Jurnal Pengabdian dan Kewirausahaan
Versi Online: http://journal.ubm.ac.id
Hasil Pengabdian

Vol. 10 (No. 1): no. 057 - no 064. Th. 2026
p-ISSN: 2581 - 2718
e-ISSN: 2620 - 3480

BIMBINGAN DAN DUKUNGAN PENERAPAN PENGGUNA TEKNOLOGI PADA PERUSAHAAN KONSULTAN TI

Guidance and Support for Technology User Implementation in IT Consulting Companies

Francka Sakti Lee[1)*], Johanes Fernandes Andry[1)], Johanes Terry[1)], Callista Chrestella Liawen[1)] dan Jennifer Theresia[1)]

[1)]Program Studi Sistem Informasi, Fakultas Teknologi dan Desain, Universitas Bunda Mulia

Diajukan 17 Januari 2026 / Disetujui 10 April 2026

Abstrak

Brainware merujuk pada individu yang terlibat langsung dalam mengoperasikan, mengorganisir, dan mengelola sistem komputer, yang merupakan komponen penting dari sistem informasi. Prosedur Operasi Standar (SOP) adalah dokumen yang menjelaskan tanggung jawab dan cara setiap tugas dilakukan untuk mendukung pencapaian tujuan spesifik perusahaan. Kebijakan Keamanan IT berperan dalam menerapkan langkah-langkah yang diperlukan untuk meminimalkan dan mengantisipasi potensi ancaman terhadap informasi rahasia perusahaan. Meningkatkan keamanan data konsumen bukan hanya tanggung jawab individu tetapi juga organisasi dalam membangun kepercayaan konsumen dan mematuhi peraturan. Berbagai risiko yang ada dan variasinya menjadi perhatian bagi semua perusahaan. Peningkatan penggunaan internet telah menyebabkan peningkatan pelanggaran data akibat lebih banyak serangan siber. Perusahaan saat ini menghadapi ancaman yang dapat membahayakan reputasi mereka, menyoroti peran brainware dalam menangani ancaman ini. Oleh karena itu, kesadaran dan pengetahuan setiap individu diperlukan untuk memotivasi penerapan langkah-langkah mengatasi ancaman ini. Kebijakan Keamanan IT dapat diterapkan dengan harapan semua pihak yang terlibat mengetahui tanggung jawab spesifik mereka dalam perusahaan. Ini diperlukan untuk menjaga ekosistem teknologi dalam organisasi perusahaan.
Kata Kunci: IT Security Policy, SOP, Keamanan, Risiko

Abstract

Brainware refers to individuals directly involved in operating, organizing, and managing computer systems, which are a crucial component of an information system. Standard Operating Procedures (SOPs) are documents that explain responsibilities and how each task is performed to support specific company goals. An IT Security Policy plays a role in implementing the necessary measures to minimize and anticipate potential threats to a company's confidential information. Enhancing consumer data security is not only an individual's responsibility but also the organization's in building consumer trust and complying with regulations. The variety and variability of risks are concerns for all companies. The increasing use of the internet has led to a rise in data breaches caused by more cyberattacks. Companies today face threats that can jeopardize their reputation, highlighting the role of brainware in addressing these threats. Therefore, awareness and knowledge of each individual are necessary to motivate the implementation of steps to overcome these threats. An IT Security Policy can be implemented with the expectation that all parties involved know their specific responsibilities within a company. This is necessary to maintain the technological ecosystem within a corporate organization.
Keywords: *IT Security Policy, SOP, Security, Risk*

Pendahuluan

Perkembangan teknologi informasi yang pesat memberikan berbagai kemudahan dalam operasional organisasi, namun juga meningkatkan risiko terhadap keamanan data dan informasi (Lee et al., 2022). Salah satu faktor utama yang mempengaruhi keamanan informasi adalah brainware, yaitu individu yang mengoperasikan dan mengelola sistem komputer (Lee et al., 2024). Kesalahan yang dilakukan oleh pengguna, baik secara sengaja maupun tidak sengaja, dapat menjadi

*Korespondensi Penulis:
E-mail: flee@bundamulia.ac.id

Vol. 10 (No. 1): no. 057 - no 064. Th. 2026
p-ISSN: 2581 - 2718
e-ISSN: 2620 - 3480

celah terjadinya kebocoran data, terutama melalui serangan social engineering (Hapsari et al., 2023).

