

**SOSIALISASI PENTINGNYA PENGENDALIAN DAN KEBIJAKAN KEAMANAN INFORMASI PADA MAHASISWA PROGRAM STUDI MANAJEMEN PENDIDIKAN ISLAM UIN STS JAMBI**

**Putri Rahmadani, Rian Pratama, Miko Septian**

Universitas Islam Negeri Sultan Thaha Saifuddin Jambi

Email: [rahmadaniputri41414@gmail.com](mailto:rahmadaniputri41414@gmail.com)

**Abstrak**

Kegiatan sosialisasi ini bertujuan untuk meningkatkan kesadaran, pemahaman, dan tanggung jawab mahasiswa Jurusan Manajemen Pendidikan Islam terhadap pentingnya pengendalian serta kebijakan keamanan informasi di era digital yang semakin maju dan dinamis. Perkembangan teknologi informasi yang begitu pesat membawa dampak besar terhadap pola komunikasi, penyimpanan data, serta aktivitas sehari-hari yang dilakukan secara daring. Kondisi ini menuntut adanya literasi digital yang kuat agar individu mampu mengenali potensi ancaman siber dan mengelola data pribadi secara aman. Melalui pendekatan deskriptif kualitatif, kegiatan ini dilaksanakan di Fakultas Tarbiyah dan Keguruan UIN Sulthan Thaha Saifuddin Jambi dengan melibatkan 18 mahasiswa angkatan 2024 sebagai peserta aktif. Materi sosialisasi disusun secara komprehensif mencakup konsep CIA Triad (Confidentiality, Integrity, Availability), prinsip kebijakan keamanan informasi, serta strategi pencegahan risiko kebocoran data dan penyalahgunaan identitas digital. Hasil kegiatan menunjukkan peningkatan signifikan dalam pengetahuan mahasiswa mengenai keamanan informasi, manajemen kata sandi, serta kesadaran akan pentingnya menjaga privasi dan etika berinternet. Selain itu, kegiatan ini juga membentuk perilaku digital yang lebih bijak, tanggap terhadap ancaman siber, serta mendorong terciptanya lingkungan akademik yang aman, etis, dan bertanggung jawab secara digital.

**Kata Kunci:** Keamanan Informasi, Sosialisasi, Mahasiswa, CIA Triad, Literasi Digital

**Abstract**

*This outreach activity (socialization) aims to increase the awareness, understanding, and responsibility of students majoring in Islamic Education Management regarding the importance of controls and information security policies in an increasingly advanced and dynamic digital era. The rapid development of information technology has brought a major impact on communication patterns, data storage, and daily activities conducted online. This condition necessitates strong digital literacy so that individuals are capable of identifying potential cyber threats and managing personal data securely. Using a qualitative descriptive approach, this activity was carried out at the Faculty of Tarbiyah and Teacher Training, UIN Sulthan Thaha Saifuddin Jambi, involving 18 students from the class of 2024 as active participants. The socialization material was compiled comprehensively, covering the CIA Triad concepts (Confidentiality, Integrity, Availability), principles of information security policy, and strategies for preventing data leakage risks and digital identity misuse. The results indicate a significant increase in student knowledge regarding information security, password management, and awareness of the importance of maintaining privacy*

**Article History**

Received: November 2025

Reviewed: November 2025

Published: November 2025

Plagiarism Checker No 579

Prefix DOI: Prefix DOI:

10.8734/sindoro.v1i2.360

Copyright: Author

Publish by: SINDORO



This work is licensed under a [Creative Commons Attribution-NonCommercial 4.0 International License](https://creativecommons.org/licenses/by-nc/4.0/).

|                                                                                                                                                                                                                                                                                                                                                    |  |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| <p><i>and internet ethics. Furthermore, this activity also fostered wiser digital behavior, responsiveness to cyber threats, and encouraged the creation of an academic environment that is secure, ethical, and digitally responsible.</i></p> <p><b>Keywords:</b> Information Security, Socialization, Students, CIA Triad, Digital Literacy</p> |  |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|

**Pendahuluan**

Arus gelombang globalisasi telah mendorong pertumbuhan ekponensial teknologi informasi yang masif di seluruh penjuru dunia, termasuk Indonesia (Wahidin & Wati, 2024). Arus deras globalisasi ini secara progresif menempatkan Indonesia sebagai suatu bagian yang tidak bisa dipisahkan dari lanskap informasi global, dengan aspirasi untuk membangun sebuah sistem informasi yang dicirikan oleh transparansi dan keterbukaan.

