DENGAN *PROTECTION MOTIVATION THEORY*

TUGAS AKHIR

Oleh:

RAHMAT AFRIYANTO
12250314432

Telah diperiksa dan disetujui sebagai Laporan Tugas Akhir
di Pekanbaru, pada tanggal 20 Januari 2026

Ketua Program Studi	Pembimbing
Angraini, S.Kom., M.Eng., Ph.D.	**Syaifullah, SE., M.Sc.**
NIP. 198408212009012008	**NIP. 198012152009121002**

LEMBAR PENGESAHAN

ANALISIS KEPATUHAN KEBIJAKAN KEAMANAN INFORMASI BERDASARKAN TREN KEAMANAN DAN PRIVASI DENGAN *PROTECTION MOTIVATION THEORY*

TUGAS AKHIR

Oleh:

RAHMAT AFRIYANTO
12250314432

Telah dipertahankan di depan sidang dewan penguji
sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer
Fakultas Sains dan Teknologi Universitas Islam Negeri Sultan Syarif Kasim Riau
di Pekanbaru, pada tanggal 14 Januari 2026

Pekanbaru, 14 Januari 2026
Mengesahkan,

Dekan	Ketua Program Studi
Dr. Yuslenita Muda, S.Si., M.Sc.	**Angraini, S.Kom., M.Eng., Ph.D.**
NIP. 197701032007102001	**NIP. 198408212009012008**

DEWAN PENGUJI:

Ketua : **Eki Saputra, S.Kom., M.Kom.**

Sekretaris : **Syaifullah, SE., M.Sc.**

Anggota 1 : **Mona Fronita, S.Kom., M.Kom.**

Anggota 2 : **Angraini, S.Kom, M.Eng., Ph.D.**

Lampiran Surat :
Nomor : Nomor 25/2021
Tanggal : 10 September 2021

SURAT PERNYATAAN

Saya yang bertandatangan di bawah ini:

Nama : RAHMAT AFRIYANTO
NIM : 12250314432
Tempat/Tgl. Lahir : Pekanbaru, 29 September 2003
Fakultas/Pascasarjana : Sains dan Teknologi
Prodi : Sistem Informasi
Judul Disertasi/Thesis/Skripsi/Karya Ilmiah lainnya*:
ANALISIS KEPATUHAN KEBIJAKAN KEAMANAN INFORMASI BERDASARKAN TREN KEAMANAN DAN PRIVASI DENGAN PROTECTION MOTIVATION THEORY

Menyatakan dengan sebenar-benarnya bahwa :

1. ~~Penulisan Disertasi~~/~~Thesis~~/Skripsi/~~Karya Ilmiah lainnya~~* dengan judul sebagaimana tersebut di atas adalah hasil pemikiran dan penelitian saya sendiri.
2. Semua kutipan pada karya tulis saya ini sudah disebutkan sumbernya.
3. Oleh karena itu ~~Disertasi~~/~~Thesis~~/Skripsi/~~Karya Ilmiah lainnya~~* saya ini, saya nyatakan bebas dari plagiat.
4. Apa bila dikemudian hari terbukti terdapat plagiat dalam penulisan ~~Disertasi/Thesis~~/Skripsi/(~~Karya Ilmiah lainnya~~)* saya tersebut, maka saya besedia menerima sanksi sesua peraturan perundang-undangan.

Demikianlah Surat Pernyataan ini saya buat dengan penuh kesadaran dan tanpa paksaan dari pihak manapun juga.

Pekanbaru, 22 Januari 2026
Yang membuat pernyataan

RAHMAT AFRIYANTO
NIM : 12250314432

pilih salah satu sasuai jenis karya tulis

LEMBAR HAK ATAS KEKAYAAN INTELEKTUAL

Tugas Akhir yang tidak diterbitkan ini terdaftar dan tersedia di Perpustakaan Universitas Islam Negeri Sultan Syarif Kasim Riau adalah terbuka untuk umum, dengan ketentuan bahwa hak cipta ada pada peneliti. Referensi kepustakaan diperkenankan dicatat, tetapi pengutipan atau ringkasan hanya dapat dilakukan atas izin peneliti dan harus dilakukan mengikuti kaedah dan kebiasaan ilmiah serta menyebutkan sumbernya.

Penggandaan atau penerbitan sebagian atau seluruh Tugas Akhir ini harus memperoleh izin tertulis dari Dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Sultan Syarif Kasim Riau. Perpustakaan dapat meminjamkan Tugas Akhir ini untuk anggotanya dengan mengisi nama, tanda peminjaman, dan tanggal pinjam pada *form* peminjaman.

LEMBAR PERNYATAAN

Dengan ini saya menyatakan bahwa dalam Tugas Akhir ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu Perguruan Tinggi, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan di dalam daftar pustaka.

Pekanbaru, 20 Januari 2026
Yang membuat pernyataan,

RAHMAT AFRIYANTO
NIM. 12250314432

LEMBAR PERSEMBAHAN

Assalamu'alaikum Warahmatullahi Wabarakatuh.

Alhamdulillahi Rabbil 'Alamin, segala puji bagi Allah *Subhanahu Wa Ta'ala* sebagai bentuk rasa syukur atas segala nikmat yang telah diberikan tanpa ada kekurangan sedikitpun. Shalawat beserta salam tidak lupa pula kita ucapkan kepada Nabi Muhammad *Shallallahu 'Alaihi Wa Sallam* dengan mengucapkan *Allahumma Sholli'ala Sayyidina Muhammad Wa'ala Ali Sayyidina Muhammad*. Semoga kita semua selalu senantiasa mendapat syafaat-Nya di dunia maupun di akhirat, *Aamiin Ya Rabbal'alaamiin*.

Tugas Akhir ini peneliti persembahkan sebagai bentuk rasa cinta dan hormat kepada kedua orang tua tercinta, Ayahanda Afrizal dan Ibunda Triwati yang dengan penuh kesabaran dan pengorbanan mendampingi serta mendorong peneliti hingga berhasil menempuh pendidikan tinggi. Ucapan terima kasih juga peneliti sampaikan kepada kakak-kakak tercinta, Septiani Afrianti, dan Putri Sa'ban atas segala do'a, dukungan, dan semangat yang senantiasa mengiringi langkah peneliti hingga penelitian ini dapat terselesaikan dengan baik. Pencapaian ini tak terlepas dari didikan dan bimbingan yang mereka berikan sepanjang perjalanan hidup peneliti. Semoga Allah *Subhanahu Wa Ta'ala* membalas segala kebaikan mereka dengan keberkahan yang melimpah.

Peneliti juga menyampaikan apresiasi dan rasa terima kasih yang sebesarbesarnya kepada seluruh Dosen Program Studi Sistem Informasi atas ilmu, bimbingan, dan pengalaman berharga yang telah diberikan selama masa perkuliahan. Ucapan terima kasih yang tulus juga peneliti sampaikan kepada sahabat-sahabat terdekat yang telah menjadi bagian penting dalam perjalanan ini kebersamaan kalian menjadikan masa studi lebih berwarna dan bermakna. Semoga segala kebaikan yang telah diberikan dibalas oleh Allah *Subhanahu Wa Ta'ala* dengan limpahan keberkahan dan rahmat-Nya.

Wassalamu'alaikum Warahmatullahi Wabarakatuh.

KATA PENGANTAR

Alhamdulillahi Rabbil 'Alamin, segala puji hanya bagi Allah *Subhanahu Wa Ta'ala* atas limpahan rahmat, taufik, dan hidayah-Nya sehingga Peneliti dapat menuntaskan penyusunan Tugas Akhir ini. Shalawat beserta salam senantiasa tercurah kepada junjungan Nabi Muhammad *Shallallahu 'Alaihi Wa Sallam*, keluarga, serta para sahabat beliau. Dengan penuh rasa syukur, Tugas Akhir ini disusun sebagai salah satu persyaratan untuk memperoleh gelar Sarjana Komputer pada Program Studi Sistem Informasi Universitas Islam Negeri Sultan Syarif Kasim Riau.

Dalam proses penyusunan Tugas Akhir ini, peneliti telah menerima banyak dukungan, bimbingan dan bantuan dari berbagai pihak. Oleh karena itu, dengan penuh rasa hormat Peneliti menyampaikan terima kasih yang sebesar-besarnya kepada:

1. Ibu Prof. Dr. Hj. Leny Nofianti MS, SE., M.Si., Ak., CA sebagai Rektor Universitas Islam Negeri Sultan Syarif Kasim Riau.
2. Ibu Dr. Yuslenita Muda, S.Si., M.Sc sebagai Dekan Fakultas Sains dan Teknologi.
3. Ibu Angraini, S.Kom., M.Eng., Ph.D sebagai Ketua Program Studi Sistem Informasi sekaligus Penguji Kedua yang telah banyak memberikan arahan, nasihat, serta masukan dalam penyelesaian Tugas Akhir ini.
4. Ibu Dr. Rice Novita, S.Kom., M.Kom sebagai Sekretaris Program Studi Sistem Informasi.
5. Bapak Syaifullah, SE., M.Sc sebagai dosen pembimbing Tugas Akhir ini yang telah memberikan bimbingan, arahan, motivasi, dan masukan yang sangat berharga dalam penyusunan Tugas Akhir ini, sehingga peneliti dapat menyelesaikannya dengan baik.
6. Bapak Muhammad Jazman, S.Kom., M.Infosys sebagai Kepala Laboratorium Program Studi Sistem Informasi.
7. Ibu Fitriani Muttakin, S.Kom., M.Cs sebagai Dosen Pembimbing Akademik yang telah memberikan bimbingan, arahan, masukan, serta motivasi kepada peneliti sejak awal perkuliahan hingga penyusunan Tugas Akhir ini.
8. Ibu Mona Fronita, S.Kom., M.Kom sebagai Dosen Penguji Pertama yang telah banyak memberikan arahan, nasihat, serta masukan dalam penyelesaian Tugas Akhir ini sehingga hasilnya menjadi lebih baik.
9. Bapak Anofrizen, S.Kom., M.Kom sebagai Dosen Pembimbing Kerja Praktek.

10. Bapak dan Ibu Dosen Program Studi Sistem Informasi Fakultas Sains dan Teknologi Universitas Islam Negeri Sultan Syarif Kasim Riau yang telah memberikan ilmu dan wawasannya kepada peneliti selama perkuliahan.
11. Orang tua peneliti tercinta, Ayahanda Afrizal dan Ibunda Triwati yang selalu memberikan dukungan dan doa kepada peneliti dari awal perkuliahan hingga penyusunan Tugas Akhir ini. Semoga Allah membalas setiap kebaikan, pengorbanan dan doa Ayahanda serta Ibunda dengan limpahan rahmat dan keberkahan yang tiada terhingga.
12. Kedua kakak peneliti yang senantiasa memberikan dukungan moril dan materil kepada peneliti selama perkuliahan yang sangat berjasa bagi peneliti.
13. Sahabat seperjuangan semasa kuliah yaitu Hafiz Aryan Siregar, Novrian Pratama, Dani Harmade, Ahmeid Aqeil, Fajri Nurhadi, Hapid Ramdani, dan Erliandika Syahputra yang telah berada di sisi saya di saat susah, senang, dan sedih. Dengan adanya mereka peneliti terus termotivasi dalam mengejar karir dan dapat menyelesaikan pendidikan ini berkat bantuan mereka.
14. Teman-teman Angkatan 2022 yang telah menjadi sahabat seperjuangan, senantiasa memberikan dukungan, serta bersama-sama berusaha mewujudkan visi, misi, dan tujuan diri.
15. Semua pihak yang tidak dapat disebutkan satu-persatu, yang telah memberikan kontribusi secara langsung maupun tidak langsung dalam menyelesaikan Tugas Akhir ini.

Semoga segala doa dan dorongan yang telah diberikan selama ini menjadi amal kebajikan dan mendapat balasan setimpal dari *Allah Subhanahu Wa Ta'ala*. Peneliti menyadari bahwa penulisan Tugas Akhir ini masih terdapat kekurangan dan jauh dari kata sempurna. Peneliti berharap untuk kritik dan saran yang membangun yang dapat disampaikan melalui e-mail 12250314432@students.uin-suska.ac.id atau rahmatafriyanto6@gmail.com untuk Tugas Akhir ini. Diharapkan Tugas Akhir ini dapat memberikan manfaat kepada pembaca, *Aamiin*.

Pekanbaru, 20 Januari 2026

Peneliti,

RAHMAT AFRIYANTO

NIM. 12250314432

ANALISIS KEPATUHAN KEBIJAKAN KEAMANAN INFORMASI BERDASARKAN TREN KEAMANAN DAN PRIVASI DENGAN *PROTECTION MOTIVATION THEORY*

RAHMAT AFRIYANTO
NIM: 12250314432

Tanggal Sidang: 14 Januari 2026
Periode Wisuda:

Program Studi Sistem Informasi
Fakultas Sains dan Teknologi
Universitas Islam Negeri Sultan Syarif Kasim Riau
Jl. Soebrantas, No. 155, Pekanbaru

ABSTRAK

Keamanan informasi menjadi isu yang semakin krusial seiring meningkatnya ketergantungan organisasi, termasuk institusi pendidikan tinggi, terhadap sistem informasi. Meskipun kebijakan keamanan informasi telah diterapkan, peningkatan serangan siber serta rendahnya kepatuhan pengguna masih menjadi permasalahan yang signifikan. Penelitian ini bertujuan untuk mengukur tingkat kepatuhan terhadap kebijakan keamanan informasi di lingkungan universitas dengan mengadopsi kerangka kerja *Protection Motivation Theory* (PMT). Model penelitian menguji pengaruh *Perceived Severity, Perceived Vulnerability, Perceived Response Efficacy, Perceived Self-Efficacy,* dan *Perceived Response Cost* terhadap *Compliance with Information Security Policy*. Data dikumpulkan melalui survei kuesioner dan dianalisis menggunakan metode *Structural Equation Modeling–Partial Least Squares* (SEM-PLS). Hasil pengujian hipotesis menunjukkan bahwa *Perceived Severity* berpengaruh positif dan signifikan terhadap kepatuhan kebijakan keamanan informasi, sedangkan *Perceived Response Cost* berpengaruh negatif dan signifikan. Sementara itu, *Perceived Vulnerability*, *Response Efficacy*, dan *Self-Efficacy* tidak menunjukkan pengaruh yang signifikan. Temuan ini mengindikasikan bahwa persepsi terhadap tingkat keparahan ancaman dan hambatan dalam penerapan perilaku keamanan lebih dominan dalam memengaruhi kepatuhan pengguna dibandingkan faktor efikasi. Penelitian ini diharapkan dapat menjadi dasar bagi institusi pendidikan tinggi dalam merancang strategi kebijakan dan program peningkatan kepatuhan keamanan informasi yang lebih efektif.