Pada perusahaan konsultan teknologi informasi, ancaman keamanan seperti social engineering menjadi risiko yang signifikan karena karyawan berperan langsung dalam pengelolaan data proyek yang bersifat sensitif (Aditya et al., 2022). Kondisi ini dapat menyebabkan kerugian finansial, penurunan reputasi, serta hilangnya kepercayaan dari klien apabila tidak ditangani dengan baik (Lee et al., 2020). Oleh karena itu, diperlukan upaya untuk meningkatkan kesadaran dan pemahaman karyawan terhadap pentingnya keamanan informasi melalui penerapan kebijakan dan prosedur yang tepat (Sockin et al., 2022).

Kegiatan ini merupakan bentuk pengabdian kepada masyarakat (PKM) yang dilakukan pada sebuah perusahaan konsultan TI sebagai mitra. Permasalahan utama yang dihadapi mitra meliputi rendahnya pemahaman karyawan terhadap kebijakan keamanan informasi, belum optimalnya penerapan SOP keamanan, serta tingginya risiko kebocoran data akibat serangan social engineering (Lee et al., 2023), (Sudarsono et al., 2023).

Berdasarkan permasalahan tersebut, kegiatan ini bertujuan untuk: (1) meningkatkan pemahaman karyawan terhadap IT Security Policy, (2) memberikan pendampingan dalam penerapan praktik keamanan informasi, serta (3) menyusun rekomendasi kebijakan dan prosedur keamanan yang sesuai dengan kebutuhan mitra.

Profil Mitra

Mitra dalam kegiatan ini adalah sebuah perusahaan konsultan teknologi informasi yang bergerak dalam pengembangan sistem dan layanan digital. Perusahaan ini memiliki sejumlah karyawan yang berperan sebagai programmer dan tim teknis yang secara langsung mengelola data proyek klien. Berdasarkan hasil observasi awal, mitra menghadapi beberapa permasalahan utama, yaitu:

1. Belum adanya pemahaman yang merata terkait kebijakan keamanan informasi,
2. Belum terdokumentasinya SOP keamanan secara sistematis, dan
3. Rendahnya kesadaran terhadap risiko serangan social engineering.

Kondisi ini menjadi dasar dilaksanakannya kegiatan pendampingan untuk meningkatkan kesiapan mitra dalam menghadapi ancaman keamanan informasi.

Metode Penelitian

Metode yang digunakan dalam kegiatan ini adalah kualitatif studi kasus dengan pendekatan eksploratif. Pendekatan ini dipilih untuk memperoleh pemahaman yang mendalam terkait permasalahan keamanan informasi yang disebabkan oleh faktor brainware dalam konteks organisasi perusahaan konsultan TI. Studi kasus memungkinkan peneliti untuk mengkaji fenomena secara spesifik dan kontekstual berdasarkan kondisi nyata di lapangan (Widhagdha et al., 2022).

Untuk meningkatkan validitas dan mengurangi bias yang sebelumnya hanya bergantung pada satu informan, penelitian ini menerapkan triangulasi sumber dan metode, dengan memadukan data primer dan sekunder. Selain itu, proses kajian juga diperkuat dengan telaah literatur yang relevan untuk memastikan keterkaitan antara teori dan praktik (Assyakurrohim et al., 2010).

Gambar 1.Skema Proses

Tahapan penelitian digambarkan dengan skema proses pada Gambar 1, dalam kegiatan ini dijelaskan secara sistematis sebagai berikut:

1. Identifikasi masalah, yaitu potensi kebocoran data akibat kesalahan manusia (*human error*/*brainware*) (Widodo et al., 2022).
2. Pengumpulan data, melalui wawancara, observasi, dokumentasi, dan kuesioner.
3. Analisis data, menggunakan teknik *thematic analysis*, yaitu mengelompokkan data ke dalam kategori utama: kebijakan (*policy*), aktivitas, permasalahan (*problem*), dan solusi (*solution*) (Bratha, 2022)..
4. Validasi data, dilakukan melalui triangulasi antara hasil wawancara, data dokumentasi, serta referensi literatur dan praktik umum di industri.