Implikasi dari arus globalisasi ini adalah percepatan perkembangan internet yang semakin hari semakin luas hingga tak terbatas, dimana setiap orang dapat mengakses dan memiliki kemudahan untuk menyebarkan beragam konten dan informasi (Nurlina et al., 2022). Tingkat ketergantungan publik terhadap ketersediaan informasi, khususnya yang beredar melalui platform media sosial, telah meningkat tajam hingga menjadi sebuah kebutuhan esensial.

Namun, dibalik banyaknya hal positif dari kecepatan perkembangan teknologi dan kemudahan untuk mendapatkan suatu informasi saat ini, kerentanan terhadap data pribadi tiap individu juga turut meningkat drastis (Sa’diyah et al., 2022). Oleh karena itu, percepatan penetrasi internet ini secara kritis menuntut hadirnya kerangka hukum yang relevan untuk menjamin keamanan dan privasi informasi individu, mengingat bahwa internet berfungsi sebagai arena publik yang dapat diakses oleh siapa pun.

Keberadaan platform media sosial selalu diterima dengan baik oleh pengguna internet sebagai wadah interaksi, baik itu secara langsung maupun tidak langsung, di ranah publik maupun privat. Eksistensi media sosial tidak dapat diabaikan karena ia berfungsi sebagai sarana untuk mengungkapkan ekspresi. Namun, pesatnya perkembangan teknologi berdampak pada peningkatan intensitas penggunaan media sosial yang sangat tinggi (Maryana et al., 2025).

Intensitas penggunaan ruang digital yang masif ini memerlukan adanya payung hukum dan kontrol yang kuat, tidak hanya untuk melindungi kebebasan berekspresi tetapi terutama untuk memastikan pengendalian dan kebijakan keamanan informasi (Pratiwi & Miarsa, 2025). Kehadiran regulasi ini mutlak diperlukan guna meminimalisir segala bentuk pelanggaran siber dan menjaga kerahasiaan data.

Dengan demikian, payung hukum tersebut berfungsi melindungi hak dan kepentingan warga negara, sekaligus merupakan manifestasi tanggung jawab negara dalam melindungi data serta kepentingan warganya dari ancaman kejahatan siber yang terus berkembang (UU No. 27 Tahun 2022 tentang PDP menjadi relevansi hukum utama).

Keamanan Informasi dapat didefinisikan sebagai sebuah kerentanan yang serius yang dapat menyebabkan kerugian signifikan bagi pemiliknya. Hal ini dikarenakan setiap informasi, yang merupakan aset penting, berisiko mengalami penyalahgunaan, pencurian, atau modifikasi oleh pihak yang tidak berwenang sehingga validitas dan kerahasiaannya patut dipertanyakan (Harahap, 2019).

Menurut ISO/IEC 27001:2022, Keamanan Informasi mencakup pemeliharaan Kerahasiaan, Integritas, dan Ketersediaan informasi. Ancaman terhadap keamanan informasi ini muncul dan berkembang seiring peningkatan aktivitas daring (online) serta disebabkan oleh beberapa faktor, di antaranya yaitu: kecerobohan pengguna dalam membagikan data pribadi di ruang publik, minimnya kesadaran literasi digital mengenai pentingnya mengidentifikasi risiko siber, serta rendahnya pemahaman teknis yang membuat seseorang rentan terhadap teknik rekayasa sosial (social engineering) (Palaloi & Rahman, 2024).

Mengingat tingginya potensi kerugian tersebut, ancaman terhadap Keamanan Informasi sendiri wajib dipahami secara komprehensif, sebab ancaman tersebut dapat diklasifikasikan menjadi beberapa jenis yang memiliki modus operandi dan tingkat bahaya yang berbeda-beda, di antaranya yaitu: ancaman berupa perangkat lunak berbahaya (malware), penipuan daring (phishing), serangan untuk melumpuhkan sistem (denial-of-service), serta risiko kebocoran data (data leakage) yang menyasar informasi sensitif (Sulaeman et al., 2023).