Kata Kunci: Keamanan Informasi, Kepatuhan Kebijakan, *Protection Motivation Theory*, SEM-PLS, Universitas

ANALYSIS OF INFORMATION SECURITY POLICY COMPLIANCE BASED ON SECURITY AND PRIVACY TRENDS USING PROTECTION MOTIVATION THEORY

RAHMAT AFRIYANTO
NIM: 12250314432

Date of Final Exam: January 14th 2026
Graduation Period:

Department of Information System
Faculty of Science and Technology
State Islamic University of Sultan Syarif Kasim Riau
Soebrantas Street, No. 155, Pekanbaru

ABSTRACT

Information security has become an increasingly crucial issue as organizations, including higher education institutions, have become more dependent on information systems. Although information security policies have been implemented, the increase in cyber attacks and low user compliance remain significant problems. This study aims to measure the level of compliance with information security policies in a university environment by adopting the Protection Motivation Theory (PMT) framework. The research model tests the influence of Perceived Severity, Perceived Vulnerability, Perceived Response Efficacy, Perceived Self-Efficacy, and Perceived Response Cost on Compliance with Information Security Policy. Data were collected through a questionnaire survey and analyzed using the Structural Equation Modeling–Partial Least Squares (SEM-PLS) method. The results of hypothesis testing show that Perceived Severity has a positive and significant effect on compliance with information security policies, while Perceived Response Cost has a negative and significant effect. Meanwhile, Perceived Vulnerability, Response Efficacy, and Self-Efficacy did not show a significant effect. These findings indicate that perceptions of the severity of threats and barriers to implementing security behaviors are more dominant in influencing user compliance than efficacy factors. This study is expected to serve as a basis for higher education institutions in designing more effective information security compliance policy and program improvement strategies.

Keywords: *Information Security, Policy Compliance, Protection Motivation Theory, SEM-PLS, University*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR SINGKATAN

SLR	:	*Systematic Literature Review*
USB	:	*Universal Serial Bus*
PMT	:	*Protection Motivation Theory*
SEM-PLS	:	*Structural Equation Modeling–Partial Least Squares*
UMISPC	:	*Unified Model of Information Security Policies Compliance*
CIA	:	*Confidentiality, Integrity, Availability*
DoS	:	*Denial of Service*
GDPR	:	*General Data Protection Regulation*
PII	:	*Personally Identifiable Information*
WoS	:	*Web of Science*
AVE	:	*Average Variance Extracted*
VIF	:	*Variance Inflation Factor*
PS	:	*Perceived Severity*
PV	:	*Perceived Vulnerability*
RC	:	*Response Cost*
RE	:	*Response Efficacy*
SE	:	*Self-Efficacy*
CISP	:	*Compliance with Information Security Policy*
CA	:	*Cronbach's alpha*
CR	:	*Composite Reliability*

BAB 1
PENDAHULUAN

1.1 Latar Belakang

Perkembangan penelitian di bidang keamanan informasi dan privasi berlangsung sangat dinamis sehingga diperlukan pendekatan yang sistematis untuk memetakan arah dan tren riset secara komprehensif (Kraus, Breier, dan Dasí-Rodríguez, 2020). *Systematic Literature Review* (SLR) merupakan metode yang banyak digunakan untuk mengidentifikasi dan mengevaluasi hasil penelitian terdahulu secara terstruktur guna menemukan pola, tema dominan, serta celah penelitian yang masih terbuka (Lim, Kumar, dan Ali, 2022). Dalam praktiknya, pendekatan SLR sering dipadukan dengan analisis bibliometrik yang memungkinkan pemetaan kuantitatif terhadap publikasi ilmiah, seperti analisis kata kunci, klaster tematik, serta jaringan sitasi dan kolaborasi penulis (Passas, 2024). Melalui kombinasi kedua pendekatan tersebut, tren penelitian keamanan dan privasi dapat diidentifikasi secara lebih objektif, terukur, dan berbasis data (Donthu, Kumar, Mukherjee, Pandey, dan Lim, 2021). Oleh karena itu, penelitian ini terlebih dahulu melakukan analisis tren menggunakan metode bibliometric sebagai dasar konseptual dalam merumuskan model penelitian empiris mengenai kepatuhan kebijakan keamanan informasi (Patricia, Sánchez, Moya, Gabriela, dan Giner, 2024).

Hasil pemetaan tren penelitian tersebut menunjukkan bahwa isu keamanan informasi dan privasi semakin mendapatkan perhatian seiring meningkatnya ketergantungan organisasi terhadap sistem informasi (Komara, Rohman, Rahmawaty, Giovanni, dan Mumtaz, 2025). Sistem Informasi telah berkembang menjadi aset vital karena fungsinya yang krusial dalam menyimpan data dan aset organisasi yang bernilai (Qatawneh, 2024). Untuk melindungi aset tersebut, organisasi umumnya mengandalkan langkah-langkah keamanan teknis, mulai dari perangkat lunak antivirus, enkripsi, hingga sistem pemantauan yang komprehensif (Alkhudhayr, Alfarraj, Aljameeli, dan Elkhdiri, 2019; Koolen, Wuyts, Joosen, dan Valcke, 2024). Namun, sekadar mengandalkan solusi teknis terbukti tidak cukup untuk menjamin keamanan informasi secara menyeluruh (Gaurav, Jayaram, Halder, Panda, dan Kishore, 2022; Akello, 2024). Celah keamanan terbesar justru sering kali bersumber dari faktor perilaku manusia, khususnya ketidakpatuhan pengguna terhadap kebijakan keamanan informasi, yang kerap menjadi pintu masuk terjadinya insiden keamanan dan pelanggaran data yang serius (Al-Momani, Ramayah, dan Al-Sharafi, 2024; Kuzior, Arefieva, Vovk, dan Brożek, 2022).

Isu keamanan ini menjadi jauh lebih kompleks saat ditarik ke dalam lingkungan akademik, mengingat universitas memiliki tantangan tersendiri dalam memastikan keamanan informasi yang disimpan dan diproses (Angraini, Alinda Alias, dan Okfalisa, 2019). Sebagai institusi yang mengelola data dalam jumlah besar dan bersifat krusial, mulai dari data akademik hingga informasi sensitif lainnya, universitas kini menjadi target utama berbagai ancaman keamanan (Symantec, 2017). Laporan global menunjukkan bahwa sektor pendidikan termasuk salah satu sektor yang paling rentan terhadap insiden keamanan siber, di mana pada tahun 2025 terjadi peningkatan serangan *ransomware* dan pencurian data hingga 50% (NCSC, 2025). Selain ancaman eksternal, ancaman keamanan informasi yang berasal dari internal organisasi, baik yang disengaja maupun tidak, juga terus meningkat dan berpotensi mengganggu aktivitas organisasi secara keseluruhan, sehingga menegaskan pentingnya kepatuhan pengguna terhadap kebijakan keamanan informasi (AlGhamdi, Win, dan Vlahu-Gjorgievska, 2022).

Ironisnya, meskipun kebijakan keamanan informasi (Information Security Policy) sudah diberlakukan untuk melindungi data, efektivitasnya sering kali tumpul akibat perilaku pengguna itu sendiri (Koohang, Anderson, Nord, dan Paliszkiewicz, 2020). Demi alasan efisiensi atau kemudahan kerja, banyak individu yang memilih untuk mengabaikan prosedur keamanan (Alzamil, 2018). Praktik-praktik berisiko masih lazim ditemukan, seperti berbagi password dengan rekan kerja, menggunakan penyimpanan USB yang tidak aman, atau membiarkan komputer tidak terkunci saat ditinggalkan (Moody, Siponen, dan Pahnila, 2018). Fenomena ini menegaskan bahwa tanpa kepatuhan pengguna, teknologi keamanan secanggih apa pun akan sia-sia, karena manusia tetap menjadi titik terlemah dalam rantai keamanan.

Dalam upaya memahami dinamika kepatuhan pada industri yang memiliki risiko tinggi, (Alrawhani, Romli, dan Al-Sharafi, 2025) meneliti sektor perbankan di Yaman menggunakan kerangka kerja *Protection Motivation Theory* (PMT) dengan analisis PLS-SEM. Penelitian ini bertujuan untuk mengatasi inkonsistensi temuan pada studi-studi sebelumnya mengenai faktor motivasi perlindungan dengan menguji pengaruh penilaian ancaman dan penilaian penyesuaian. Hasil analisis mereka mengonfirmasi bahwa *perceived self-efficacy, response efficacy,* dan *severity* secara signifikan meningkatkan niat perilaku karyawan untuk mematuhi kebijakan, meskipun persepsi kerentanan *(vulnerability)* dan biaya respons *(response cost)* tidak terbukti berpengaruh signifikan dalam konteks tersebut (Alrawhani dkk., 2025).

Sementara itu, dalam perspektif yang lebih luas, (Alraja, Butt, dan Abbod, 2023) melakukan studi lintas negara yang melibatkan karyawan dari tujuh negara berbeda (seperti AS, Inggris, dan Malaysia) untuk memvalidasi model *Unified Model of Information Security Policies Compliance* (UMISPC). Studi ini merespons keterbatasan penelitian kepatuhan yang umumnya hanya berfokus pada satu wilayah geografis saja. Temuan mereka menyoroti bahwa rasa takut *(fear)* dan nilai peran *(role values)* adalah prediktor utama kepatuhan, namun faktor kebiasaan (habit) justru ditemukan tidak memiliki dampak signifikan terhadap niat kepatuhan, yang menandakan bahwa perilaku keamanan belum sepenuhnya menjadi rutinitas otomatis bagi karyawan global (Alraja dkk., 2023).

Lebih spesifik pada konteks institusi pendidikan tinggi, (Angraini, Alinda Alias, dan Okfalisa, 2019) melakukan survei pendahuluan yang menyoroti adanya kesenjangan nyata antara kesadaran manajemen dan perilaku operasional pengguna. Meskipun manajemen universitas menyadari pentingnya kepatuhan kebijakan untuk mengurangi insiden keamanan, studi ini mengungkap bahwa ketidakpatuhan pengguna masih sering terjadi dan banyak implementasi kebijakan yang tidak disertai dengan instrumen evaluasi yang memadai. Kesimpulan dari studi ini menegaskan bahwa universitas membutuhkan model yang tepat untuk mengevaluasi kepatuhan kebijakan keamanan informasi guna menutup celah keamanan yang ada (Angraini, Alinda Alias, dan Okfalisa, 2019).

Berdasarkan tren penelitian terkini, keamanan informasi menjadi isu yang semakin penting seiring dengan meningkatnya ketergantungan organisasi terhadap sistem informasi. Namun, pada institusi pendidikan tinggi justru masih ditemukan peningkatan serangan siber (NCSC, 2025), yang diperparah oleh adanya kesenjangan antara kesadaran manajemen dan perilaku pengguna dalam mematuhi kebijakan keamanan informasi (Angraini, Alinda Alias, dan Okfalisa, 2019). Kondisi ini menunjukkan bahwa ketidakpatuhan pengguna masih menjadi permasalahan krusial, sehingga diperlukan upaya evaluasi terhadap tingkat kepatuhan kebijakan keamanan informasi di lingkungan universitas.

Oleh karena itu, penelitian ini dilakukan untuk mengukur tingkat kepatuhan kebijakan keamanan informasi di lingkungan universitas sebagai upaya menjawab permasalahan tersebut. Penelitian ini mengadopsi kerangka kerja *Protection Motivation Theory* (PMT) karena kemampuannya yang komprehensif dalam menjelaskan bagaimana dua proses kognitif utama, yaitu penilaian ancaman (*threat appraisal*) dan penilaian penyesuaian (*coping appraisal*), memengaruhi motivasi perlindungan individu (Ogbanufe, Crossler, dan Biros, 2023). Dalam model penelitian

ini, diuji pengaruh variabel *Perceived Self-Efficacy, Perceived Response Efficacy, Perceived Response Cost, Perceived Vulnerability*, dan *Perceived Severity* terhadap kepatuhan kebijakan keamanan informasi. Pengumpulan data dilakukan melalui instrumen kuesioner survei yang selanjutnya dianalisis menggunakan metode *Structural Equation Modeling–Partial Least Squares* (SEM-PLS). Metode SEM-PLS dipilih karena efektif dalam menguji model teoritis yang kompleks sekaligus memprediksi hubungan antarvariabel secara akurat. (Alrawhani dkk., 2025).

1.2 Perumusan Masalah

Adapun rumusan masalah pada penelitian ini adalah:

1. Bagaimana menganalisis perkembangan dan tren isu keamanan dan privasi menggunakan *Bibliometric* melalui *software* Rstudio.
2. Bagaimana implementasi pengukuran kepatuhan kebijakan keamanan informasi di universitas dengan pendekatan *Protection Motivation Theory*.

1.3 Batasan Masalah

Batasan masalah Tugas Akhir ini adalah:

1. Penelitian ini menggunakan metode *Bibliometric* dari *software* RStudio.
2. Penelitian ini me-*review* artikel jurnal internasional dari *Database* Scopus.
3. Artikel yang digunakan adalah artikel tahun 2014 sampai 2024.
4. Penelitian ini dilakukan pada Pegawai di Fakultas Sains dan Teknologi Universitas Islam Negeri Sultan Syarif Kasim Riau seperti dosen dan tenaga kependidikan.
5. Penelitian ini menggunakan Metode *Protection Motivation Theory* (PMT).
6. Penelitian ini menggunakan *tools SmartPLS* dalam mengelola data.
7. Penelitian ini menggunakan Metode Kuantitatif dan *Simple Random Sampling* dalam melakukan pengambilan data.

1.4 Tujuan

Tujuan Tugas Akhir ini adalah:

1. Mengidentifikasi perkembangan isu keamanan dan privasi.
2. Mengukur kepatuhan kebijakan keamanan informasi pegawai di Fakultas Sains dan Teknologi di Universitas Islam Negeri Sultan Syarif Kasim Riau.

1.5 Manfaat

Manfaat Tugas Akhir ini adalah:

1. Menyediakan sebuah peta intelektual *(intellectual map)* yang komprehensif mengenai evolusi dan struktur bidang riset keamanan dan privasi.

2. Memberikan hasil dari tingkat kepatuhan kebijakan keamanan informasi pegawai di Fakultas Sains dan Teknologi di Universitas Islam Negeri Sultan Syarif Kasim Riau.

1.6 Sistematika Penulisan

Sistematika penulisan laporan adalah sebagai berikut:

BAB 1. PENDAHULUAN

BAB 1 pada Tugas Akhir ini berisi tentang latar belakang masalah, perumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitan, dan sistematika penulisan Tugas Akhir.

BAB 2. LANDASAN TEORI

BAB 2 pada Tugas Akhir ini berisi tentang teori-teori yang digunakan dalam penelitian ini.

BAB 3. METODOLOGI PENELITIAN

BAB 3 ini menjelaskan alur dari penelitian ini, yang mana penelitian ini dimulai dengan melakukan tahap perencanaan, tahap pengumpulan data, tahap pengolahan data, dan tahap analisis dan hasil.

BAB 4. HASIL DAN ANALISA

BAB 4 ini berisi tentang hasil dan analisa *Systematic Literature Review* perkembangan dan tren isu keamanan dan privasi, dan impelementasi tren berupa pengukuran tingkat kepatuhan kebijakan keamanan informasi. Bagian ini membahas pengaruh variabel-variabel dalam *Protection Motivation Theory* (seperti *threat appraisal* dan *coping appraisal*) terhadap perilaku kepatuhan pegawai di Fakultas Sains dan Teknologi.

BAB 5. PENUTUP

BAB 5 Tugas Akhir ini berisikan tentang kesimpulan dan saran dari penelitian.

BAB 2
LANDASAN TEORI

2.1 Keamanan Informasi

Landasan teoretis keamanan informasi adalah disiplin ilmu yang berfokus pada perlindungan aset informasi dari berbagai ancaman untuk menjamin kelangsungan bisnis, meminimalkan risiko, dan memaksimalkan laba atas investasi (Shoufan dan Damiani, 2017). Fondasi konseptual dari disiplin ini secara universal bertumpu pada Triad CIA (*Confidentiality, Integrity, Availability*), sebuah model yang mengartikulasikan tiga pilar utama perlindungan data (Lundgren dan Möller, 2017; De Oliveira Albuquerque, Villalba, Orozco, Buiati, dan Kim, 2014).