Teknik pengumpulan data yang digunakan meliputi:

1. Wawancara semi-terstruktur, dilakukan terhadap satu informan utama yaitu seorang *programmer* pada perusahaan konsultan TI. Wawancara bertujuan untuk menggali informasi terkait kebijakan keamanan (IT *Security Policy*), SOP, aktivitas harian, serta potensi kegagalan *brainware* (Nurdin et al., 2022)..
2. Observasi terbatas, dilakukan terhadap praktik kerja harian (*daily activity*) yang berkaitan dengan penerapan keamanan informasi (Anggraini et al., 2023).
3. Dokumentasi, berupa analisis dokumen internal seperti SOP, kebijakan keamanan, serta praktik kerja yang berlaku di perusahaan.
4. Kuesioner (*Google Form*), digunakan untuk memperkuat temuan terkait tingkat kesadaran keamanan (*security awareness*) sebagai bentuk validasi tambahan dari data wawancara.

Meskipun penelitian ini berfokus pada satu organisasi, pendekatan yang digunakan dirancang untuk menghasilkan insight kontekstual yang tetap memiliki relevansi dan potensi replikasi pada organisasi sejenis, khususnya dalam konteks peningkatan kesadaran keamanan informasi berbasis brainware (Afifi, 2020). Penelitian ini memiliki keterbatasan pada jumlah informan yang terbatas, namun untuk mengurangi bias, data diperkuat melalui triangulasi dengan literatur dan praktik standar keamanan informasi. Dengan demikian, hasil yang diperoleh tidak hanya bersifat deskriptif, tetapi juga memiliki dasar konseptual yang kuat.

Kondisi ini menjadi dasar dilaksanakannya kegiatan pendampingan untuk meningkatkan kesiapan mitra dalam menghadapi ancaman keamanan informasi. Selain pengumpulan data, kegiatan ini juga mencakup intervensi pengabdian berupa:

1. Penyuluhan terkait IT *Security Policy*,
2. Pendampingan penerapan praktik keamanan informasi,
3. Diskusi dan evaluasi bersama mitra terkait risiko keamanan, serta
4. Penyusunan rekomendasi kebijakan dan SOP keamanan.

Kegiatan dilaksanakan secara bertahap dan sistematis, dengan melibatkan partisipasi aktif karyawan sebagai peserta utama dalam proses pendampingan dan penerapan keamanan informasi.

Hasil Dan Pembahasan

Proses

1. ***IT Security Policy***

IT *Security Policy* yang ada pada perusahaan konsultan TI yaitu larangan untuk memperjual-belikan data projek yang bertujuan untuk menjaga kerahasiaan dan privasi dari projek yang sedang dikerjakan, mempertahankan kepercayaan pelanggan yang bertujuan untuk membangun hubungan yang lebih kuat, mempertahankan reputasi sebagai perusahaan yang bertanggung jawab, dapat diandalkan, dan meningkatkan *value* perusahaan.

2. ***Daily Activities***

Daily activities yang dijalankan pada perusahaan konsultan TI yaitu mengadakan scrum meeting atau disebut dengan *daily scrum* saat akan mulai kerja yang merupakan salah satu prosedur sehari-hari yang bertujuan untuk membangun komunikasi yang terbuka antar karyawan untuk mengetahui perkembangan pekeraan masing-masing, mendorong rasa kebersamaan, rasa saling support, dan motivasi antar tim. Mereka juga melakukan *progress report* sebelum jam kerja selesai yang akan meningkatkan akuntabilitas dan kemajuan kerja demi membangun rasa tanggung jawab individu atas perkerjaannya.

3. ***Problem***

Permasalahan yang terjadi diperusahaan konsultan TI berdasarkan narasumber potensi kebocoran data/informasi yang disebabkan oleh *social engineering* yang menjadi salah satu tantangan yang cukup sulit untuk diatasi. Singkatnya, *social engineering* adalah teknik manipulasi agar seseorang memberikan informasi rahasia tanpa mereka sadari, lalu data tersebut disalahgunakan untuk iklan. Bisa juga digunakan atau diperjualbelikan secara ilegal. Apabila kebocoran terjadi itu sangat merugikan pengguna dan perusahaan karena dapat merusak citra, reputasi dan kepercayaan publik.

