# ANALISIS KEAMANAN SISTEM MANAJEMEN INFORMASI RUMAH SAKIT UMUM DAERAH NABIRE

**Youce Albertus Wilar[1*], Kristia Yuliawan[2], Akhmad Amiruddin Natsir[3]**

[1-2]STMIK PESAT NABIRE
[3]L2DIKTI 14 Papua

Email Koresponden: Youcewilar2712@gmail.com

Disubmit: 28 Juli 2023 Diterima: 24 September 2023 Diterbitkan: 01 Oktober 2023
Doi: https://doi.org/10.33024/mahesa.v3i10.11246

## *ABSTRACT*

*In today's digital era, Nabire Regional General Hospital (RSUD) and other health institutions face increasingly complex information security challenges. Information management system security is a crucial issue to maintain the confidentiality, integrity, and availability of patient health data. The purpose of this study was to analyze the security of the information management system at RSUD Nabire. This study uses a qualitative research method that involves analyzing the security of the information management system at RSUD Nabire. The data in this study were collected through interviews with relevant parties at Nabire Regional General Hospital, direct observation of the system, and analysis of documents and policies related to information security. Interviews were used to obtain information from parties experienced in hospital information management systems. The data that has been collected is then analyzed thematically. The results showed that the security of the Nabire Hospital information management system was measured by three dimensions which showed that employee knowledge in managing information management system security understood the rules and guidelines governing the use of information systems. While in the attitude dimension, employees have a high awareness of the importance of maintaining information security. Then the behavior dimension has a high awareness of the importance of maintaining information security and acting proactively to protect hospital data and information systems.*

***Keywords**: Security, System, Management, Information*

## ABSTRAK

Pada era digital saat ini, Rumah Sakit Umum Daerah (RSUD) Nabire dan institusi kesehatan lainnya menghadapi tantangan keamanan informasi yang semakin kompleks. Keamanan sistem manajemen informasi menjadi isu krusial untuk menjaga kerahasiaan, integritas, dan ketersediaan data kesehatan pasien. Tujuan dari penelitian ini adalah untuk menganalisis keamanan sistem manajemen informasi di RSUD Nabire. Penelitian ini menggunakan metode penelitian kualitatif yang melibatkan analisis keamanan sistem manajemen informasi RSUD Nabire. Data pada penelitian ini dikumpulkan melalui wawancara dengan pihak terkait di Rumah Sakit Umum Daerah Nabire, observasi langsung terhadap sistem, serta analisis dokumen dan kebijakan terkait keamanan informasi. Wawancara digunakan untuk mendapatkan informasi dari pihak yang

berpengalaman dalam sistem manajemen informasi rumah sakit. Data yang telah terkumpul kemudian dianalisis secara tematik. Hasil peneltian menunjukan bahwa keamanan sistem manajemen informasi RSUD Nabire diukur dengan tiga dimensi yang menunjukan bahwa pengetahuan karyawan dalam mengelola keamanan sistem manajemen informasi memahami aturan dan pedoman yang mengatur penggunaan sistem informasi. Sedangkan pada dimensi sikap, karyawan memiliki kesadaran yang tinggi terhadap pentingnya menjaga keamanan informasi. Kemudian dimensi perilaku memiliki kesadaran yang tinggi akan pentingnya menjaga keamanan informasi dan bertindak secara proaktif untuk melindungi data dan sistem informasi rumah sakit.

**Kata Kunci:** Keamanan, Sistem, Manajemen, Informasi

## PENDAHULUAN

Di era informasi ini, rumah sakit dituntut untuk meningkatkan kinerja dan daya saing sebagai badan usaha tanpa mengurangi misi sosialnya. Upaya untuk mencapai hal tersebut, rumah sakit perlu merumuskan kebijakan strategis yang melibatkan internal organisasi, manajemen, dan sumber daya manusia. Mereka juga harus memiliki kemampuan dalam pengambilan keputusan yang cepat dan tepat guna meningkatkan kualitas pelayanan kesehatan kepada masyarakat secara responsif, inovatif, efektif, efisien, dan menguntungkan bagi pemilik modal (Handiwidjojo, 2015).

Sistem Informasi Manajemen Rumah Sakit (SIMRS) adalah suatu sistem komputer yang mengintegrasikan seluruh proses bisnis dalam layanan kesehatan, termasuk koordinasi, pelaporan, dan administrasi, dengan tujuan untuk mendapatkan informasi secara cepat, tepat, dan akurat. Saat ini, SIMRS berbasis komputer menjadi sarana pendukung yang sangat penting, bahkan mutlak, dalam pengelolaan operasional rumah sakit (Rusman & Suwardoyo, 2022).

Keamanan sistem manajemen informasi menjadi isu krusial untuk menjaga kerahasiaan, integritas, dan ketersediaan data kesehatan pasien. Keamanan Sistem Informasi sangat penting untuk melindungi aset informasi yang berharga. Perusahaan harus memperhatikan keamanan aset informasinya, karena kebocoran informasi atau kegagalan dalam sistem dapat menyebabkan kerugian finansial dan menurunkan produktivitas perusahaan (Whitman & Mattord, 2012). Upaya untuk mengukur keamanan sistem informasi, terdapat tiga komponen yang dibagi menjadi tiga dimensi, yaitu pengetahuan (knowledge), sikap (attitude), dan perilaku (behaviour). Dimensi-dimensi ini digunakan untuk mengembangkan pemahaman tentang pengetahuan individu, sikap mereka, dan perilaku mereka terkait dengan keamanan sistem informasi (Kruger & Kerney, 2006).