Kerahasiaan *(Confidentiality)* adalah prinsip yang memastikan bahwa informasi sensitif tidak diungkapkan atau tersedia bagi individu, entitas, atau proses yang tidak berwenang. Mekanisme utama untuk menegakkan kerahasiaan mencakup penggunaan kriptografi (enkripsi) untuk data saat disimpan *(at-rest)* dan saat dikirim *(in-transit)*, serta penerapan skema kontrol akses *(access control)* yang ketat (De Oliveira Albuquerque dkk., 2014).

Integritas *(Integrity)* merujuk pada penjagaan akurasi, konsistensi, dan kepercayaan *(trustworthiness)* data selama seluruh siklus hidupnya. Data tidak boleh diubah, dirusak, atau dihapus secara tidak sah atau tidak terdeteksi. Teknik yang umum digunakan untuk menjamin integritas data meliputi penggunaan fungsi *hash* (seperti SHA-256) dan tanda tangan digital *(digital signatures)* untuk memverifikasi bahwa data belum dimodifikasi (Chowdhury dkk., 2023).

Ketersediaan *(Availability)* adalah prinsip yang memastikan bahwa sistem, aplikasi, dan data dapat diakses serta digunakan oleh pengguna yang sah kapan pun dibutuhkan. Ini melibatkan perlindungan terhadap kegagalan sistem atau serangan yang bertujuan mengganggu layanan, seperti serangan *Denial of Service* (DoS). Strategi untuk menjamin ketersediaan seringkali mencakup implementasi redundansi perangkat keras, *failover clustering,* dan praktik pencadangan *(backup)* serta pemulihan bencana *(disaster recovery)* yang solid (De Oliveira Albuquerque dkk., 2014). Meskipun Triad CIA adalah inti, banyak literatur akademis memperluas model ini dengan menyertakan konsep-konsep tambahan seperti Keaslian *(Authenticity)*, Akuntabilitas *(Accountability)*, dan Tidak Dapat Disangkal *(Non-Repudiation)* untuk memberikan gambaran keamanan yang lebih komprehensif (Shoufan dan Damiani, 2017).

2.2 Privasi

Berbeda dari keamanan yang berfokus pada perlindungan data, privasi *(privacy)* adalah konsep multidisiplin mencakup hukum, etika, dan sistem informasi yang berpusat pada hak individu. Secara fundamental, privasi adalah hak untuk mengontrol informasi pribadi seseorang, sering disebut sebagai *Personally Identifiable Information* (PII) (Acquisti, Brandimarte, dan Loewenstein, 2015). Landasan teoretis modern privasi sering menjauh dari gagasan sekadar kerahasiaan (secrecy) dan lebih menekankan pada otonomi individu. Ini adalah hak atas determinasi mandiri informasional *(informational self-determination)*, yaitu kemampuan seseorang untuk menentukan sendiri kapan, bagaimana, dan sejauh mana informasi tentang dirinya dikomunikasikan kepada orang lain.

Privasi bukan sebagai satu hak tunggal, melainkan sebagai sekumpulan hak terkait yang dapat dilanggar melalui berbagai aktivitas, termasuk pengumpulan, pemrosesan, agregasi, dan penyebaran data yang tidak semestinya (Solove, 2006). Dari kerangka kerja ini, muncul prinsip-prinsip privasi inti yang kini menjadi dasar banyak regulasi data global, seperti *General Data Protection Regulation* (GDPR). Prinsip-prinsip ini mencakup manajemen persetujuan (consent), di mana individu harus memberikan izin yang jelas dan terinformasi sebelum data mereka diproses, pembatasan tujuan *(purpose limitation)*, yang mengharuskan data hanya digunakan untuk tujuan spesifik yang diungkapkan saat pengumpulan; dan minimalisasi data *(data minimization)*, yang menyatakan bahwa hanya data yang benar-benar diperlukan untuk tujuan tersebut yang boleh dikumpulkan (Spiekermann dan Cranor, 2009).

2.3 Teori Motivasi Perlindungan (*Protection Motivation Theory*)

Protection Motivation Theory (PMT) pertama kali diperkenalkan oleh Rogers (Rogers, 1975), sebagai kerangka kerja untuk menjelaskan bagaimana perilaku perlindungan manusia diinisiasi dan dipertahankan dalam menghadapi ancaman. Revisi selanjutnya terhadap teori ini menambahkan komunikasi persuasif yang berfokus pada proses kognitif yang memfasilitasi perubahan perilaku (Rogers, 1983). Dua dimensi fundamental membentuk PMT, yaitu "penilaian ancaman" dan "penilaian penanggulangan", di mana opsi perilaku untuk menghindari ancaman dievaluasi. Penilaian ancaman adalah "seberapa parah dan seberapa besar kemungkinan ancaman tersebut menyebabkan konsekuensi yang tidak diinginkan", sedangkan penilaian penanggulangan adalah kemampuan yang dirasakan untuk melakukan perilaku perlindungan. Menghindari ancaman tersebut bergantung pada

mengikuti perilaku adaptif tertentu. Efektivitas perilaku tersebut ditentukan oleh *response efficacy* (misalnya, bantuan dari teman sebaya atau instruktur) dan *self-efficacy* (misalnya, pengetahuan sebelumnya tentang topik yang menjadi perhatian). Respons yang tepat mungkin memerlukan waktu dan sumber daya (*Response Cost*). Untuk strategi yang efektif, ancaman yang dirasakan harus melebihi respons mal-adaptif, sementara penilaian penanggulangan harus melebihi *Response Cost*. PMT bertujuan untuk memotivasi individu agar dapat melindungi diri sendiri dari resiko kerentanan yang dapat mengancam individu tersebut (Rogers, 1975)

2.3.1 Persepsi Efikasi Diri *(Perceived Self-Efficacy)*

Dalam penelitian ini, *Perceived Self-Efficacy* (PSE) diidentifikasi sebagai sejauh mana karyawan meyakini kemampuan dan keterampilan mereka dalam menghadapi ancaman siber. Menurut penelitian sebelumnya, PSE meningkatkan kemampuan pekerja untuk merespons secara adaptif dan kesediaan mereka secara keseluruhan untuk menerapkan respons tersebut (Sharma dan Aparicio, 2022). Selain itu, individu yang menganggap kebijakan keamanan memberikan informasi yang substansial tentang nilai aktivitas mereka dan efisiensi solusi yang direkomendasikan dalam mengurangi probabilitas pelanggaran keamanan informasi cenderung mengembangkan niat yang positif. Sikap positif terhadap kebijakan ini meningkatkan kemungkinan mereka untuk mematuhi langkah-langkah keamanan informasi (Alsaad dan Al-Okaily, 2022). Semakin tinggi efikasi diri, semakin besar kecenderungan karyawan untuk mematuhi aturan keamanan.

2.3.2 Persepsi Efikasi Respons *(Perceived Response Efficacy)*

Keyakinan bahwa perilaku kepatuhan yang dilakukan (seperti mengikuti instruksi kebijakan) benar-benar efektif dalam melindungi organisasi dari ancaman. Individu yang yakin akan efektivitas protokol keamanan memiliki peluang lebih tinggi untuk benar-benar mematuhinya.

2.3.3 Persepsi Biaya Respons *(Perceived Response Cost)*

Merujuk pada pengorbanan berupa waktu, upaya ekstra, atau kenyamanan yang harus dikeluarkan individu untuk melaksanakan perilaku protektif. Semakin tinggi biaya atau hambatan yang dirasakan dalam mematuhi kebijakan, maka motivasi untuk patuh cenderung menurun.

2.3.4 Persepsi Kerentanan *(Perceived Vulnerability)*

Merujuk pada keyakinan atau penilaian individu mengenai seberapa besar kemungkinan mereka atau organisasi mereka akan terkena dampak negatif dari an-

caman keamanan informasi. Karyawan yang merasa sistem organisasinya sangat rentan cenderung lebih bersedia mengadopsi tindakan perlindungan

2.3.5 Persepsi Keparahan *(Perceived Severity)*

Merujuk pada penilaian individu terhadap besarnya dampak atau keseriusan konsekuensi yang ditimbulkan jika ancaman keamanan benar-benar terjadi, seperti kehilangan data sensitif atau kerusakan reputasi. Tingkat ketakutan yang muncul dari persepsi keparahan yang tinggi dapat mendorong perilaku kepatuhan yang lebih kuat.

2.3.6 Kepatuhan Kebijakan Keamanan Informasi *(Information Security Policy Compliance)*

Dalam penelitian ini, Kepatuhan Kebijakan Keamanan Informasi *(Information Security Policy Compliance)* ditempatkan sebagai perilaku nyata atau komitmen karyawan untuk mematuhi peraturan organisasi guna menjaga integritas, kerahasiaan, dan ketersediaan data. Kepatuhan ini bukan sekadar mengikuti aturan, melainkan komponen kritis dari postur keamanan organisasi secara keseluruhan.

Penelitian menunjukkan bahwa perilaku kepatuhan dipengaruhi secara langsung oleh faktor-faktor kognitif dalam PMT, di mana individu melakukan evaluasi apakah manfaat dari perlindungan lebih besar daripada pengorbanan yang dilakukan. Dalam konteks perbankan, kepatuhan yang kuat sangat penting untuk melindungi data keuangan sensitif dari ancaman internal maupun eksternal.

Dalam perspektif *Protection Motivation Theory*, perilaku kepatuhan tersebut tidak muncul secara spontan, melainkan merupakan hasil dari proses penilaian kognitif individu terhadap ancaman yang dihadapi dan kemampuan yang dimiliki untuk mengatasinya. Proses ini melibatkan evaluasi terhadap tingkat risiko, efektivitas tindakan perlindungan, serta pengorbanan yang harus dilakukan sebelum individu memutuskan untuk bertindak secara protektif.

2.3.7 Posisi Kepatuhan dalam *Protection Motivation Theory*

Protection Motivation Theory menjelaskan bahwa perilaku protektif individu terbentuk melalui dua proses utama, yaitu *threat appraisal* dan coping appraisal. *Threat appraisal* berkaitan dengan penilaian individu terhadap tingkat keparahan ancaman *(perceived severity)* dan kemungkinan terjadinya ancaman *(perceived vulnerability)*. Sementara itu, coping appraisal berkaitan dengan penilaian individu terhadap efektivitas respons perlindungan *(response efficacy)*, efikasi diri *(*self-efficacy), serta biaya yang harus dikeluarkan untuk melakukan tindakan perlindungan *(response cost)*. Kedua proses tersebut memengaruhi cara individu

mengambil keputusan dalam menghadapi ancaman keamanan informasi.

Dalam kerangka PMT, hasil dari proses *threat appraisal* dan coping appraisal tidak secara langsung menghasilkan perilaku, tetapi terlebih dahulu membentuk motivasi perlindungan (protection motivation) yang umumnya dipahami sebagai niat (intention) untuk bertindak. Intention mencerminkan kesiapan individu untuk melakukan perilaku protektif berdasarkan penilaian terhadap ancaman dan kemampuan yang dimilikinya. Dengan demikian, intention berperan sebagai mekanisme psikologis yang menghubungkan faktor-faktor kognitif dalam PMT dengan perilaku protektif yang ditunjukkan oleh individu.

Penelitian-penelitian terdahulu dalam konteks kepatuhan kebijakan keamanan informasi menunjukkan bahwa faktor-faktor PMT berpengaruh signifikan terhadap intention, dan intention tersebut merupakan prediktor utama dari perilaku kepatuhan. Berdasarkan pemahaman tersebut, penelitian ini memposisikan kepatuhan terhadap kebijakan keamanan informasi sebagai perilaku berbasis niat *(intention-based behavior)*. Oleh karena itu, konstruk intention tidak diukur sebagai variabel terpisah, melainkan dianggap telah terinternalisasi dalam perilaku kepatuhan karyawan yang diamati dalam penelitian ini.

2.4 *Bibliometric*

Analisis *bibliometric* adalah pendekatan kuantitatif yang menggunakan metode statistik untuk menganalisis data publikasi ilmiah, seperti jurnal dan prosiding konferensi. Tujuannya adalah untuk memetakan struktur intelektual, mengukur dampak, dan mengidentifikasi tren dalam suatu bidang penelitian (Aria dan Cuccurullo, 2017). Metode ini memungkinkan peneliti untuk secara objektif mengidentifikasi penulis, institusi, dan karya paling berpengaruh. Lebih jauh, analisis bibliometrik dapat melacak evolusi tema penelitian dari waktu ke waktu melalui teknik seperti analisis ko-sitasi untuk menemukan karya fundamental (Small, 1973) dan analisis kemunculan bersama kata kunci untuk memetakan tema-tema dominan (Callon, Courtial, Turner, dan Bauin, 1983).

Dalam praktiknya, analisis bibliometrik mencakup berbagai indikator yang berfungsi untuk mengukur kualitas dan pengaruh penelitian. Beberapa indikator utama antara lain jumlah sitasi, h-indeks, serta faktor dampak jurnal. Indikator-indikator tersebut tidak hanya menilai kuantitas publikasi, tetapi juga mengukur sejauh mana karya ilmiah berkontribusi pada pengembangan ilmu pengetahuan. Dengan demikian, bibliometrik menjadi instrumen penting untuk menilai reputasi akademik baik individu maupun institusi (Donthu dkk., 2021).

Selain indikator, analisis *Bibliometric* juga mencakup berbagai teknik utama yang sering digunakan untuk memahami struktur dan dinamika suatu bidang penelitian. Pertama, *citation analysis* (kutipan analisis) digunakan untuk menilai pengaruh suatu karya ilmiah dengan menghitung jumlah sitasi yang diterima (Garfield, 1972). Kedua, *co-author analysis* (analisis kolaborasi penulis) berfokus pada pemetaan kolaborasi antarpenulis, institusi, maupun negara, yang memberikan gambaran mengenai jejaring kerja sama dalam komunitas ilmiah (Glänzel dan Schubert, 2005; Gülmez, Özteke, dan Gümüş, 2020). Ketiga, *co-citation analysis* (analisis kolaborasi kutipan) digunakan untuk menilai keterkaitan antarartikel atau penulis berdasarkan frekuensi mereka disitasi bersama dalam publikasi lain, sehingga membantu menemukan fondasi intelektual dari suatu bidang (Small, 1973). Keempat, *co-word analysis* (analisis kolaborasi kata) memanfaatkan kemunculan bersama kata kunci, judul, maupun abstrak untuk memetakan struktur konseptual, tren tema penelitian, serta isu-isu yang sedang berkembang (Callon dkk., 1983). Dengan memanfaatkan kombinasi teknik ini, peneliti dapat memperoleh pemahaman yang lebih menyeluruh mengenai hubungan, pengaruh, dan arah perkembangan suatu domain ilmu (Syaifullah, Ariffin, dan Nordin, 2024).