4. ***Solution***

Berdasarkan permasalahan kebocoran data yang diidentifikasi pada perusahaan mitra, kegiatan pengabdian ini memberikan beberapa bentuk intervensi yang terarah. Pertama, dilakukan penyuluhan dan edukasi terkait keamanan informasi untuk meningkatkan kesadaran karyawan dalam menjaga kerahasiaan data serta menghindari praktik yang berisiko, seperti membagikan informasi sensitif secara tidak sengaja. Kedua, dilakukan pendampingan dalam penerapan kebijakan keamanan informasi, termasuk sosialisasi IT *Security Policy* dan penyusunan rekomendasi SOP keamanan yang lebih terstruktur dan mudah dipahami oleh seluruh karyawan. Ketiga, tim memberikan rekomendasi implementasi kontrol keamanan teknis, seperti penggunaan *multi-factor authentication* (MFA) untuk mengurangi risiko akses tidak sah, serta penerapan prosedur backup data secara berkala untuk meminimalkan dampak kehilangan data.

Selain itu, dilakukan *diskusi* dan evaluasi bersama mitra terkait potensi risiko social engineering serta langkah-langkah mitigasi yang dapat diterapkan dalam aktivitas kerja sehari-hari. Melalui rangkaian intervensi tersebut, mitra memperoleh pemahaman yang lebih baik mengenai pentingnya keamanan informasi serta mulai menerapkan praktik keamanan dasar dalam operasional organisasi.

5. **Model Keterkaitan Masalah–Intervensi–Luaran**

Untuk memperjelas hubungan antara permasalahan yang ditemukan dengan solusi yang diusulkan serta luaran yang diharapkan, maka disusun model keterkaitan yang ditampilkan pada Tabel 1:

Tabel 1. Model Keterkaitan

Masalah	Intervensi	Luaran
Kebocoran data akibat social engineering	Pelatihan *security awareness*	Peningkatan pemahaman karyawan
Kurangnya kontrol akses	Implementasi MFA (*Multi-Factor Authentication*)	Penurunan risiko akses ilegal
Tidak adanya SOP jelas	Penyusunan SOP keamanan	Standarisasi proses kerja
Rendahnya kesadaran keamanan	Edukasi dan simulasi serangan	Perubahan perilaku pengguna

Model ini menunjukkan bahwa setiap permasalahan yang diidentifikasi memiliki intervensi yang spesifik dan terarah, serta menghasilkan luaran yang dapat diukur baik secara kualitatif maupun kuantitatif.

6. **Indikator Keberhasilan Progam**

Untuk mengukur efektivitas kegiatan yang telah dilakukan, ditetapkan beberapa indikator keberhasilan yang mencerminkan perubahan pada aspek pengetahuan, perilaku, kepatuhan, teknis, dan organisasi, sebagai berikut:

a. Indikator Pengetahuan
   Peningkatan pemahaman karyawan terhadap IT Security Policy yang diukur melalui kuesioner sebelum dan sesudah kegiatan.
b. Indikator Perilaku

Penurunan praktik tidak aman, seperti menyimpan password di *browser* atau membiarkan perangkat dalam kondisi tidak terkunci.

c. Indikator Kepatuhan
Meningkatnya tingkat kepatuhan terhadap SOP keamanan yang telah ditetapkan dalam aktivitas kerja harian.

d. Indikator Teknis
Implementasi kontrol keamanan, seperti penggunaan *Multi-Factor Authentication* (MFA), mekanisme *backup data*, dan enkripsi.

e. Indikator Organisasi
Tersusunnya dokumen kebijakan keamanan, seperti SOP dan *Non-Disclosure Agreement* (NDA), sebagai bentuk standarisasi keamanan informasi.