Pengendalian Keamanan Informasi adalah tindakan nyata dan terstruktur yang wajib dilakukan untuk menjamin kualitas aset informasi. Inti dari pengendalian ini adalah menjaga tiga pilar utama keamanan, yang dikenal sebagai CIA Triad (Supangkat et al., 2025). Pilar pertama, Kerahasiaan (Confidentiality), adalah perlindungan utama, memastikan data rahasia tidak bocor atau diakses oleh pihak yang tidak memiliki wewenang sama sekali. Selanjutnya adalah pilar Integritas (Integrity), yaitu jaminan bahwa data selalu utuh, akurat, dan tidak pernah diubah tanpa izin, baik saat data sedang dikirimkan maupun ketika disimpan. Pilar terakhir, Ketersediaan (Availability), memastikan bahwa sistem dan semua data pendukungnya selalu dapat diakses dan digunakan oleh pihak yang berhak, kapan pun mereka membutuhkannya—bahkan setelah terjadi serangan siber atau bencana (Harahap et al., 2023).

Jika salah satu dari tiga pilar CIA Triad ini gagal berfungsi karena pengendalian yang lemah, maka nilai informasi tersebut akan langsung jatuh dan kerugian besar akan segera terjadi. Oleh karena itu, semua kegiatan teknis ini harus didukung dan diatur oleh Kebijakan Keamanan Informasi yang kuat. Mengingat bahwa mahasiswa, khususnya Generasi Z, adalah kelompok dengan intensitas penggunaan media sosial dan interaksi digital paling tinggi (Santi et al., 2025), mereka menjadi kelompok yang paling rentan terhadap risiko siber. Oleh karena itu, sosialisasi mengenai pentingnya Pengendalian dan Kebijakan Keamanan Informasi pada mahasiswa merupakan langkah yang fundamental untuk membangun kesadaran dan ketahanan di garis depan ruang digital (Aprianti et al., 2025).

## **Metode Penelitian**

Berdasarkan permasalahan mengenai kerentanan siber dan perlunya penguatan kesadaran akan pentingnya keamanan informasi, maka perlu diterapkan kegiatan sosialisasi dan edukasi untuk meningkatkan wawasan para mahasiswa Jurusan Manajemen Pendidikan Islam terkait pentingnya pengendalian dan kebijakan keamanan informasi.

Kegiatan sosialisasi ini dilakukan di Gedung Kuliah Fakultas Tarbiyah dan Keguruan, pada tanggal 15 September 2025. Materi sosialisasi yang disampaikan disusun secara komprehensif, mencakup pemahaman mendalam mengenai CIA Triad (Kerahasiaan, Integritas, Ketersediaan) hingga bagaimana cara atau tindakan yang dapat dilakukan untuk menjaga keamanan informasi. Setelah kegiatan pemaparan materi selesai, kegiatan dilanjutkan dengan sesi tanya jawab dan berdiskusi. Sosialisasi ini berlangsung selama 120 menit dan diikuti oleh 18 orang

mahasiswa dari Program Studi Manajemen Pendidikan Islam angkatan 2024 di Universitas Islam Negeri Sulthan Thaha Saifuddin Jambi.

Secara teoritis, penelitian ini menerapkan pendekatan deskriptif berbasis kualitatif. Metode ini dipilih untuk mengamati keadaan mahasiswa khususnya angkatan 2024, pandangan mereka, serta peristiwa yang sedang berlangsung. Sejalan dengan hal tersebut, penelitian ini menggunakan pendekatan kualitatif deskriptif dengan fokus terhadap studi kasus (Ilhami, 2024).

## **Pelaksanaan Kegiatan**

### **1. Tahap Perencanaan**

Sebelum melaksanakan kegiatan sosialisasi, tahapan awal yang dilakukan adalah menetapkan jadwal kegiatan seperti waktu dan tempat pelaksanaan kegiatan yaitu di Universitas Islam Negeri Sulthan Thaha Saifuddin Jambi, Fakultas Tarbiyah dan Keguruan, Program Studi Manajemen Pendidikan Islam, dengan target audiens yaitu mahasiswa angkatan 2024 di ruang gedung kuliah. Setelah lokasi ditetapkan, kami merumuskan tujuan utama sosialisasi yaitu untuk meningkatkan pemahaman serta wawasan dan kesadaran mahasiswa mengenai pentingnya menjaga keamanan informasi dan urgensi kebijakan keamanan informasi di era digital saat ini mengingat juga bahwa para mahasiswa angkatan 2024 ini adalah generasi Z yang kehidupannya banyak menggunakan teknologi dalam kegiatan sehari-hari. Selanjutnya, mempersiapkan materi yang disesuaikan dengan tujuan awal kegiatan yang disesuaikan dengan tingkat pemahaman mahasiswa Jurusan Manajemen Pendidikan Islam sebagai pengguna aktif media sosial.