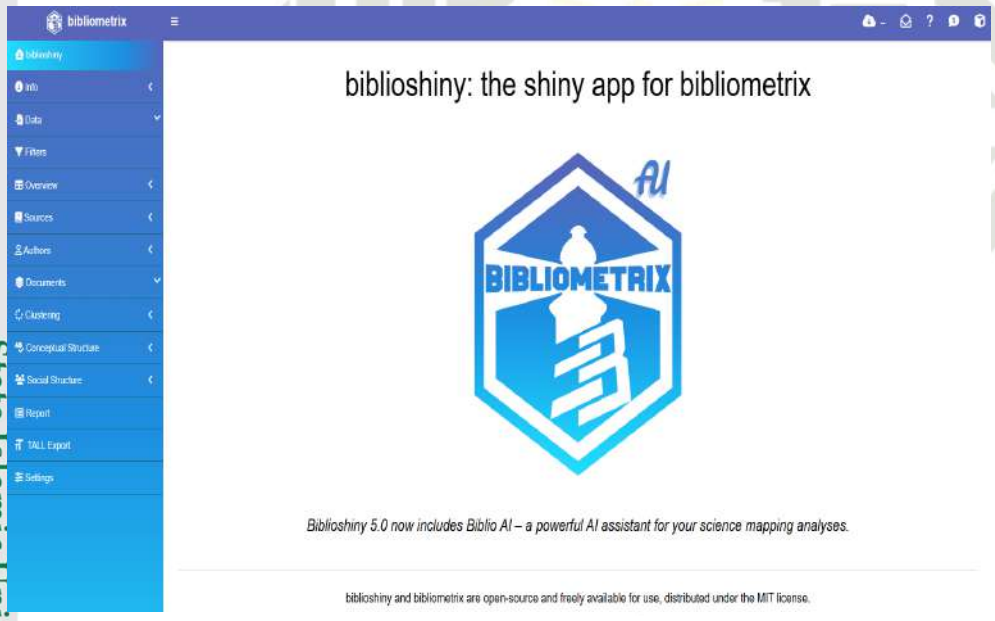
Penerapan metode-metode ini menjadi semakin relevan ketika difokuskan pada area penelitian tertentu, karena mampu memberikan gambaran yang lebih spesifik mengenai dinamika dan arah perkembangan sebuah domain ilmu. Misalnya, dalam bidang keamanan dan privasi pada *cloud computing*, *analisis bibliometric* dapat dimanfaatkan untuk menelusuri tren penelitian, mengidentifikasi topik-topik dominan, serta memetakan kontribusi peneliti maupun institusi dalam pengembangan pengetahuan di bidang tersebut.

Untuk melaksanakan analisis semacam ini, dibutuhkan perangkat yang dapat mengolah data publikasi secara sistematis dan menyajikan hasil dalam bentuk yang mudah diinterpretasikan. Salah satu perangkat yang banyak digunakan adalah Biblioshiny, yaitu antarmuka berbasis web dari paket *Bibliometric* di R (Aria dan Cuccurullo, 2017). Keunggulan utama Biblioshiny adalah kemampuannya menyajikan analisis *bibliometric* secara interaktif tanpa memerlukan keahlian pemrograman yang mendalam, sehingga memudahkan peneliti dalam mengeksplorasi data literatur ilmiah.

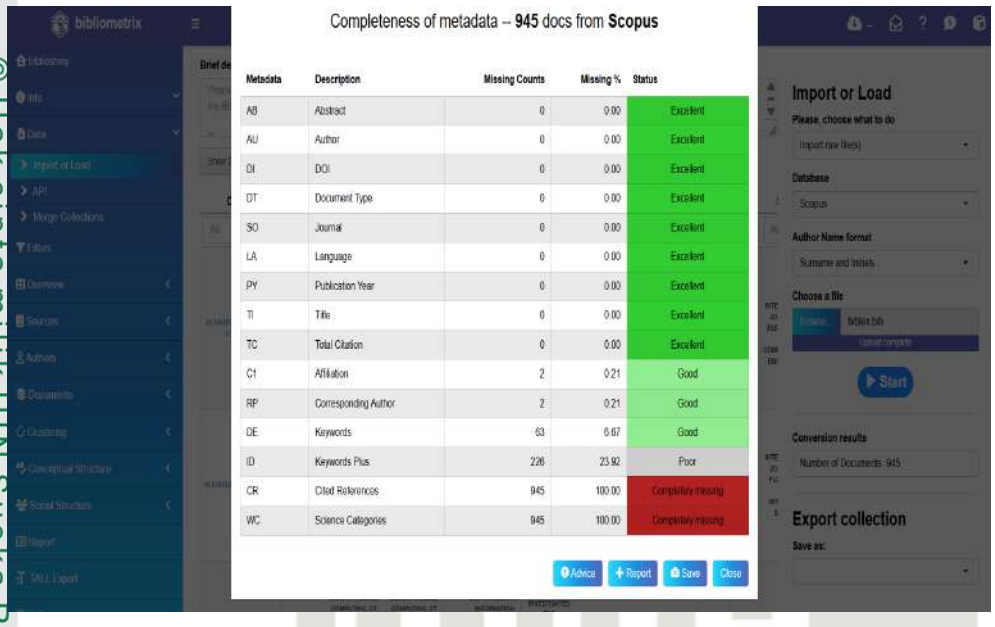
Biblioshiny menyediakan berbagai fitur analisis, termasuk analisis performa (jumlah publikasi, sitasi, dan produktivitas penulis), analisis sitasi (karya dan jurnal paling berpengaruh), serta analisis jaringan (network analysis) seperti kolaborasi antar penulis, institusi, maupun negara. Fitur visualisasi yang disediakan juga men-

dukung pemetaan tren kata kunci dan evolusi topik dari waktu ke waktu, sehingga peneliti dapat memperoleh gambaran yang komprehensif mengenai perkembangan suatu bidang penelitian.

Selain itu, Biblioshiny memiliki fleksibilitas untuk mengolah data dari berbagai sumber basis data besar seperti Scopus, *Web of Science* (WoS), maupun Dimensions. Hal ini membuatnya relevan untuk penelitian lintas disiplin maupun penelitian yang fokus pada domain spesifik. Integrasi tersebut memperkuat keandalan hasil analisis karena data yang digunakan mencakup cakupan literatur yang luas dan berkualitas. Dengan dukungan tersebut, analisis *bibliometric* melalui Biblioshiny memberikan kerangka kerja yang komprehensif untuk memahami perkembangan suatu bidang penelitian. Melalui kombinasi indikator kuantitatif, teknik analisis, serta visualisasi interaktif, pendekatan ini mampu mengungkap tren, tema dominan, dan jaringan kolaborasi ilmiah secara sistematis. Halaman utama Biblioshiny yang menjadi titik awal proses analisis *bibliometric* dapat dilihat pada Gambar 2.1 dan Gambar 2.2 halaman setelah impor data.



Gambar 2.1. Halaman Bibliometrix Sebelum Impor Data



Gambar 2.2. Halaman Bibliometrix Setelah Impor Data

2.5 Penelitian Terdahulu

Dalam beberapa tahun terakhir, telah banyak penelitian yang dilakukan terkait kepatuhan kebijakan keamanan informasi. Tabel 2.1 menyajikan ringkasan dari beberapa penelitian terdahulu yang relevan dengan topik ini.

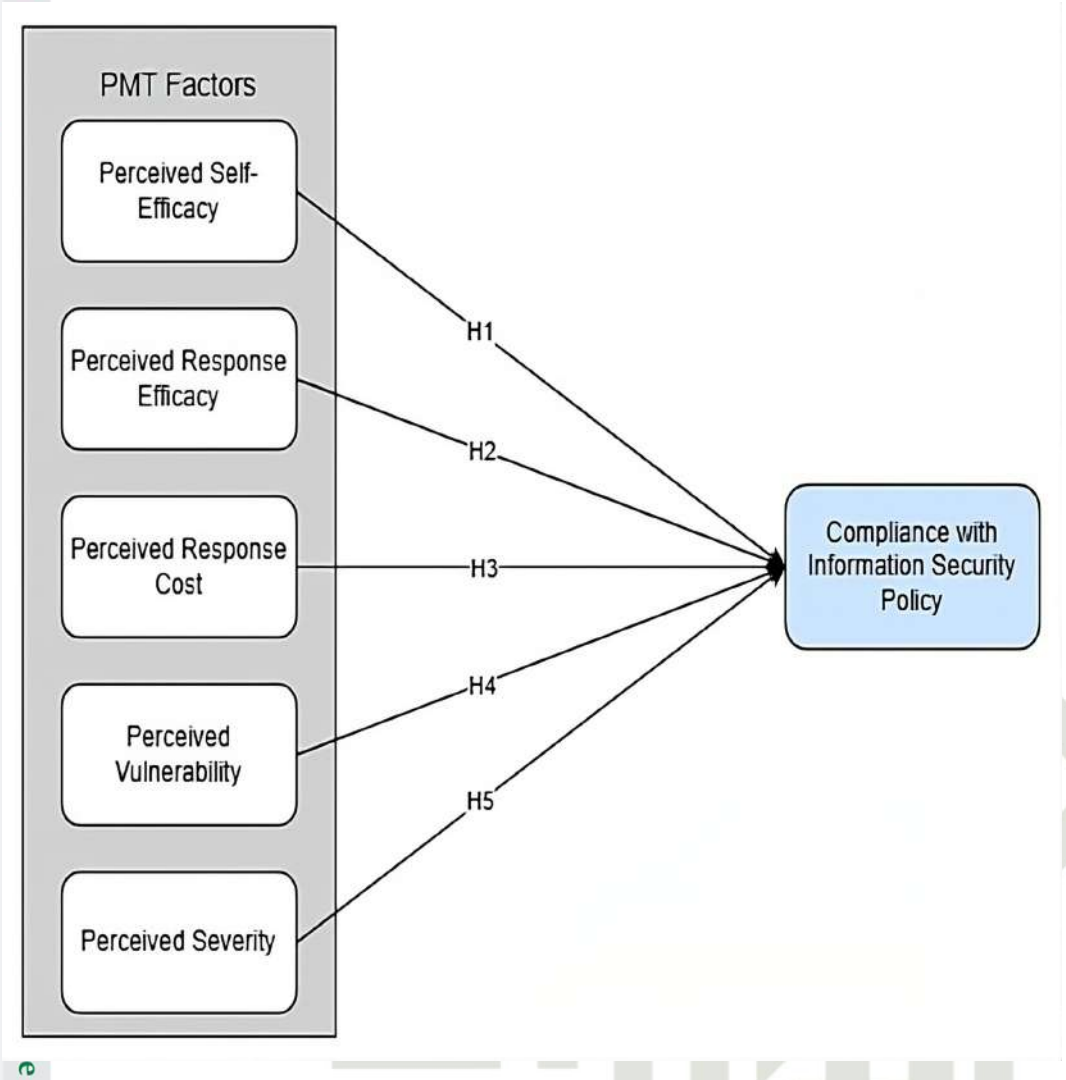
Tabel 2.1. Penelitian Terdahulu

Penulis	Judul Penelitian	Hasil Penelitian
(Angraini, Alias, dan Okfalisa, 2019)	*Information Security Policy Compliance: Systematic Literature Review*	Penelitian ini menemukan bahwa kajian kepatuhan kebijakan keamanan informasi masih didominasi oleh pendekatan teori perilaku manusia, sementara evaluasi kepatuhan dan pengembangan instrumen pengukuran kepatuhan kebijakan keamanan informasi masih terbatas.
(Angraini, Alinda Alias, dan Okfalisa, 2019)	*Need for Compliance With Information Security Policy In Universities: a Preliminary survey*	Penelitian ini menemukan bahwa manajemen menyadari pentingnya kepatuhan terhadap kebijakan keamanan informasi untuk mengurangi insiden keamanan informasi. Universitas memerlukan model yang tepat untuk mengevaluasi kepatuhan terhadap kebijakan keamanan informasi

Tabel 2.1 Penelitian Terdahulu (lanjutan...)

Penulis	Judul Penelitian	Hasil Penelitian
(Alrawhani dkk., 2025)	*Evaluating the role of protection motivation theory in information security policy compliance: Insights from the banking sector using PLS-SEM approach*	Studi ini mengevaluasi perilaku kepatuhan kebijakan keamanan informasi pada 210 karyawan bank di Yaman menggunakan kerangka Protection Motivation Theory (PMT) dan analisis PLS-SEM. Studi ini menunjukkan bahwa *self-efficacy*, *response efficacy*, dan *perceived severity* berpengaruh signifikan terhadap niat kepatuhan kebijakan keamanan informasi, sedangkan *perceived vulnerability* dan *response cost* tidak berpengaruh signifikan dalam konteks perbankan di negara berkembang.
(de Veluz dkk., 2025)	*Expanding integrated protection motivation theory and theory of planned behavior: The role of source of influence in flood and typhoon risk preparedness intentions*	Penelitian ini menganalisis niat evakuasi masyarakat dalam menghadapi risiko banjir dan topan. Penelitian ini menemukan bahwa sumber pengaruh (keluarga, komunitas, media, dan pengalaman masa lalu) berpengaruh signifikan terhadap persepsi risiko dan niat perilaku protektif, sementara tingkat pendidikan menjadi satu-satunya faktor demografis yang berpengaruh signifikan.
(Alraja dkk., 2023)	*Information security policies compliance in a global setting: An employee's perspective*	Penelitian ini menguji faktor-faktor pendorong kepatuhan dan reaktansi terhadap kebijakan keamanan informasi. Hasil penelitian menunjukkan bahwa nilai peran (role values) dan rasa takut (fear) merupakan prediktor terkuat yang memengaruhi niat kepatuhan, sementara teknik netralisasi dan rasa takut secara signifikan memengaruhi munculnya reaktansi atau penolakan karyawan terhadap kebijakan.

2.6 Pengembangan Hipotesis



Gambar 2.3. Kerangka Konseptual
(Alrawhani dkk., 2025)

Perilaku kepatuhan terhadap kebijakan keamanan informasi dipengaruhi oleh proses penilaian kognitif individu terhadap ancaman dan kemampuan penanggulangan yang dimilikinya. PMT menjelaskan bahwa individu akan terdorong untuk melakukan perilaku protektif apabila mereka menilai ancaman sebagai sesuatu yang serius dan merasa mampu untuk melakukan tindakan perlindungan yang efektif. Kerangka konseptual PMT dapat dilihat pada Gambar 2.3.

Dalam konteks kepatuhan kebijakan keamanan informasi, *self-efficacy* mencerminkan keyakinan pegawai terhadap kemampuannya dalam memahami dan menjalankan kebijakan keamanan yang berlaku. Pegawai yang merasa mampu cen-

derung lebih yakin untuk mematuhi aturan keamanan informasi yang ditetapkan organisasi. Oleh karena itu, dapat dirumuskan hipotesis sebagai berikut:

H1: *Self-Efficacy* (SE) berpengaruh positif terhadap *Compliance with Information Security Policy* (CISP).

Selain itu, *Response Efficacy* menunjukkan sejauh mana pegawai meyakini bahwa kebijakan dan prosedur keamanan informasi yang diterapkan organisasi efektif dalam mencegah atau mengurangi ancaman. Apabila kebijakan keamanan dipersepsikan efektif, pegawai akan lebih termotivasi untuk mematuhi kebijakan tersebut. Dengan demikian, dirumuskan hipotesis sebagai berikut:

H2: *Response Efficacy* (RE) berpengaruh positif terhadap *Compliance with Information Security Policy* (CISP).

Di sisi lain, *Response Cost* menggambarkan persepsi pegawai terhadap pengorbanan yang harus dilakukan dalam menjalankan kebijakan keamanan informasi, seperti tambahan waktu, usaha, atau ketidaknyamanan. Tingginya biaya yang dirasakan dapat menurunkan motivasi pegawai untuk berperilaku patuh. Oleh karena itu, hipotesis yang dirumuskan adalah:

H3: *Response Cost* (RC) berpengaruh negatif terhadap *Compliance with Information Security Policy* (CISP).