Indikator-indikator ini digunakan sebagai dasar evaluasi terhadap keberhasilan intervensi yang dilakukan, sehingga hasil kegiatan tidak hanya bersifat deskriptif, tetapi juga dapat diukur secara sistematis dan memberikan gambaran peningkatan kualitas keamanan informasi dalam organisasi.

Berdasarkan indikator yang telah ditetapkan, hasil kegiatan menunjukkan adanya peningkatan pemahaman keamanan informasi sebesar ±30% berdasarkan kuesioner internal. Selain itu, terjadi peningkatan kepatuhan terhadap SOP keamanan dalam aktivitas kerja harian. Dari aspek teknis, organisasi juga mulai mengimplementasikan kontrol keamanan dasar, seperti penggunaan autentikasi ganda (multi-factor authentication) dan prosedur backup data secara berkala. Hasil ini menunjukkan bahwa intervensi yang dilakukan tidak hanya meningkatkan aspek pengetahuan, tetapi juga berdampak pada perubahan perilaku dan penerapan praktik keamanan informasi dalam organisasi.

Hasil ini menunjukkan bahwa kegiatan pendampingan yang dilakukan memberikan dampak langsung terhadap peningkatan pemahaman dan perubahan perilaku mitra dalam menerapkan praktik keamanan informasi.

7. Pembahasan

a. IT *Security Policy Implementation*

Saat IT *security policy* (ISP) sudah dibuat dan disusun, penting sekali untuk memastikan bahwa kebijakan tersebut bukan hanya sekedar tulisan, namun merupakan pengalaman nyata yang nantinya akan dialami oleh semua pihak yang terlibat. Mengkomunikasikan IT *security policy* kepada seluruh karyawan, memberikan pelatihan, dan memantau ketika policy tersebut dijalankan serta memapaparkan dengan jelas berupa tanggung jawab dan harapan secara spesifik kepada semua orang di organisasi dapat memberikan manfaat dalam menjaga ekosistem teknologi informasi yang terdapat pada organisasi tersebut.

Tujuan utama dari pelatihan adalah untuk memastikan setiap individual memiliki keahlian, kemampuan, dan pengetahuan yang diperlukan dalam implementasi *security policy*, dibalik dari tujuan utama tersebut, kesadaran tiap karyawan akan pentingnya untuk mematuhi *security policy* yang ada harus dibangun karena umumnya kebijakan yang ada akan dipatuhi jika karyawan memiliki pemahaman terhadap kebijakan-kebijakan tersebut. Pelatihan, edukasi, komitmen, keterlibatan, partisipasi serta pemberdayaan menjadi faktor utama dalam mencapai kesuksesan (Assen, 2021).

Berdasarkan hasil evaluasi yang telah diperoleh, temuan ini menunjukkan bahwa faktor manusia (*brainware*) merupakan titik kritis dalam keamanan informasi, sejalan dengan konsep "human as weakest link" (Selvam, 2020). Intervensi berbasis edukasi dan kebijakan terbukti lebih efektif ketika dikombinasikan dengan kontrol teknis, sehingga pendekatan holistik diperlukan dalam implementasi keamanan informasi. Hal ini mengindikasikan bahwa peningkatan kesadaran dan kepatuhan pengguna harus menjadi prioritas utama dalam strategi keamanan informasi organisasi.

b. McCumber *Cube*

Keamanan sistem informasi harus memiliki jaminan perlindungan terhadap resiko-resiko yang dapat menyebabkan kebobolan dalam akses, penggunaan, gangguan, modifikasi, ataupun penghancuran informasi yang dilakukan oleh orang yang tidak bertanggung jawab. John McCumber

memperkenalkan kerangka kerja yang disebut McCumber Cube pada tahun 1991, yang digunakan untuk mengatur tindakan keamanan dan perlindungan. Keamanan informasi dalam organisasi dapat dipahami melalui prinsip dasar yang menekankan pada aspek kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*). Prinsip ini menunjukkan bahwa data harus terlindungi dari akses tidak sah, tetap akurat, serta tersedia saat dibutuhkan. Dalam konteks kegiatan ini, penerapan kebijakan keamanan, pelatihan pengguna, dan kontrol teknis seperti autentikasi ganda menjadi langkah penting dalam menjaga ketiga aspek tersebut secara terpadu.

c. *Using and Enforcing Security Policies*

Penerapan dan penegakan kebijakan keamanan informasi merupakan aspek penting dalam menjaga keamanan sistem organisasi (Nugroho et al., 2023). Dalam kegiatan ini, kebijakan keamanan tidak hanya dipahami sebagai aturan tertulis, tetapi juga sebagai praktik yang harus diterapkan secara konsisten dalam aktivitas kerja sehari-hari.