### **2. Tahap Pendahuluan**

Pada tahapan ini kami memperkenalkan konsep dan pengertian mengenai CIA Triad. Tahap awal kegiatan sosialisasi dimulai dengan Memperkenalkan konsep fundamental Keamanan Informasi, yaitu CIA Triad, dan alasan mengapa prinsip ini sangat penting untuk diterapkan. Kami memperkenalkan terlebih dahulu pilar-pilar utama, seperti Kerahasiaan (Confidentiality), lalu Integritas (Integrity), dan diakhiri dengan Ketersediaan (Availability). Dijelaskan juga mengapa pentingnya untuk menjaga ketiga pilar ini karena dapat melindungi informasi dari berbagai ancaman siber. Saat sesi penyampaian materi kepada Mahasiswa Jurusan Manajemen Pendidikan Islam UIN STS Jambi, kami tidak hanya memberikan teori, namun kami juga memberikan contoh praktis bagaimana implementasi Kerahasiaan (misalnya, penggunaan password manager) dan Integritas (misalnya, memverifikasi keaslian file sebelum diunduh).

Setelah memberikan contoh, kami juga mengulang kembali pemahaman mengenai CIA Triad kepada mahasiswa dengan melakukan sesi tanya jawab di sela-sela penyampaian materi agar mereka lebih paham lagi. Melalui sosialisasi ini mahasiswa diharapkan dapat mengembangkan penghargaan yang lebih besar terhadap nilai data dan kerahasiaannya, sehingga mendorong mereka agar lebih menghargai pentingnya menjaga keamanan informasi.

### **3. Tahap Pengenalan Isu**

Tahap berikutnya yaitu menjelaskan kenapa bahaya siber itu sangat penting untuk diketahui. Kepada mahasiswa, kami menjelaskan macam-macam kerugian dan masalah besar yang terjadi kalau data kita sampai dicuri atau diserang peretas. Kami memberikan contoh yang mudah dan nyata.

Contoh pertama yaitu tentang risiko uang dan data hilang. Kalau kita ceroboh dan tidak hati-hati membuang informasi penting (seperti kata sandi atau foto KTP) di internet, data itu sangat mudah diambil orang jahat. Ini ibaratnya seperti kita kehilangan kunci rumah. Ujung-ujungnya, uang mahasiswa bisa terkuras atau identitasnya dicuri, yang jelas bikin rugi besar. Misalnya, peretas bisa membajak akun media sosial kita yang isinya banyak rahasia, lalu dipakai untuk menipu teman-teman kita dengan cara pura-pura pinjam uang.

Contoh kedua itu tentang risiko nama baik atau reputasi. Misalnya, kalau mahasiswa tidak menjaga akun media sosialnya, dan akun itu dipakai orang lain untuk menyebar berita palsu atau kata-kata yang tidak pantas, ini bisa merusak nama baiknya di kampus. Hal ini bisa membuat mereka dapat sanksi dan masa depannya terganggu. Kedua contoh ini membuktikan bahwa kebiasaan buruk kita dalam mengelola data bisa menyebabkan masalah besar, bukan cuma untuk diri sendiri, tapi juga untuk lingkungan di sekitar kita.

#### **4. Tahapan Evaluasi dan Diskusi Interaktif**

Pada tahap akhir ini, sesi sosialisasi kami memasuki segmen interaktif, yaitu tanya jawab singkat. Sesi ini bukan hanya sekedar bertanya, tetapi juga merupakan alat ukur apakah teman-teman mahasiswa selama penyampaian materi mereka bisa menangkap inti materi dengan baik atau tidak. Tujuannya jelas yaitu untuk menilai seberapa jauh tingkat pemahaman mereka mengenai materi yang sudah disampaikan dan seberapa besar perhatian yang diberikan mahasiswa selama sesi berlangsung. Suasana menjadi lebih hidup dan kompetitif saat kami melemparkan pertanyaan-pertanyaan ringan namun fundamental, yang dirancang untuk memancing pemikiran kritis mereka. Beberapa pertanyaan pancingan yang kami sampaikan untuk memulai diskusi antara lain:

- a. Apa sih tujuan utama kita pasang kata sandi di perangkat elektronik, misalnya seperti HP dan Laptop?
- b. Biasanya, teman-teman kalau bikin kata sandi itu pakai nama panggilan, tanggal lahir, makanan/minuman favorit?
- c. Mana yang lebih aman: pakai satu kata sandi untuk semua akun medsos kita atau kata sandinya berbeda-beda untuk setiap akun?