Faktor *threat appraisal* dalam PMT juga berperan penting dalam membentuk perilaku kepatuhan.*Perceived vulnerability* mencerminkan persepsi pegawai terhadap kemungkinan terjadinya ancaman keamanan informasi yang dapat berdampak pada dirinya maupun organisasi. Semakin tinggi tingkat kerentanan yang dirasakan, semakin besar dorongan pegawai untuk mematuhi kebijakan keamanan informasi. Dengan demikian, dirumuskan hipotesis berikut:

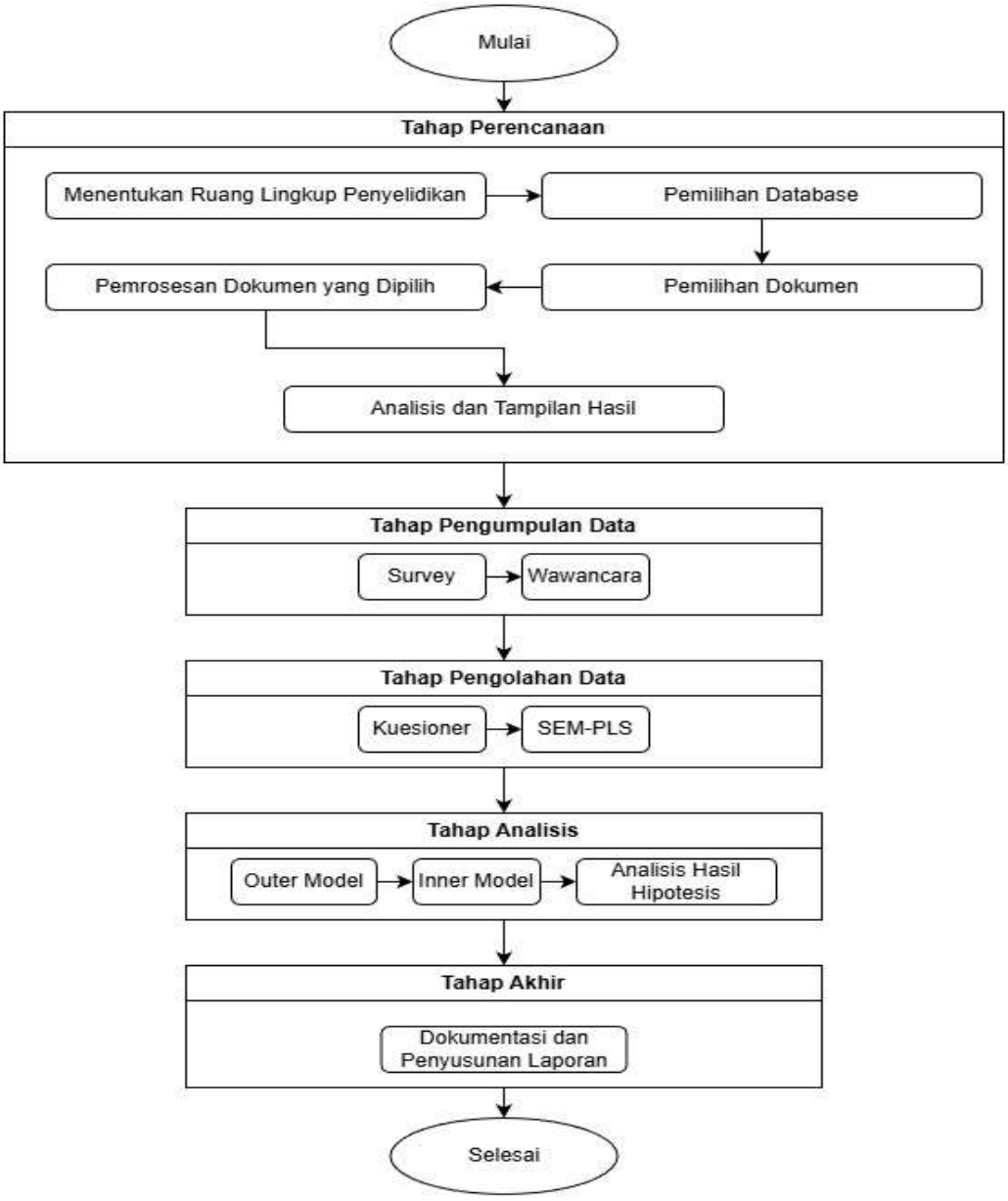
H4:*Perceived Vulnerability* (PV) berpengaruh positif terhadap *Compliance with Information Security Policy* (CISP).

Selanjutnya, *Perceived Severity* menggambarkan persepsi pegawai terhadap tingkat keparahan dampak yang dapat timbul apabila terjadi pelanggaran keamanan informasi. Ancaman yang dipersepsikan memiliki konsekuensi serius cenderung mendorong individu untuk melakukan perilaku protektif. Oleh karena itu, dirumuskan hipotesis sebagai berikut:

H5: *Perceived Severity* (PS) berpengaruh positif terhadap *Compliance with Information Security Policy* (CISP).

BAB 3
METODOLOGI PENELITIAN

Metodologi adalah serangkaian metode, prosedur, dan teknik yang digunakan untuk mengumpulkan dan menganalisis data guna mencapai tujuan penelitian atau proyek tertentu. Dalam penelitian ini Metodologi yang digunakan oleh peniliti dapat dilihat pada Gambar 3.1.



Gambar 3.1. Metodologi Penelitian

3.1 Tahap Perencanaan

Tahap perencanaan dilakukan melalui *Systematic Literature Review* (SLR) untuk menentukan ruang lingkup penelitian, mengidentifikasi tren dan research gap, mendapatkan peta tematik topik, klaster penelitian masa depan serta merumuskan model dan variabel penelitian.

3.1.1 Ruang Lingkup Penyelidikan

Penentuan ruang lingkup penyelidikan dilakukan untuk membatasi fokus penelitian agar sesuai dengan tujuan yang telah ditetapkan. Ruang lingkup ini mencakup topik penelitian, serta periode publikasi, sehingga kajian literatur yang dilakukan tetap terarah dan tidak melebar dari permasalahan penelitian.

Fokus penelitian ditetapkan pada isu *security* dan *privacy* dalam *cloud computing*. Pemilihan tema ini didasarkan pada relevansi akademis maupun praktis, di mana keamanan dan privasi menjadi faktor penting dalam menjaga kepercayaan pengguna, sementara teknologi *cloud computing* sendiri terus berkembang dan semakin luas diadopsi. Setelah menetapkan tema, peneliti melakukan pencarian kata kunci yang diperlukan untuk pengambilan data dari *database* seperti Scopus (Maalej dan Kallel, 2020).

3.1.2 Pemilihan *Database*

Penelitian mengenai keamanan dan privasi pada *cloud computing* banyak dipublikasikan melalui berbagai media ilmiah, seperti jurnal, prosiding konferensi, maupun buku, yang memiliki standar kualitas yang berbeda-beda. Salah satu indikator penting dari kualitas publikasi adalah adanya proses *peer review*. Oleh karena itu, penelitian ini menggunakan Scopus sebagai sumber utama pengumpulan data, karena artikel yang terindeks di dalamnya telah melalui proses peninjauan oleh pakar di bidangnya. Scopus sendiri merupakan basis data kutipan dan abstrak yang dikelola secara profesional oleh Elsevier dan mencakup literatur ilmiah dari berbagai disiplin ilmu. Berdasarkan hasil penelusuran di website resmi Scopus, diperoleh sejumlah artikel yang sesuai dengan tema penelitian, yaitu *security* dan *privacy* dalam *cloud computing*. Namun, jumlah artikel tersebut kemudian disaring lebih lanjut berdasarkan kriteria tertentu, sehingga hanya publikasi yang memenuhi persyaratan yang digunakan sebagai sumber data dalam penelitian ini.

3.1.3 Pemilihan Dokumen

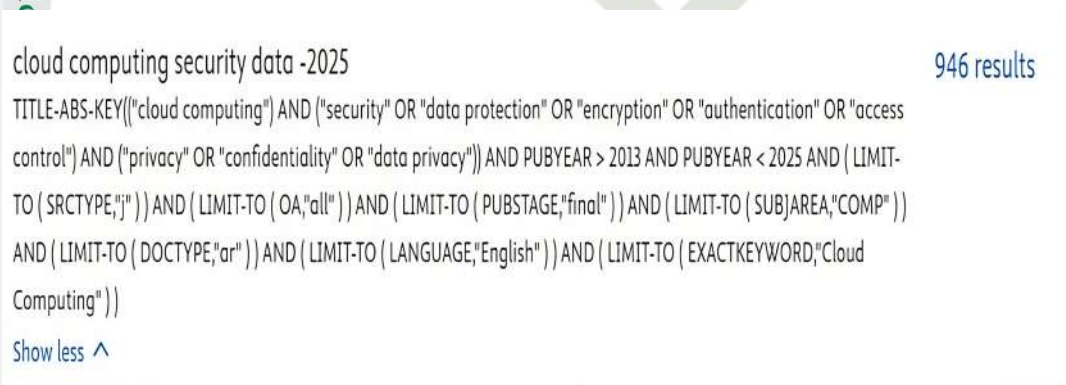
Pemilihan dokumen dilakukan dengan menggunakan kata kunci yang relevan dengan topik penelitian. Artikel yang diperoleh kemudian diseleksi berdasarkan

kriteria seperti pemilihan query pencarian, bahasa, tahap publikasi, sumber publikasi, jenis publikasi, tahun terbit, dan akses dokumen sehingga hanya dokumen yang relevan yang digunakan dalam penelitian.

3.1.3.1 Identifikasi *Keyword*

Identifikasi kata kunci merupakan langkah yang dilakukan peneliti untuk menentukan istilah pencarian yang digunakan dalam penelitian. Pada penelitian ini, identifikasi dilakukan dengan meninjau artikel dan jurnal yang relevan terkait isu *security* dan *privacy* dalam konteks *cloud computing*. Kata kunci berperan penting karena menjadi dasar untuk mengevaluasi tren penelitian, jumlah publikasi, serta kontribusi ilmiah pada topik tertentu, sekaligus menyederhanakan proses pencarian literatur dan membantu memahami peta penelitian di bidang terkait. Kata kunci tersebut kemudian disusun dengan bantuan operator logika Boolean, seperti AND dan OR, guna mengombinasikan istilah pencarian secara efektif sehingga cakupan pencarian lebih luas namun tetap relevan, dan dapat mendukung analisis bibliometrik yang akurat serta terarah.

Penelitian ini menggunakan keyword pencarian *"Security", "Privacy"* dan *"Cloud Computing"* dengan *syntax* pencarian: TITLE-ABS-KEY(*"cloud computing"* AND *"security"* OR *"data protection"* OR *"encryption"* OR *"authentication"* OR *"access control"* AND *privacy* OR *"confidentiality"* OR *"data privacy"*) AND PUBYEAR >2013 AND PUBYEAR <2025 AND (LIMIT-TO (SRCTYPE,"j")) AND (LIMIT-TO (OA,"all")) AND (LIMIT-TO (PUBSTAGE,*"final"*)) AND (LIMIT-TO (SUBJAREA,*"COMP"*)) AND (LIMIT-TO (DOCTYPE,"ar")) AND (LIMIT-TO (LANGUAGE,*"English"*)) AND (LIMIT-TO (EXACTKEYWORD,*"Cloud Computing"*)). *Keyword* inilah yang nantinya digunakan peneliti dalam mencari data di *database* Scopus mengenai topik tersebut. Pencarian *keyword* dalam *database* Scopus dapat dilihat pada Gambar 3.2.



Gambar 3.2. Pencarian *Keyword* di Database Scopus

3.1.3.2 Batasan Search within *Title, Abstract* dan *Keyword*

Pencarian artikel dilakukan dengan menggunakan opsi *Search Title, Abstract,* dan *Keyword* pada Scopus. Opsi ini dipilih agar hasil pencarian lebih fokus dan relevan, karena hanya menampilkan artikel yang secara eksplisit memuat kata kunci pada judul, abstrak, atau daftar kata kunci. Dengan demikian, publikasi yang diperoleh memiliki keterkaitan yang jelas dengan tema penelitian, yaitu *security* dan *privacy* dalam *cloud computing*, serta mengurangi kemungkinan masuknya artikel yang tidak relevan.

3.1.3.3 Batasan Tahun 2014 sampai 2024

Penelitian ini membatasi rentang waktu publikasi antara tahun 2014 hingga 2024. Rentang ini dipilih untuk memperoleh literatur yang relatif mutakhir sekaligus cukup panjang untuk mengidentifikasi pola perkembangan penelitian selama satu dekade terakhir. Dengan batasan ini, analisis dapat menangkap tren jangka panjang sekaligus melihat arah penelitian terbaru di bidang keamanan dan privasi *cloud computing*.

3.1.3.4 Batasan Bahasa Inggris

Artikel yang dipilih dibatasi pada publikasi berbahasa Inggris. Pertimbangan ini didasarkan pada fakta bahwa bahasa Inggris merupakan bahasa internasional dalam komunikasi ilmiah, sehingga literatur yang diperoleh lebih mudah dibandingkan secara konsisten dan memiliki jangkauan audiens yang lebih luas (Hyland, 2016).

3.1.3.5 Batasan Final Publikasi

Hanya artikel dengan status *final publication* yang digunakan dalam penelitian ini. Hal ini bertujuan untuk menghindari penggunaan artikel dalam status *in press* atau versi pra-cetak, yang masih mungkin mengalami perubahan. Dengan demikian, data yang digunakan lebih stabil, kredibel, dan dapat dipertanggungjawabkan secara ilmiah.

3.1.3.6 Batasan Jurnal

Peneliti membatasi media publikasi atau membatasi tipe dokumen yaitu artikel dan *source type* jurnal dalam melakukan pencarian data di *database* Scopus. Hal ini dilakukan peneliti dengan tujuan untuk memperkecil jangkauan pencarian data.

3.1.3.7 Batasan Dokumen Artikel

Jenis dokumen yang dipilih dibatasi pada artikel yang terindeks Scopus. Dokumen tipe buku, bab atau prosiding konferensi tidak dimasukkan dalam penelitian ini. Hal ini untuk menjaga konsistensi dan menjamin bahwa data bersumber dari publikasi ilmiah yang diakui secara internasional.

3.1.3.8 Batasan Dokumen *Open Access*

Penelitian ini juga menerapkan batasan pada artikel *open access*, agar data yang digunakan dapat diakses secara penuh tanpa hambatan. Selain memudahkan proses verifikasi dan analisis lebih lanjut, penggunaan artikel open access juga sejalan dengan prinsip keterbukaan akses pengetahuan ilmiah.

3.1.4 Pemrosesan Dokumen yang Dipilih

Dokumen yang telah terpilih selanjutnya diproses dengan menelaah isi artikel. Pada tahap ini, peneliti mengidentifikasi informasi penting seperti tujuan penelitian, metode yang digunakan, variabel, serta temuan utama yang berkaitan dengan penelitian.

3.1.5 Analisis dan Tampilan Hasil

Tahap analisis dilakukan dengan mengkaji hasil pemrosesan dokumen untuk mengidentifikasi pola, kesamaan, dan perbedaan antar penelitian terdahulu. Hasil analisis kemudian disajikan secara sistematis dalam bentuk peta tematik sebagai dasar pendukung dalam penyusunan dan pengembangan penelitian ini.

3.2 Implementasi Penelitian

Penelitian ini menggunakan pendekatan kuantitatif karena penelitian ini bertujuan untuk menguji hipotesis serta mengukur hubungan antar variabel secara numerik menggunakan analisis statistik. Desain ini memungkinkan peneliti untuk melakukan generalisasi hasil temuan dari sampel terhadap populasi yang diteliti.