Melalui kegiatan pendampingan, mitra diberikan pemahaman mengenai pentingnya kontrol akses, perlindungan data, serta penerapan kebijakan keamanan dalam penggunaan sistem. Selain itu, dilakukan sosialisasi terkait praktik penggunaan sistem yang aman untuk meminimalkan risiko akses tidak sah dan kesalahan pengguna (*human error*).

Hasil kegiatan menunjukkan bahwa karyawan mulai memahami pentingnya kepatuhan terhadap kebijakan keamanan, serta mulai menerapkan praktik yang lebih aman dalam penggunaan sistem. Hal ini sejalan dengan temuan bahwa penerapan kebijakan yang disertai edukasi dan pengawasan yang baik dapat meningkatkan keamanan informasi dalam organisasi.

Dengan demikian, penerapan kebijakan keamanan yang efektif memerlukan kombinasi antara aturan yang jelas, peningkatan kesadaran pengguna, serta evaluasi yang dilakukan secara berkelanjutan sesuai dengan kebutuhan organisasi.

d. *IT Security Policy Compliance Habits Impact*

Information Security Policy pada umumnya diperuntukkan untuk melindungi suatu sistem informasi, tidak memungkiri bahwa faktanya *brainware* merupakan *weakest link* atau rantai terlemah dalam keamanan dan jaminan informasi. Saat kebijakan sedang dikembangkan, organisasi harus mengerti bagaimana kebijakan tersebut akan memberi dampak kepada karyawan (Nord et al., 2012).

Kepatuhan terhadap kebijakan keamanan informasi merupakan aspek krusial dalam menjaga *integrity*, *confidentiality*, *availability* (McCumber Cube *Foundational Principle*). Karyawan yang mematuhi kebijakan ini cenderung lebih waspada terhadap ancaman dan menghindari tindakan berisiko yang dapat membahayakan sistem informasi (Baloyi, 2020). Dalam praktiknya, kebiasaan tidak mematuhi kebijakan keamanan informasi dapat menimbulkan celah yang cukup signifikan terhadap keamanan dan jaminan informasi dalam suatu organisasi yang dapat menyebabkan timbulnya insiden keamanan seperti pelanggaran data, serangan siber, dan hilangnya informasi penting. Selain itu, pelatihan keamanan kepada karyawan yang kurang baik merupakan penyebab utama kelemahan keamanan informasi dan kegagalan dan keberlanjutan (Mee et al., 2021).

Penanaman kesadaran akan kepatuhan kebijakan keamanan informasi dapat berfungsi sebagai fondasi yang kokoh dalam melindungi organisasi dan ancaman keamanan data yang semakin melonjak dan terus berkembang.

e. *Compliance Laws*

Kepatuhan terhadap kebijakan keamanan informasi merupakan aspek penting dalam menjaga keamanan sistem organisasi. Karyawan yang memahami dan mematuhi kebijakan cenderung lebih waspada terhadap potensi ancaman serta menghindari praktik yang berisiko. Dalam kegiatan ini, peningkatan kesadaran dan kepatuhan terhadap kebijakan menjadi salah satu fokus utama, karena faktor manusia merupakan titik lemah yang paling sering dimanfaatkan dalam serangan siber.

f. Dampak Intervensi kepada Mitra

Kegiatan pendampingan yang dilakukan memberikan dampak nyata terhadap mitra, khususnya dalam peningkatan pemahaman dan kesadaran keamanan informasi. Berdasarkan hasil evaluasi, terjadi peningkatan pemahaman sebesar ±30% serta perubahan perilaku dalam praktik penggunaan sistem yang lebih aman.