Melalui interaksi yang cair ini, kami berharap konsep yang tadinya hanya teori bisa langsung tersimpan dalam ingatan jangka pendek serta jangka panjang mereka. Jika pemahaman dasar ini sudah kuat, akan lebih mudah bagi mereka untuk menerapkannya secara berulang sebagai kebiasaan baik dalam jangka panjang.

#### **Hasil dan Pembahasan**

Kegiatan sosialisasi mengenai pentingnya Pengendalian dan Kebijakan Keamanan Informasi ini dilaksanakan di gedung kuliah, Fakultas Tarbiyah dan Keguruan UIN STS Jambi dan diikuti oleh 18 mahasiswa Program Studi Manajemen Pendidikan Islam angkatan 2024. Sasaran ini dipilih secara spesifik karena dua alasan utama:

(1) sebagai mahasiswa yang aktif di era digital, mereka dituntut untuk memiliki literasi keamanan digital yang lebih tinggi.

(2) sebagai Generasi Z, mereka memiliki intensitas penggunaan media sosial yang sangat tinggi, menjadikan mereka kelompok yang paling rentan terhadap risiko siber.

Berdasarkan tahapan evaluasi yang dilakukan melalui sesi tanya jawab interaktif, teridentifikasi adanya peningkatan kesadaran dan pemahaman dasar yang signifikan di kalangan peserta. Sebelum sosialisasi, mayoritas mahasiswa cenderung meremehkan pentingnya keamanan kata sandi yang kuat (seperti tercermin dari kecenderungan

menggunakan nama panggilan atau tanggal lahir) dan masih banyak yang menggunakan satu kata sandi untuk berbagai akun. Hal ini menunjukkan tingkat kewaspadaan yang rendah terhadap pilar Kerahasiaan (Confidentiality) dalam CIA Triad.

Setelah sesi penyampaian materi dan diskusi, terjadi perubahan perspektif yang nyata, di antaranya:

- 1.) Peningkatan Pemahaman CIA Triad: Peserta mampu menjelaskan kembali dengan tepat tiga pilar utama keamanan informasi (Kerahasiaan, Integritas, Ketersediaan) dan memberikan contoh praktis penerapan masing-masing pilar dalam kegiatan digital sehari-hari.
- 2.) Perubahan Sikap Terhadap Kata Sandi: Mahasiswa menunjukkan pemahaman bahwa tujuan utama kata sandi adalah sebagai benteng pertama perlindungan (kunci rumah), bukan hanya formalitas. Mereka menyadari risiko besar dari penggunaan kata sandi tunggal.
- 3.) Kesadaran Risiko Reputasi dan Keuangan: Pemberian contoh kasus nyata mengenai dampak peretasan pada kerugian finansial dan reputasi di media sosial sangat efektif. Mahasiswa menunjukkan kekhawatiran yang lebih tinggi terhadap risiko-risiko tersebut, yang menjadi motivasi kuat untuk mengubah perilaku digital mereka.
- 4.) Penting untuk dicatat bahwa meskipun pemahaman teoritis meningkat, implementasi Kebijakan Keamanan Informasi yang komprehensif masih memerlukan pendampingan lebih lanjut. Sosialisasi ini berhasil menanamkan dasar kesadaran (awareness) yang menjadi fondasi utama sebelum mendorong adopsi kebijakan keamanan yang lebih ketat dan terstruktur.

## Kesimpulan

Kegiatan "Sosialisasi Pentingnya Pengendalian dan Kebijakan Keamanan Informasi" telah berhasil dilaksanakan pada mahasiswa Program Studi Manajemen Pendidikan Islam angkatan 2024 di UIN STS Jambi. Tujuan utama kegiatan ini, yaitu meningkatkan kesadaran dan literasi digital mahasiswa mengenai Keamanan Informasi, tercapai dengan baik.