3.2.1 Tahap Pengumpulan Data

Pada fase pengumpulan data, dikumpulkan data data yang dapat berpengaruh terhadap kepatuhan kebijakan keamanan informasi untuk melakukan sebuah Analisa. Penelitian ini menggunakan metode pengambilan data kuantitatif yaitu dengan menyebarkan kuesioner. Menyebarkan kuesioner ini dilakukan secara *offline* dan *online* agar data yang dihasilkan rill sudah tersusun dan mudah untuk dikelola. Pengambilan data responden tersebut menggunakan Metode *Simple Random Sampling* yaitu pengambilan data sampel secara acak. Data responden yang didapatkan

sebanyak 31 jawaban responden, dimana 18 data didapat secara *offline* dan 13 data dari *online* melalui *Google Form*. Data yang didapat tersebut diolah menggunakan *tools* SmartPLS. Dimana yang menjadi kriteria responden dalam penelitian tersebut adalah Pegawai di Fakultas Sains dan Teknologi Universitas Islam Negeri Sultan Syarif Kasim Riau seperti dosen dan tenaga kependidikan, yang mana merupakan pengguna sistem informasi di Universitas yang mengelola data akademik.

Pada kuesioner yang disebarkan menggunakan beberapa skala likert dengan Panjang 5 point dengan masing-masing point 1. Sangat Tidak Setuju (STS), 2. Tidak Setuju (TS), 3. Netral (N), 4. Setuju (S), dan 5. Sangat Setuju (SS). Pertanyaan yang digunakan pada kuesioner tersebut menggunakan pertanyaan yang berasal dari penelitian terdahulu. Indikator Pengukuran penelitian ini dapat dilihat pada Tabel 3.1 di bawah ini.

Tabel 3.1. Indikator Pengukuran

Variabel	Pernyataan
Efikasi Diri *(Self-Efficacy)*	SE1: Saya mengetahui langkah-langkah yang harus dilakukan untuk menjaga keamanan informasi di Universitas SE2 : Saya mampu mengikuti kebijakan keamanan informasi yang berlaku di Universitas SE3 : Saya percaya diri dalam mengamankan akun dan data kerja saya di Universitas
Efikasi Respons *(Response Efficacy)*	RE1: Kebijakan keamanan informasi Universitas efektif dalam melindungi data RE2 : Prosedur keamanan informasi dapat mencegah insiden keamanan informasi RE3 : Kepatuhan terhadap kebijakan keamanan informasi meningkatkan keamanan sistem Universitas
Biaya Respons *(Response Cost)*	RC1: Penerapan kebijakan keamanan informasi Universitas menghambat pekerjaan saya RC2 : Prosedur keamanan informasi memerlukan waktu tambahan dalam pelaksanaan pekerjaan RC3 : Kepatuhan terhadap kebijakan keamanan informasi terasa merepotkan
Persepsi Kerentanan *(Perceived Vulnerability)*	PV1: Saya berpotensi mengalami insiden keamanan informasi saat menggunakan sistem informasi Universitas PV2 : Data yang saya kelola di Universitas berisiko bocor atau disalahgunakan PV3 : Akun atau perangkat kerja saya dapat menjadi target penyalahgunaan

Persepsi Keparahan *(Perceived Severity)*	PS1: Pelanggaran keamanan informasi dapat merugikan reputasi Universitas PS2 : Kebocoran data mahasiswa atau pegawai dapat menimbulkan dampak yang serius PS3 : Saya dapat dikenai sanksi jika melanggar kebijakan keamanan informasi Universitas
Kepatuhan Kebijakan Keamanan Informasi *(Compliance with Information Security Policy)*	CISP1: Saya mematuhi kebijakan keamanan informasi yang berlaku di Universitas CISP2: Saya tidak membagikan akun atau kata sandi kepada pihak lain CISP3: Saya mengikuti prosedur keamanan informasi saat mengelola data Universitas

3.2.1.1 Survei

Pengumpulan data pada penelitian ini dilakukan melalui metode survei dengan menggunakan kuesioner sebagai instrumen utama. Survei bertujuan untuk memperoleh data primer terkait persepsi dan perilaku responden terhadap kepatuhan kebijakan keamanan informasi. Kuesioner disusun berdasarkan konstruk dalam *Protection Motivation Theory* (PMT), yang meliputi *perceived severity, perceived vulnerability, response efficacy, self-efficacy,* dan *response cost*, serta variabel kepatuhan kebijakan keamanan informasi. Setiap pernyataan dirancang untuk menggambarkan penilaian individu terhadap ancaman keamanan informasi dan mekanisme koping yang memengaruhi keputusan responden dalam mematuhi kebijakan yang berlaku. Pengukuran dilakukan menggunakan skala Likert.

3.2.1.2 Wawancara

Selain survei, metode wawancara digunakan sebagai data pendukung dalam tahap pengumpulan data. Wawancara dilakukan secara terstruktur kepada salah satu pegawai di Fakultas Sains dan Teknologi untuk menggali pemahaman yang lebih mendalam mengenai motivasi, pengalaman, dan faktor-faktor yang memengaruhi kepatuhan terhadap kebijakan keamanan informasi (Lampiran A). Hasil wawancara digunakan untuk memperkaya interpretasi data survei serta memberikan konteks terhadap temuan kuantitatif yang diperoleh (Lampiran A).

3.2.2 Tahap Pengolahan Data

Pada fase pengolahan data, data yang berhasil dikumpulkan dari kuesioner yang disebarkan kepada responden selanjutnya akan diolah dengan mengelompokkan data sesuai dengan klasifikasi penelitian terdahulu seperti jumlah respon-

den, jumlah data berdasarkan gender, serta jabatan responden (Lampiran B). Data tersebut akan diolah menggunakan *tools* SmartPLS.

3.2.2.1 Kuesioner

Data yang diperoleh dari kuesioner selanjutnya diproses pada tahap pengolahan data. Pada tahap ini dilakukan pemeriksaan terhadap kelengkapan dan konsistensi jawaban responden. Data yang tidak lengkap atau tidak memenuhi kriteria penelitian dikeluarkan dari proses analisis. Selanjutnya, jawaban responden dikodekan ke dalam bentuk numerik dan disusun sesuai dengan indikator masing-masing konstruk PMT dan variabel kepatuhan kebijakan keamanan informasi. Tahap ini bertujuan untuk memastikan bahwa data yang digunakan siap untuk dianalisis secara statistik.

3.2.2.2 SEM-PLS

Setelah data kuesioner dinyatakan layak, pengolahan data dilanjutkan dengan menggunakan metode *Structural Equation Modeling–Partial Least Squares* (SEM-PLS). Metode ini digunakan karena mampu menganalisis hubungan antar variabel laten secara simultan serta sesuai untuk menguji model penelitian berbasis PMT yang bersifat prediktif. Pada tahap ini dilakukan pemodelan konstruk laten dan indikator berdasarkan kerangka konseptual penelitian.

3.2.3 Tahap Analisis

Setelah melakukan proses pengolaha n data menggunakan *tools* SmartPLS, fase yang dilakukan berikutnya adalah analisis dan uji statistika yang mana pada fase tersebut peneliti menggunakan metode deskriptif dalam menganalisis hasil dari statistika yang telah diproses menggunakan *tools* SmartPLS, yang mana metode tersebut merupakan metode yang digunakan untuk memberikan gambaran ringkas mengenai karakteristik data yang ada.

3.2.3.1 *Outer Model*

Analisis *outer model* dilakukan untuk mengevaluasi hubungan antara indikator dan konstruk laten dalam model penelitian. Pengujian ini bertujuan untuk menilai validitas dan reliabilitas indikator yang digunakan dalam mengukur konstruk PMT dan kepatuhan kebijakan keamanan informasi. Validitas dan reliabilitas diuji untuk memastikan bahwa setiap indikator mampu merepresentasikan konstruk yang diukur secara akurat dan konsisten.

3.2.3.2 *Inner Model*

Setelah *outer model* memenuhi kriteria yang ditetapkan, analisis dilanjutkan pada *inner model*. Analisis ini bertujuan untuk menguji hubungan antar konstruk dalam kerangka *Protection Motivation Theory*, khususnya pengaruh persepsi ancaman dan mekanisme penyelesaian terhadap kepatuhan kebijakan keamanan informasi. Hasil analisis *inner model* digunakan untuk menguji hipotesis penelitian serta menjelaskan kekuatan dan arah hubungan antar variabel dalam model penelitian.

3.2.3.3 Analisis Hasil Hipotesis

Tahap analisis hasil hipotesis merupakan tahap lanjutan setelah evaluasi model pengukuran *(outer model)* dan model struktural *(inner model)* dinyatakan memenuhi kriteria kelayakan. Pada tahap ini dilakukan pengujian hipotesis penelitian untuk mengetahui arah dan besaran pengaruh antar variabel dalam model penelitian yang telah dirumuskan.

BAB 5
PENUTUP

5.1 Kesimpulan

Bagian ini menyajikan kesimpulan dari seluruh rangkaian penelitian yang telah dilakukan. Kesimpulan disusun untuk merangkum temuan utama penelitian secara sistematis. Pembahasan pada bagian ini bertujuan untuk menjawab tujuan penelitian dan menegaskan kontribusi penelitian terhadap pengembangan kajian keamanan dan privasi data, dan perilaku kepatuhan pengguna.

5.1.1 Perkembangan Isu Keamanan dan Privasi

Berdasarkan hasil analisis bibliometrik terhadap publikasi ilmiah periode 2014–2024, dapat disimpulkan bahwa isu keamanan dan privasi pada *cloud computing* menunjukkan perkembangan yang signifikan dan berkelanjutan. Jumlah publikasi mengalami peningkatan yang cukup tajam sejak tahun 2018 dan mencapai puncaknya pada tahun-tahun berikutnya, meskipun terjadi fluktuasi pada periode tertentu. Pola rata-rata kutipan tahunan juga memperlihatkan bahwa topik ini memiliki dampak ilmiah yang kuat, ditandai dengan meningkatnya perhatian akademisi terhadap isu keamanan dan privasi, khususnya pada periode ketika teknologi *cloud computing* semakin luas diadopsi. Dominasi jurnal bereputasi seperti IEEE Access serta produktivitas penulis dan negara tertentu, terutama China dan India, menunjukkan bahwa penelitian di bidang ini telah menjadi fokus utama dalam kajian global.

Hasil analisis jaringan kata kunci dan word cloud menunjukkan bahwa *cloud computing*, *cryptography*, dan *data privacy* merupakan topik yang paling sering dibahas dan memiliki keterkaitan yang kuat satu sama lain. Peta kolaborasi internasional memperlihatkan adanya kerja sama lintas negara yang intens, terutama antara negara-negara Asia, Eropa, dan Amerika, dengan China, India, Australia, Inggris, dan Malaysia sebagai pusat kolaborasi utama. Hal ini mengindikasikan bahwa penelitian keamanan dan privasi dalam *cloud computing* bersifat global dan multidisipliner, serta terus berkembang melalui kolaborasi internasional.

Berdasarkan analisis peta tematik, klaster *Data Privacy* berada pada posisi yang strategis dan memiliki peran penting dalam struktur penelitian keamanan dan privasi *cloud computing*. Oleh karena itu, klaster *Data Privacy* dipilih sebagai tema besar yang mendasari penelitian ini. Fokus penelitian selanjutnya diarahkan pada analisis kebijakan keamanan informasi sebagai bentuk implementasi perlindungan

privasi data di dalam organisasi. Pemilihan fokus ini dinilai relevan karena kebijakan keamanan informasi merupakan instrumen utama dalam mengendalikan perilaku pengguna serta menjaga keamanan dan privasi data dalam lingkungan *cloud computing*.

5.1.2 Kepatuhan Kebijakan Keamanan Informasi

Hasil evaluasi model pengukuran menunjukkan bahwa model telah memenuhi kriteria validitas dan reliabilitas. Seluruh konstruk memenuhi validitas konvergen (AVE $>$ 0,50) dengan rentang angka 0.522 - 0.834 dan validitas diskriminan berdasarkan kriteria Fornell–Larcker. Uji reliabilitas menunjukkan bahwa seluruh konstruk memenuhi kriteria composite reliability dengan rentang angka 0.749 - 0.938, dan uji multikolinearitas menunjukkan tidak adanya masalah multikolinearitas (VIF $<$ batas yang direkomendasikan) dengan rentang angka 1.184 - 1.552. Dengan demikian, model pengukuran dan model struktural dinyatakan layak untuk analisis lanjutan.

Berdasarkan hasil pengujian hipotesis menggunakan metode bootstrapping, ditemukan bahwa dari lima hipotesis yang diuji, hanya *Perceived Severity* dan *Response Cost* yang terbukti berpengaruh signifikan terhadap Compliance with Information Security Policy dengan angka. *Perceived Severity* diterima, berpengaruh positif, dan signifikan dengan nilai p-value (0,041) lebih kecil dari 0,05, dan nilai t-statistic sebesar 2,046 lebih besar dari 1,96, yang mengindikasikan bahwa semakin tinggi persepsi individu terhadap tingkat keparahan ancaman keamanan informasi, maka semakin tinggi tingkat kepatuhan terhadap kebijakan keamanan informasi. Sebaliknya, *Response Cost* diterima, berpengaruh negatif, dan signifikan dengan nilai p-value (0,009) lebih kecil dari 0,05, dan nilai t-statistic sebesar 2,609 lebih besar dari 1,96, yang menunjukkan bahwa semakin besar persepsi individu terhadap biaya atau hambatan dalam menerapkan perilaku keamanan, maka tingkat kepatuhan akan menurun secara signifikan. Sementara itu, *Perceived Vulnerability*, *Response Efficacy*, dan *Self-Efficacy* tidak menunjukkan pengaruh yang signifikan. Secara keseluruhan, temuan ini menegaskan bahwa faktor ancaman dan hambatan perilaku lebih dominan dalam memengaruhi kepatuhan kebijakan keamanan informasi dibandingkan faktor efikasi dalam konteks penelitian ini.

5.2 Saran

Seiring dengan perkembangan teknologi informasi dan meningkatnya penggunaan sistem informasi dalam organisasi, permasalahan keamanan informasi menjadi isu yang semakin penting untuk diperhatikan. Berdasarkan hasil penelitian

ini, disarankan agar organisasi meningkatkan upaya dalam membangun kesadaran keamanan informasi kepada pengguna, khususnya terkait dampak serius yang dapat ditimbulkan akibat pelanggaran kebijakan keamanan informasi. Upaya tersebut dapat dilakukan melalui pelatihan, simulasi insiden keamanan, serta penyampaian kebijakan secara berkala.

Selain itu, organisasi disarankan untuk meninjau dan menyederhanakan kebijakan keamanan informasi agar lebih mudah dipahami dan diterapkan oleh pengguna. Pengurangan hambatan dalam penerapan kebijakan diharapkan dapat meningkatkan tingkat kepatuhan pengguna terhadap kebijakan keamanan informasi yang telah ditetapkan.

Bagi penelitian selanjutnya, disarankan untuk menambahkan variabel lain di luar *Protection Motivation Theory*, seperti faktor budaya organisasi, pengaruh manajemen, atau mekanisme pengawasan, guna memperoleh gambaran yang lebih luas mengenai faktor-faktor yang memengaruhi kepatuhan kebijakan keamanan informasi. Penelitian selanjutnya juga dapat dilakukan pada objek dan sektor yang berbeda agar hasil penelitian dapat dibandingkan dan digeneralisasikan dengan lebih baik.

DAFTAR PUSTAKA

Acquisti, A., Brandimarte, L., dan Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509-514. Retrieved from https://www.science.org/doi/abs/10.1126/science.aaa1465 doi: 10.1126/science.aaa1465

Akello, B. O. (2024, February). Organizational information security threats: Status and challenges. *World Journal of Advanced Engineering, Engineering Technology and Sciences*, *11*(1), 148–162.