Selain itu, mitra juga mulai menerapkan kontrol keamanan dasar seperti autentikasi ganda dan prosedur backup data. Hal ini menunjukkan bahwa intervensi yang diberikan tidak hanya bersifat konseptual, tetapi juga memberikan manfaat praktis dalam meningkatkan keamanan informasi organisasi.

Simpulan

Kegiatan ini menunjukkan bahwa permasalahan utama dalam keamanan informasi pada perusahaan konsultan TI terletak pada faktor *brainware*, khususnya rendahnya kesadaran dan pemahaman karyawan terhadap risiko keamanan seperti phishing, pengelolaan perangkat yang tidak aman, serta penggunaan sistem yang belum optimal. Kesalahan yang dilakukan, baik secara sengaja maupun tidak sengaja, berpotensi menyebabkan kebocoran data dan mengancam keberlangsungan organisasi. Melalui intervensi berupa penyusunan kebijakan keamanan (IT *Security Policy* dan SOP), pelatihan *security awareness*, serta penerapan kontrol keamanan teknis, terjadi peningkatan pemahaman dan kepatuhan karyawan terhadap praktik keamanan informasi. Berdasarkan indikator hasil, kegiatan ini menunjukkan adanya peningkatan *awareness* sebesar ±30% serta mulai diterapkannya praktik keamanan dasar, seperti penggunaan autentikasi ganda dan prosedur *backup data*. Dengan demikian, pendekatan yang mengintegrasikan aspek kebijakan, edukasi, dan teknologi terbukti efektif dalam meningkatkan keamanan informasi organisasi. Upaya ini perlu dilakukan secara berkelanjutan untuk memastikan adaptasi terhadap perkembangan ancaman siber yang semakin kompleks serta untuk memperkuat budaya keamanan informasi dalam organisasi. Kegiatan pengabdian ini memberikan kontribusi nyata dalam meningkatkan kesiapan mitra dalam menghadapi ancaman keamanan informasi.

Daftar Pustaka

Aditya, A. R. M., Putri, A. W. O. K., Musthofa, D. L., & Widodo, P. (2022). Serangan Hacking Tools sebagai Ancaman Siber dalam Sistem Pertahanan Negara (Studi Kasus: Predator). *Global Political Studies Journal*, *6*(1), 35–46. doi: 10.34010/gpsjournal.v6i1.6698

Afifi, M. A. M. (2020). Assessing Information Security Vulnerabilities and Threats to Implementing Security Mechanism and Security Policy Audit. *Journal of Computer Science*, *16*(3), 321–329. doi: 10.3844/JCSSP.2020.321.329

Anggraini, N. S., Kuntadi, C., & Pramukty, R. (2023). Pengaruh Teknologi Informasi, Pengendalian Internal dan Kompetensi Pengguna Terhadap Kualitas Sistem Informasi Akuntansi. *Manajemen Kreatif Jurnal (MAKREJU)*, *1*(3), 28–39. doi: 10.55606/makreju.v1i3.1599

Assen, M. F. van. (2021). Training, employee involvement and continuous improvement–the moderating effect of a common improvement method. *Production Planning and Control*, *32*(2), 132–144. doi: 10.1080/09537287.2020.1716405

Assyakurrohim, D., Ikhram, D., Sirodj, R. A., & Afgani, M. W. (2010). Metode Studi Kasus dalam Penelitian. *Jurnal Pendidikan Sains Dan Komputer*, *3*(1), 1–9. doi: 10.47709/jpsk.v3i01.1951

Baloyi, G. T. (2020). Toxicity of leadership and its impact on employees: Exploring the dynamics of leadership in an academic setting. *HTS Teologiese Studies / Theological Studies*, *76*(2), 1–8. doi: 10.4102/hts.v76i2.5949

Bratha, W. G. E. (2022). Literature Review Komponen Sistem Informasi Manajemen: Software, Database Dan Brainware. In Jurnal Ekonomi Manajemen Sistem Informasi (Vol. 3, Issue 3, pp. 344–360). doi: 10.31933/jemsi.v3i3.824

Hapsari, R. D., & Pambayun, K. G. (2023). Ancaman Cybercrimedi Indonesia: Sebuah Tinjauan Pustaka Sistematis. *Jurnal Konstituen*, *5*(1), 1–17. doi: 10.33701/jk.v5i1.3208