Sosialisasi ini menyoroti pentingnya CIA Triad (Confidentiality, Integrity, Availability) sebagai kerangka kerja fundamental. Melalui sesi interaktif dan studi kasus sederhana, mahasiswa menunjukkan peningkatan pemahaman yang signifikan terhadap risiko siber, khususnya yang berkaitan dengan kerentanan data pribadi, potensi kerugian finansial, dan rusaknya reputasi digital. Hasil evaluasi menunjukkan bahwa mahasiswa kini memiliki apresiasi yang lebih tinggi terhadap pentingnya kebijakan keamanan yang ketat, terutama dalam pengelolaan kata sandi dan pencegahan terhadap t. Diharapkan dengan adanya kegiatan ini, mahasiswa UIN STS Jambi dapat menjadi agen perubahan yang menerapkan praktik keamanan digital yang baik dan bertanggung jawab, sehingga dapat meminimalisir risiko kejahatan siber di lingkungan kampus maupun publik.

## Dokumentasi



## Daftar Pustaka

- Apriani R., Sumardiono., Setiawan S., & Sudarsono T (2025). Sosialisasi Dan Edukasi Cyber Crime untuk Meningkatkan kesadaran Keamanan Digital Dan Cerdas berinternet Bagi Siswa. *Jurnal Pengabdian Masyarakat Ilmu Komputer*, 2(2), 116-123.
- Harahap A., Andani C., Christie A., Nurhaliza D., Fauzi A. (2023). Pentingnya Peranan CIA Triad Dalam Keamanan Informasi dan Data Untuk Pemangku Kepentingan atau Stakeholder. *Jurnal Manajemen dan Pemasaran Digital* 1(2), 73-83.
- Ilhami WM., Nurfajriani VW., Mahendra A., Sirodj A & Afgani WM.,  
Penerapan Metode Studi Kasus Dalam Penelitian Kualitatif. *Jurnal Ilmiah Wahana Pendidikan*, 10(9), 462-469.
- International Organization for Standardization (ISO). (2022). ISO/IEC 27001:2022 - Information Security, Cybersecurity and Privacy Protection.
- Palaloi & Rahman (2024). Analisis Dan Pencegahan Serangan Sosial Engineering Pada Jaringan Komputer Studi Kasus Penipuan Investasi Crypto. *Jurnal Riset Sistem Informasi*, 1(3), 8-16.
- Pratiwi FY., Miarsa FRD. (2025). Urgensi Edukasi Publik dalam Menangkal Penyalahgunaan Data Pribadi. *Journal of Artificial Intelligence and Digital Business (RIGGS)*, 4(2), 1342-1349.
- Maryana D., Boer M.K., Purwanti S., & Ibrizah Z. (2025). Dampak Penggunaan Media Sosial Terhadap Perilaku Phubbing Pada Mahasiswa Program Studi Ilmu Komunikasi Angkatan 2022. *Jurnal Teknologi dan Komputasi* 7(2), 30-53.
- Nurlina M., Anggraini A., Meriyandah (202). Hubungan intensitas Penggunaan Media Sosial Pada Tingkat Kecemasan Generasi Z Mahasiswa Keperawatan Di Stikes Medistra Indonesia tahun 2022. *Jurnal Ilmiah Kesehatan Mandira Cendikia* 1(1), 97-104.
- Republik Indonesia. (2022). *Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (UU PDP)*. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 226. Jakarta: Sekretariat Negara.

Sa'diyah M., Naskiyah., Rosyadi A.R, Hubungan Intensitas Penggunaan Media Sosial dengan Kesehatan Mental Mahasiswa dalam Pendidikan Agama Islam, 11(3), 713-730.

Santi M., Sholekah S., Hasanah S., Zainuddin M. & Khaer M (2025). Pendampingan Generasi Z dan Generasi Alpha Dalam Beretika di Media Sosial dan Pengamanan Akun Pribadi di Desa Bulusari Kedungwaru Tulungagung, 4(1), 25-38.

Sulaeman S., Utomo H., Suryana A (2023) Penilaian Risiko Keamanan Informasi Pada Sistem Informasi Akademik (Siakad) Dengan Menggunakan Framework NIST-SP 800 30. Prosiding Seminar Nasional Teknologi Komputer dan Sains, 1(1), 414-432.

Supangkat, F. (2025). Analisis Peran Kecerdasan Buatan Dalam Meningkatkan Keamanan Data Di Era Digital, 6(2), 159-169.

Wahidin & Wati (2024). Peluang Dan Tantangan Transformasi Digital Di Indonesia, 8(7), 311-322.