AlGhamdi, S., Win, K. T., dan Vlahu-Gjorgievska, E. (2022). Employees' intentions toward complying with information security controls in saudi arabia's public organisations. *Government Information Quarterly*, *39*(4), 101721. Retrieved from https://www.sciencedirect.com/science/article/pii/S0740624X22000545 doi: https://doi.org/10.1016/j.giq.2022.101721

Alkhammash, R. (2023). Bibliometric, network, and thematic mapping analyses of metaphor and discourse in covid-19 publications from 2020 to 2022. *Frontiers in Psychology*, *Volume 13 - 2022*. Retrieved from https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2022.1062943 doi: 10.3389/fpsyg.2022.1062943

Alkhudhayr, F., Alfarraj, S., Aljameeli, B., dan Elkhdiri, S. (2019). Information security:a review of information security issues and techniques. Dalam (hal. 5). IEEE.

Al-Momani, A. M., Ramayah, T., dan Al-Sharafi, M. A. (2024). Exploring the impact of cybersecurity on using electronic health records and their performance among healthcare professionals: A multi-analytical sem-ann approach. *Technology in Society*, *77*, 102592. Retrieved from https://www.sciencedirect.com/science/article/pii/S0160791X24001404 doi: https://doi.org/10.1016/j.techsoc.2024.102592

Alraja, M. N., Butt, U. J., dan Abbod, M. (2023). Information security policies compliance in a global setting: An employee's perspective. *Computers & Security*, *129*, 103208. Retrieved from https://www.sciencedirect.com/science/article/pii/S0167404823001189 doi: https://doi.org/10.1016/j.cose.2023.103208

Alrawhani, E. M., Romli, A., dan Al-Sharafi, M. A. (2025). Evaluating the role of protection motivation theory in information security policy compli-

ance: Insights from the banking sector using pls-sem approach. *Journal of Open Innovation: Technology, Market, and Complexity*, *11*(1), 100463. Retrieved from https://www.sciencedirect.com/science/article/pii/S2199853124002579 doi: https://doi.org/10.1016/j.joitmc.2024.100463

Alzamil, Z. A. (2018). Information security practice in saudi arabia: A case study on saudi organizations. *Information and Computer Security*, *26*(5), 568–583. Retrieved from https://doi.org/10.1108/ICS-01-2018-0006 doi: 10.1108/ICS-01-2018-0006

Amrillah, A. (2023, Nov.). Code switching pada multilingual: Analisis bibliometrik pada tren penelitian. *Jurnal Sinestesia*, *13*(2). Retrieved from https://sinestesia.pustaka.my.id/journal/article/view/477

Angraini, Alias, R. A., dan Okfalisa. (2019). Information security policy compliance: Systematic literature review. *Procedia Computer Science*, *161*, 1216-1224. Retrieved from https://www.sciencedirect.com/science/article/pii/S1877050919319465 (The Fifth Information Systems International Conference, 23-24 July 2019, Surabaya, Indonesia) doi: https://doi.org/10.1016/j.procs.2019.11.235

Angraini, Alinda Alias, R., dan Okfalisa, O. (2019). Need for compliance with information security policy in universities: a preliminary survey. Dalam *2019 fourth international conference on informatics and computing (icic)* (hal. 1-6). doi: 10.1109/ICIC47613.2019.8985949

Aria, M., dan Cuccurullo, C. (2017). bibliometrix: An r-tool for comprehensive science mapping analysis. *Journal of Informetrics*, *11*(4), 959-975. Retrieved from https://www.sciencedirect.com/science/article/pii/S1751157717300500 doi: https://doi.org/10.1016/j.joi.2017.08.007

Ayulya, A. M., Syaifullah, S., Hamzah, M. L., Ahsyar, T. K., dan Saputra, E. (2024, 4). Developments and trends in indonesian tourism technology using bibliometric analysis. *IJCCS*, *18*(2).

Callon, M., Courtial, J.-P., Turner, W. A., dan Bauin, S. (1983). From translations to problematic networks: An introduction to co-word analysis. *Social Science Information*, *22*(2), 191-235. Retrieved from https://doi.org/10.1177/053901883022002003 doi: 10.1177/053901883022002003

Chowdhury, M. M., Rifat, N., Ahsan, M., Latif, S., Gomes, R., dan Rahman, M. S. (2023, May). Chatgpt: A threat against the cia triad of cyber security. Dalam *2023 ieee international conference on electro information technology (eit)*. IEEE. Retrieved from https://doi.org/10.1109/

eIT57321.2023.10187355 doi: 10.1109/eit57321.2023.10187355

de Veluz, M. R. D., Ong, A. K. S., Ngurah Perwira Redi, A. A., Maaliw, R. R., Lagrazon, P. G., dan Monetiro, C. N. (2025). Expanding integrated protection motivation theory and theory of planned behavior: The role of source of influence in flood and typhoon risk preparedness intentions in quezon province, philippines. *Climate Risk Management*, *48*, 100706. Retrieved from https://www.sciencedirect.com/science/article/pii/S2212096325000208 doi: https://doi.org/10.1016/j.crm.2025.100706

De Oliveira Albuquerque, R., Villalba, L. J. G., Orozco, A. L. S., Buiati, F., dan Kim, T.-H. (2014). A layered trust information security architecture. *Sensors*, *14*(12), 22754–22772. Retrieved from https://www.mdpi.com/1424-8220/14/12/22754 doi: 10.3390/s141222754

Donthu, N., Kumar, S., Mukherjee, D., Pandey, N., dan Lim, W. M. (2021). How to conduct a bibliometric analysis: An overview and guidelines. *Journal of Business Research*, *133*, 285-296. Retrieved from https://www.sciencedirect.com/science/article/pii/S0148296321003155 doi: https://doi.org/10.1016/j.jbusres.2021.04.070

Fornell, C., dan Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, *18*(1), 39-50. Retrieved from https://doi.org/10.1177/002224378101800104 doi: 10.1177/002224378101800104

Garfield, E. (1972). Citation analysis as a tool in journal evaluation. *Science*, *178*(4060), 471-479. Retrieved from https://www.science.org/doi/abs/10.1126/science.178.4060.471 doi: 10.1126/science.178.4060.471

Gaurav, Jayaram, N., Halder, S., Panda, K. P., dan Kishore, P. S. V. (2022). Design and analysis of a simplified non-isolated bidirectional dc-dc converter for energy storage systems. Dalam *2022 international conference on intelligent controller and computing for smart power (iciccsp)* (hal. 1-6). doi: 10.1109/ICICCSP53532.2022.9862364

Glänzel, W., dan Schubert, A. (2005). Analysing scientific networks through co-authorship. Dalam H. F. Moed, W. Glänzel, dan U. Schmoch (Eds.), *Handbook of quantitative science and technology research: The use of publication and patent statistics in studies of s&t systems* (hal. 257–276). Dordrecht: Springer Netherlands. Retrieved from https://doi.org/10.1007/1-4020-2755-9_12 doi: 10.1007/1-4020-2755-9_12

Gülmez, D., Özteke, İ., dan Gümüş, S. (2020, December). Overview of educational research from turkey published in international journals: A bibliometric analysis. *Education and Science*, *46*(206), 213–239. Retrieved from https://educationandscience.ted.org.tr/article/view/1967 doi: 10.15390/EB.2020.9317

Hair, J., Sarstedt, M., Ringle, C., dan Gudergan, S. (2017). *Advanced issues in partial least squares structural equation modeling*.

Hair, J., Sarstedt, M., Ringle, C., dan Gudergan, S. (2023). *Advanced issues in partial least squares structural equation modeling (2nd ed.)*.

Hair, J. F. (2019). When to use and how to report the results of PLS-SEM. , *31*(1), 2–24. doi: 10.1108/EBR-11-2018-0203

Hair, J. F., Hult, G. T. M., dan Ringle, C. M. (2017). *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*. SAGE Publications, Inc.

Hyland, K. (2016). Academic publishing and the myth of linguistic injustice. *Journal of Second Language Writing*, *31*, 58-69. Retrieved from https://www.sciencedirect.com/science/article/pii/S1060374316300054 doi: https://doi.org/10.1016/j.jslw.2016.01.005

Khaldi, H., dan Prado-Gascó, V. (2021, 10). Bibliometric maps and co-word analysis of the literature on international cooperation on migration. *Quality & Quantity*, *55*(5), 1845-1869.

Komara, D. A., Rohman, H. A., Rahmawaty, A. P., Giovanni, F., dan Mumtaz, S. R. (2025). Bibliometric analysis of research trends in information seeking on social media. , *3*(1), 18–35.

Koohang, A., Anderson, J., Nord, J. H., dan Paliszkiewicz, J. (2020). Building an awareness-centered information security policy compliance model. *Industrial Management & Data Systems*, *120*(1), 231–247. Retrieved from https://doi.org/10.1108/IMDS-07-2019-0412 doi: 10.1108/IMDS-07-2019-0412

Koolen, C., Wuyts, K., Joosen, W., dan Valcke, P. (2024). From insight to compliance: Appropriate technical and organisational security measures through the lens of cybersecurity maturity models. *Computer Law & Security Review*, *52*, 105914. Retrieved from https://www.sciencedirect.com/science/article/pii/S0267364923001243 doi: https://doi.org/10.1016/j.clsr.2023.105914

Kraus, S., Breier, M., dan Dasí-Rodríguez, S. (2020, September). The art of craft-

ing a systematic literature review in entrepreneurship research. *Int. Entrep.. Manag. J.*, *16*(3), 1023–1042.

Kuzior, A., Arefieva, O., Vovk, O., dan Brożek, P. (2022). Innovative development of circular systems while ensuring economic security in the industry. *Journal of Open Innovation: Technology, Market, and Complexity*, *8*(3), 139. Retrieved from https://www.sciencedirect.com/science/article/pii/S2199853122007405 doi: https://doi.org/10.3390/joitmc8030139

Lim, W. M., Kumar, S., dan Ali, F. (2022). Advancing knowledge through literature reviews: 'what', 'why', and 'how to contribute'. *The Service Industries Journal*, *42*(7-8), 481–513. doi: 10.1080/02642069.2022.2047941

Lundgren, B., dan Möller, N. (2017, November). Defining information security. *Science and Engineering Ethics*, *25*(2), 419–441. Retrieved from http://dx.doi.org/10.1007/s11948-017-9992-1 doi: 10.1007/s11948-017-9992-1

Maalej, A., dan Kallel, I. (2020, 07). Does keystroke dynamics tell us about emotions? a systematic literature review and dataset construction. Dalam (hal. 60-67). doi: 10.1109/IE49459.2020.9155004

Moody, G. D., Siponen, M., dan Pahnila, S. (2018, 03). Toward a unified model of information security policy compliance1. *Management Information Systems Quarterly*, *42*(1), 285-311. Retrieved from https://doi.org/10.25300/MISQ/2018/13853 doi: 10.25300/MISQ/2018/13853

NCSC, N. C. S. C. (2025, 12). *Ncsc annual review 2025 - ncsc.gov.uk*. Retrieved from https://www.ncsc.gov.uk/collection/ncsc-annual-review-2025 ([Online; accessed 2025-12-16])

Parlina, A., Ramli, K., dan Murfi, H. (2020, February 1). Theme mapping and bibliometrics analysis of one decade of big data research in the scopus database. *Information (Switzerland)*, *11*(2). doi: 10.3390/info11020069

Passas, I. (2024). Bibliometric Analysis : The Main Steps. , 1014–1025.

Patricia, E., Sánchez, B., Moya, I., Gabriela, C., dan Giner, R. (2024). Discover Sustainability Bibliometric analysis and systematic literature review of the relationship between sustainable development goals and sustainable entrepreneurship over time. *Discover Sustainability*(2025). Retrieved from https://doi.org/10.1007/s43621-024-00572-0 doi: 10.1007/s43621-024-00572-0

Qatawneh, N. (2024). Empirical insights into business intelligence adoption and decision-making performance during the digital transformation era: Ex-

tending the toe model in the jordanian banking sector. *Journal of Open Innovation: Technology, Market, and Complexity*, *10*(4), 100401. Retrieved from https://www.sciencedirect.com/science/article/pii/S2199853124001951 doi: https://doi.org/10.1016/j.joitmc.2024.100401

Rejeb, A., Rejeb, K., dan Treiblmaier, H. (2023). Mapping metaverse research: Identifying future research areas based on bibliometric and topic modeling techniques. *Information*, *14*(7). Retrieved from https://www.mdpi.com/2078-2489/14/7/356 doi: 10.3390/info14070356

Saputri, A. M., dan Syaifullah, S. (2024, 1). "developments and trends in cybersecurity against human factors and time pressure using bibliometric analysis". *"IJCCS"*, *18*(1), "107".

Shoufan, A., dan Damiani, E. (2017). On inter-rater reliability of information security experts. *Journal of Information Security and Applications*, *37*, 101-111. Retrieved from https://www.sciencedirect.com/science/article/pii/S2214212617301217 doi: https://doi.org/10.1016/j.jisa.2017.10.006

Small, H. (1973). Co-citation in the scientific literature: A new measure of the relationship between two documents. *Journal of the American Society for Information Science*, *24*(4), 265-269. Retrieved from https://asistdl.onlinelibrary.wiley.com/doi/abs/10.1002/asi.4630240406 doi: https://doi.org/10.1002/asi.4630240406

Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review*, *154*(3), 477–570.

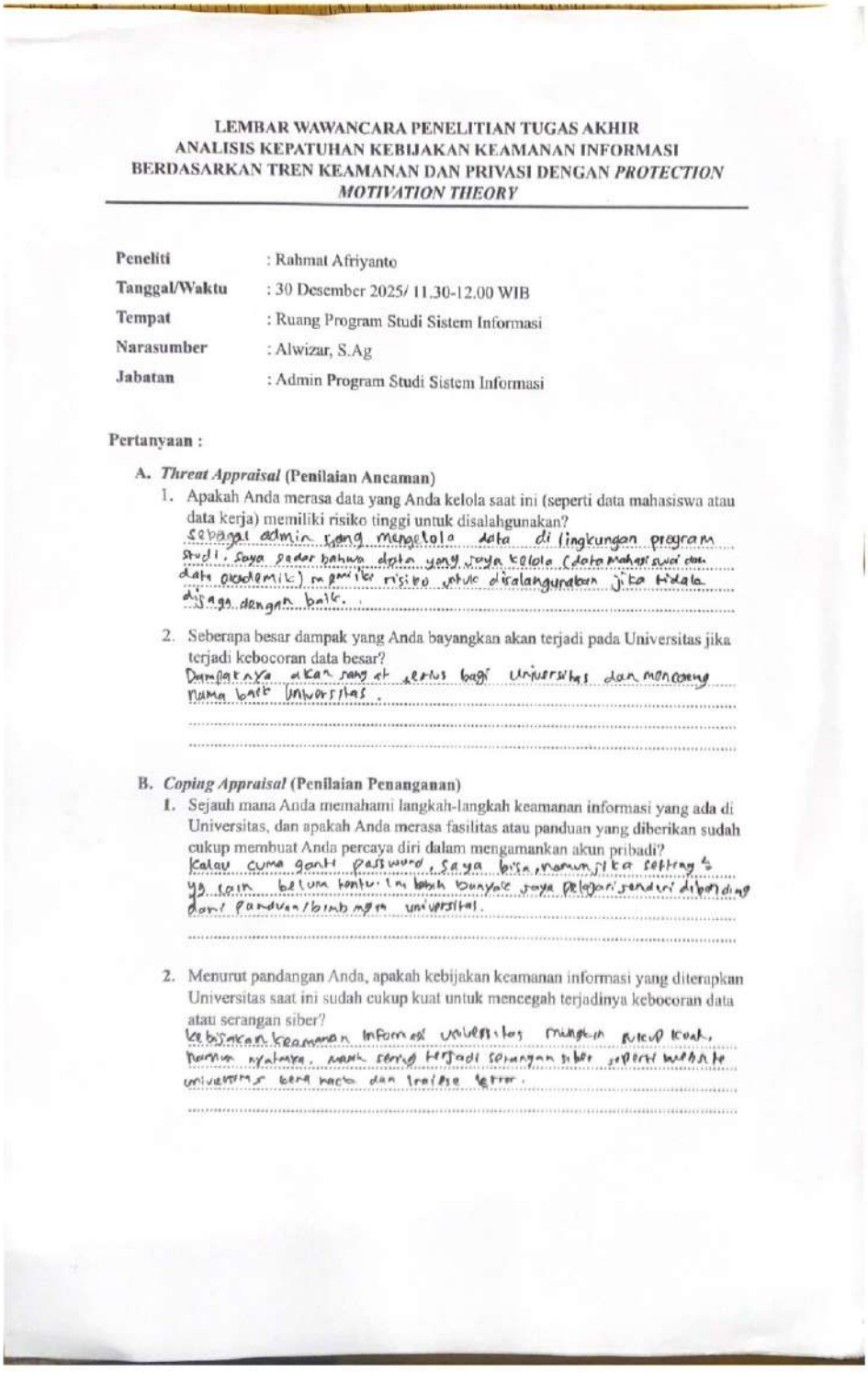
Spiekermann, S., dan Cranor, L. (2009, January). Engineering privacy. *IEEE Transactions on Software Engineering*, *35*(1), 67–82. Retrieved from http://doi.org/10.1109/TSE.2008.88 doi: 10.1109/tse.2008.88