Lee, F. S., Andry, J. F., Christianto, K., Honni, H., & Clara, M. (2023). Audit of Attendance Information System At Motorcycle Factory Using Cobit 5. *Jurnal Teknoinfo*, *17*(1), 148–155. doi: 10.33365/jti.v17i1.2316

Lee, F. S., Aprilia, K., Dinata, D. F., Fernando, W., & Andry, J. F. (2024). Aplikasi Pengelolaan Stok Bahan Baku dengan Metode Waterfall Pada Pabrik Plastik. *Jurnal Teknologi Dan Sistem Informasi Bisnis*, *6*(2), 258–265. doi: 10.47233/jteksis.v6i2.1273

Lee, F. S., & Isputrawan, M. F. (2022). Peningkatan Kualitas Layanan Warga Kelurahan Duri Kepa dengan Aplikasi LINGKOE. *Jurnal Informatika*, *9*(1), 61–70. doi: 10.31294/inf.v9i1.11538

Lee, F. S., Vera, D., Pranata, M., Stevanus, S., & Karepowan, N. (2020). Analisis Aplikasi Klinikedika Berbasis Risiko dengan ITIL pada Domain Service Design. *JBASE - Journal of Business and Audit Information Systems*, *3*(2), 9–20. doi: 10.30813/jbase.v3i2.2267

Mee, R. W. M., Pek, L. S., Von, W. Y., Ghani, K. A., Shahdan, T. S. T., Ismail, M. R., & Rao, Y. S. (2021). A conceptual model of analogue gamification to enhance learners' motivation and attitude. *International Journal of Language Education*, *5*(2), 40–50. doi: 10.26858/ijole.v5i2.18229

Nord, J. H., Koohang, A., Floyd, K., & Paliszkiewicz, J. (2012). Issues in Information Systems. *Issues in Information Systems*, *13*(2), 112–122. doi: 10.48009/3_iis_2020_217-226

Nugroho, J. A., Hartono, D. J., Koesdinar, D. A., Sekartani, B. P., Panjaitan, C. P., & Paramarta, V. (2023). Pengaruh Hardware, Software dan Brainware Terhadap Ketepatan Waktu (Timeliness) dalam Penyajian Informasi yang Relevan di Sistem Informasi Manajemen Rumah Sakit. *COMSERVA : Jurnal Penelitian Dan Pengabdian Masyarakat*, *3*(08), 3013–3020. doi: 10.59141/comserva.v3i08.1076

Nurdin, N., & Pettalongi, S. S. (2022). Menggunakan Paradigma Studi Kasus Kualitatif Interpretatif Online dan Offline Untuk Memahami Efektivitas Penerapan E-Procurement. *Coopetition : Jurnal Ilmiah Manajemen*, *13*(2), 155–168. doi: 10.32670/coopetition.v13i2.1518

Selvam, V. S. D. (2020). Human Error in IT Security. *Arxiv*. Retrieved from http://arxiv.org/abs/2005.04163

Sockin, J., Sojourner, A., & Starr, E. P. (2022). Non-Disclosure Agreements and Externalities from Silence. *Academy of Management Proceedings*, *2022*(1–85). doi: 10.5465/ambpp.2022.15402abstract

Sudarsono, B. G., Cornelius, W., Lesmana, K., Samuel, S., Natanael, J., & Andry, J. F. (2023). IT Policy di Perusahaan Pelayaran. *JBASE - Journal of Business and Audit Information Systems*, *6*(2), 26–33. doi: 10.30813/jbase.v6i2.4672

Widhagdha, M. F., & Ediyono, S. (2022). Case Study Approach in Community Empowerment Research in Indonesia. *Indonesian Journal of Social Responsibility Review (IJSRR)*, *1*(1), 71–76. doi: 10.55381/ijsrr.v1i1.19

Widodo, D. S., & Yandi, A. (2022). Model Kinerja Karyawan: Kompetensi, Kompensasi dan Motivasi, (Literature Review MSDM). *Jurnal Ilmu Multidisplin*, *1*(1), 1–14. doi: 10.38035/jim.v1i1.1