Syaifullah, S., Ariffin, S. A., dan Nordin, N. M. (2024, Dec.). Mobile tourism research and practices: A comprehensive bibliometric exploration and future study direction. *Journal of Applied Engineering and Technological Science (JAETS)*, *6*(1), 21–47. Retrieved from https://journal.yrpipku.com/index.php/jaets/article/view/4970 doi: 10.37385/jaets.v6i1.4970

Symantec. (2017). *Internet security threat report istr.* Retrieved from https://docs.broadcom.com/doc/istr-22-2017-en ([Online; accessed 2025-12-16])

LAMPIRAN A
HASIL WAWANCARA

Gambar A.1. Wawancara



LEMBAR WAWANCARA PENELITIAN TUGAS AKHIR
ANALISIS KEPATUHAN KEBIJAKAN KEAMANAN INFORMASI
BERDASARKAN TREN KEAMANAN DAN PRIVASI DENGAN *PROTECTION MOTIVATION THEORY*

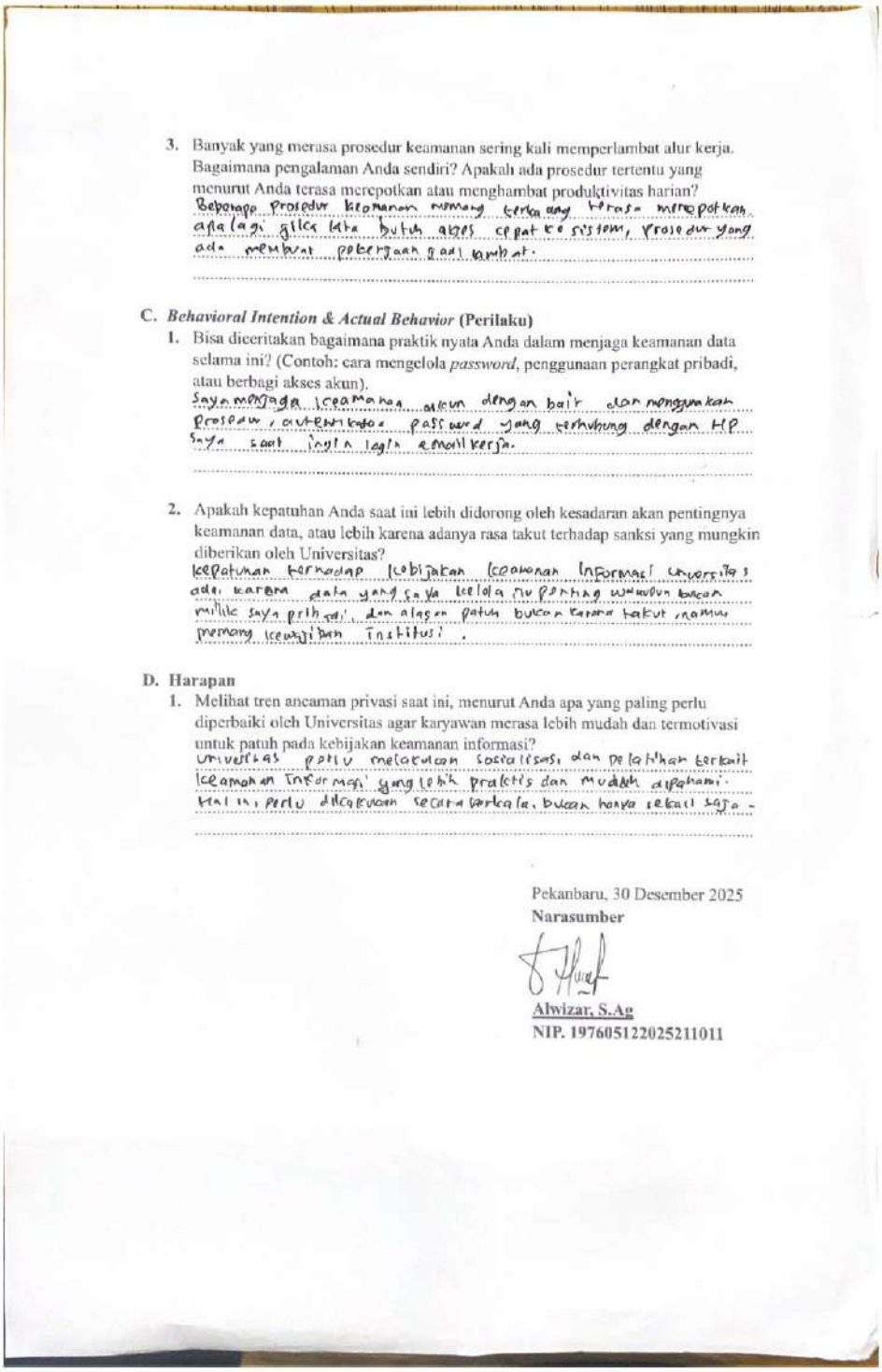
Peneliti : Rahmat Afriyanto
Tanggal/Waktu : 30 Desember 2025/ 11.30-12.00 WIB
Tempat : Ruang Program Studi Sistem Informasi
Narasumber : Alwizar, S.Ag
Jabatan : Admin Program Studi Sistem Informasi

Pertanyaan :

A. *Threat Appraisal* (Penilaian Ancaman)
1. Apakah Anda merasa data yang Anda kelola saat ini (seperti data mahasiswa atau data kerja) memiliki risiko tinggi untuk disalahgunakan?
   sebagai admin yang mengelola data di lingkungan program studi, saya sadar bahwa data yang saya kelola (data mahasiswa dan data akademik) memiliki risiko untuk disalahgunakan jika tidak dijaga dengan baik.
2. Seberapa besar dampak yang Anda bayangkan akan terjadi pada Universitas jika terjadi kebocoran data besar?
   Dampaknya akan sangat serius bagi universitas dan mencoreng nama baik universitas.

B. *Coping Appraisal* (Penilaian Penanganan)
1. Sejauh mana Anda memahami langkah-langkah keamanan informasi yang ada di Universitas, dan apakah Anda merasa fasilitas atau panduan yang diberikan sudah cukup membuat Anda percaya diri dalam mengamankan akun pribadi?
   Kalau cuma ganti password, saya bisa, namun jika setting yg lain belum bantu. Ini lebih banyak saya belajar sendiri dibanding dari panduan/bimbingan universitas.
2. Menurut pandangan Anda, apakah kebijakan keamanan informasi yang diterapkan Universitas saat ini sudah cukup kuat untuk mencegah terjadinya kebocoran data atau serangan siber?
   kebijakan keamanan informasi universitas mungkin cukup kuat, namun nyatanya, masih sering terjadi serangan siber, seperti website universitas yang mati dan terblokir.

Gambar A.2. Formulir Wawancara Halaman 1



3. Banyak yang merasa prosedur keamanan sering kali memperlambat alur kerja. Bagaimana pengalaman Anda sendiri? Apakah ada prosedur tertentu yang menurut Anda terasa merepotkan atau menghambat produktivitas harian?
   Beberapa prosedur keamanan memang terkadang terasa merepotkan, apalagi ketika kita butuh akses cepat ke sistem, prosedur yang ada membuat pekerjaan jadi lambat.

C. *Behavioral Intention & Actual Behavior* (Perilaku)

1. Bisa diceritakan bagaimana praktik nyata Anda dalam menjaga keamanan data selama ini? (Contoh: cara mengelola *password*, penggunaan perangkat pribadi, atau berbagi akses akun).
   Saya menjaga keamanan akun dengan baik dan menggunakan prosedur autentikasi password yang terhubung dengan HP saya saat ingin login email kerja.

2. Apakah kepatuhan Anda saat ini lebih didorong oleh kesadaran akan pentingnya keamanan data, atau lebih karena adanya rasa takut terhadap sanksi yang mungkin diberikan oleh Universitas?
   kepatuhan terhadap kebijakan keamanan informasi universitas ada karena data yang saya kelola itu penting untuk kepentingan publik saya pribadi dan alasan patuh bukan karena takut namun memang kewajiban institusi.

D. Harapan

1. Melihat tren ancaman privasi saat ini, menurut Anda apa yang paling perlu diperbaiki oleh Universitas agar karyawan merasa lebih mudah dan termotivasi untuk patuh pada kebijakan keamanan informasi?
   universitas perlu melakukan sosialisasi dan pelatihan terkait keamanan informasi yang lebih praktis dan mudah dipahami. hal ini perlu dilakukan secara berkala, bukan hanya sekali saja.

Pekanbaru, 30 Desember 2025
Narasumber

Alwizar, S.Ag
NIP. 197605122025211011

Gambar A.3. Formulir Wawancara Halaman 2

LAMPIRAN B

KUESIONER PENELITIAN

SURVEI KUESIONER PENELITIAN TUGAS AKHIR
ANALISIS KEPATUHAN KEBIJAKAN KEAMANAN INFORMASI BERDASARKAN TREN KEAMANAN DAN PRIVASI DENGAN PROTECTION MOTIVATION THEORY

Petunjuk Pengisian Kuesioner :

Responden diminta untuk memberikan jawaban yang sesuai dengan menandai ceklis (✓) dan penilaian dilakukan dengan menggunakan Skala Likert lima poin.

Keterangan :

Sangat Tidak Setuju (STS) Setuju (S)
Tidak Setuju (TS) Sangat Setuju (SS)
Netral (N)

Identitas Responden

Jenis Kelamin	☐ Laki-laki ☐ Perempuan
Usia	☐ < 25 Tahun ☐ 45-54 Tahun ☐ 25-34 Tahun ☐ > 55 Tahun ☐ 35-44 Tahun
Status Pekerjaan	☐ Dosen ☐ Tenaga Kependidikan ☐ Lainnya ……..……..……..……....
Unit Kerja	☐ Akademik ☐ Umum ☐ Keuangan ☐ Lainnya ……..……..……..……....
Apakah Anda pernah mengikuti pelatihan keamanan informasi?	☐ Pernah ☐ Tidak Pernah
Seberapa sering Anda menggunakan sistem informasi Universitas (Website Akademik FST, iRaise, E-Learning, dan lainnya) dalam pekerjaan sehari-hari?	☐ Jarang ☐ Kadang-kadang ☐ Sering ☐ Sangat Sering

Gambar B.1. Kuesioner Penelitian

Daftar Pernyataan

No	Pernyataan	STS	TS	N	S	SS
1.	Saya mengetahui langkah-langkah yang harus dilakukan untuk menjaga keamanan informasi di Universitas					
2.	Saya mampu mengikuti kebijakan keamanan informasi yang berlaku di Universitas					
3.	Saya percaya diri dalam mengamankan akun dan data kerja saya di Universitas					
4.	Kebijakan keamanan informasi Universitas efektif dalam melindungi data					
5.	Prosedur keamanan informasi dapat mencegah insiden keamanan informasi					
6.	Kepatuhan terhadap kebijakan keamanan informasi meningkatkan keamanan sistem Universitas					
7.	Penerapan kebijakan keamanan informasi Universitas menghambat pekerjaan saya					
8.	Prosedur keamanan informasi memerlukan waktu tambahan dalam pelaksanaan pekerjaan					
9.	Kepatuhan terhadap kebijakan keamanan informasi terasa merepotkan					
10.	Saya berpotensi mengalami insiden keamanan informasi saat menggunakan sistem informasi Universitas					
11.	Data yang saya kelola di Universitas berisiko bocor atau disalahgunakan					
12.	Akun atau perangkat kerja saya dapat menjadi target penyalahgunaan					
13.	Pelanggaran keamanan informasi dapat merugikan reputasi Universitas					
14.	Kebocoran data mahasiswa atau pegawai dapat menimbulkan dampak yang serius					
15.	Saya dapat dikenai sanksi jika melanggar kebijakan keamanan informasi Universitas					
16.	Saya mematuhi kebijakan keamanan informasi yang berlaku di Universitas					
17.	Saya tidak membagikan akun atau kata sandi kepada pihak lain					
18.	Saya mengikuti prosedur keamanan informasi saat mengelola data Universitas					

LAMPIRAN C
DOKUMENTASI

Gambar C.1. Dokumentasi Responden Kuesioner

DAFTAR RIWAYAT HIDUP

Rahmat Afriyanto lahir di Pekanbaru pada tanggal 24 September 2003. Peneliti merupakan anak dari Bapak Afrizal dan Ibu Triwati, serta merupakan anak terakhir dari tiga bersaudara. Pendidikan formal peneliti dimulai pada tahun 2010 di MIS Darul Ulum. Setelah menyelesaikan pendidikan Sekolah Dasar, peneliti melanjutkan pendidikan ke jenjang Sekolah Menengah Pertama di SMP Negeri 13 Pekanbaru dan lulus pada tahun 2019. Selanjutnya, peneliti menempuh pendidikan Sekolah Menengah Kejuruan di SMK Negeri 1 Pekanbaru dengan jurusan Teknik Komputer dan Jaringan. Setelah lulus pada tahun 2022, peneliti melanjutkan pendidikan ke jenjang Strata-1 sebagai Mahasiswa Program Studi Sistem Informasi, Fakultas Sains dan Teknologi, Universitas Islam Negeri Sultan Syarif Kasim Riau. Selama masa perkuliahan, peneliti aktif dalam berbagai kegiatan organisasi dan kepanitiaan, di antaranya tergabung dalam Information System Networking Club (ISNC) Research, serta Himpunan Mahasiswa Sistem Informasi (HIMASI). Tidak hanya berfokus pada pembelajaran di dalam kelas, peneliti turut mengikuti Program Merdeka Belajar Kampus Merdeka (MBKM) melalui studi independen bersertifikat di Bangkit Academy 2024 Batch 2 pada alur pembelajaran Cloud Computing. Peneliti menyelesaikan pendidikan Strata-1 setelah berhasil menuntaskan Tugas Akhir dengan judul "Analisis Kepatuhan Kebijakan Keamanan Informasi Berdasarkan Tren Keamanan Dan Privasi Dengan Protection Motivation Theory"