Rumah Sakit Umum Daerah (RSUD) Nabire adalah rumah sakit umum daerah milik Pemerintah dan merupakan salah satu rumah sakit tipe C yang terletak di wilayah Kabupaten Nabire, Papua. Rumah sakit ini memberikan pelayanan di bidang kesehatan yang didukung oleh layanan dokter spesialis serta ditunjang dengan fasilitas medis lainnya. Selain itu, RSUD Nabire juga sebagai rumah sakit rujukan dari faskes tingkat 1, seperti puskesmas atau klinik. RSUD ini memiliki SIMRS dalam pengelolaanya, namun belum

pernah dilakukan analisa mengenai keamanan SIMRnya.

Pada penelitian terdahulu yang diakukan oleh (Alghifary et all, 2023) analisis keamanan sistem informasi manajemen rumah sakit dilakukan dengan framework COBIT di RSUD Palembang BARI. Penelitian lain juga dilakukan oleh (Windriya, 2013) yang melakukan analaisis keamanan sistem informasi manajemen pada rumah sakit umum daerah berdasarkan ISO 27002. Kebaharuan penelitian ini adalah dari objek penelitiannya itu sendiri yakni RSUD Nabire berdasarkan dimensi pengetahuan (knowledge), sikap (attitude), dan perilaku (behaviour). Tujuan dari penelitian ini adalah untuk menganalisis keamanan sistem manajemen informasi di Rumah Sakit Umum Daerah Nabire.

## TINJAUAN PUSTAKA

### Definisi

Sistem Informasi Rumah Sakit (SIRS) adalah suatu aktifitas terstruktur yang berkaitan dengan proses pengumpulan data, pengelolaan, analisis, penyajia dan pengambilan keputusan oleh rumah sakit (Rusman, 2022); (Suryantoko, 2020). Lebih lengkapnya sistem informasi rumah sakit (SIRS) adalah suatu tatanan yang berurusan dengan pengumpulan data, pengelolaan data, penyajian informasi, analisis dan penyimpulan informasi serta penyampaian informasi yang dibutuhkan untuk kegiatan rumah sakit (Harsono, 2015). Sedangkan sistem informasi manajemen rumah sakit (SIMRS) adalah sebuah sistem informasi yang dirancang untuk membantu kinerja manajemen rumah sakit dan perencanaan program kesehatan yang dilakukan dari mulai pengumpulan data hingga penyajian data yang mudah untuk dipahami semua departemen yang terlibat (Setyawan, 2016).

Berdasarkan dari kedua pengertian tersebut maka dapat dijelaskan perbedaan SIRS dan SIMRS, dimana keduanya dilihat dari penerapan proses bisnis yang lebih luas. Sistem Informasi Rumah Sakit (SIRS) dikaitkan dengan bidang yang lebih luas yang berhubungan dengan pemanfaatan teknologi sistem informasi untuk berbagai proses kebutuhan rumah sakit, sedangkan sistem informasi manajemen rumah sakit (SIMRS) diterapkan pada objek bisnis yang lebih spesifik dari itu, dengan tujuan mencapai target implementasi.

### Fungsi dan Manfaat Sistem Informasi Manajemen Rumah Sakit (SIMRS)

Walaupun hanya sebagai media dan alat bantu dalam melaksanakan berbagai aktivitas manajemen Rumah sakit, sistem informasi rumah sakit (SIRS) juga mampu menjadi bidang divisi baru yang tidak bisa lepas dari keberadaan rumah sakit itu sendiri. Berikut ini merupakan fungsi dan manfaat sistem informasi rumah sakit baik untuk kelangsungan manajemen maupun masyarakat luas yang berinteraksi langsung (Fitri, 2023).

Menjamin efisiensi penggunaan sumber daya oleh rumah sakit dengan menyediakan berbagai platform elektronik sehingga dapat menggantikan media analog pada sistem sebelumnya. Contoh paling banyak dari implementasi proses bisnis ini adalah peralihan penggunaan media kertas menjadi sekumpulan file terenkripsi yang lebih efisien, aman dan tidak banyak memakan tempat. Selain itu penggunaan sistem informasi manajemen rumah sakit (SIMRS) juga berpotensi menekan jumlah sumber daya manusia (SDM) karena sebagian besar pekerjaan sudah dapat

ditangani oleh sistem yang dikembangkan.

Menjamin keamanan dan kerahasiaan data tanpa menghilangkan manfaat kemudahan aksesibilitas. Dengan menggunakan sistem yang baik, data dan informasi rumah sakit dapat dikemas secara ringkas, aman, mudah dibagikan dan mudah diakses oleh pihak yang berwenang. Ini mungkin merupakan fungsi yang cukup sulit dikembangkan karena selain informasi harus tetap bersifat rahasia namun juga harus tetap dapat dibagikan secara mudah kepada pihak-pihak yang berkepentingan.

Meningkatkan akurasi dan mengurangi resiko kesalahan pencatatan data pasien. Melalui sistem yang baik maka dibutuhkan validasi pencatatan berlapis-lapis untuk memperoleh hasil informasi yang akurat. Sistem informasi manajemen rumah sakit (SIMRS) dirancang untuk mengurangi resiko terjadinya kesalahan yang biasa dilakukan oleh petugas (user) tanpa menghilangkan kecepatan pencatatan itu sendiri.

Sebagai alat yang memberikan informasi dan rekomendasi dalam pengendalian biaya operasional. Sebuah sistem rumah sakit yang baik, memberikan kemajuan dalam hal mitigasi anggaran yang merepresentasikan kesehatan finansial rumah sakit (Amelia, 2021). Dengan adanya sistem informasi rumah sakit maka proses pengendalian anggaran dan biaya akan berlangsung dengan mudah dan mendapatkan rekomendasi yang tepat untuk memutuskan alokasi dana yang tepat sasaran.

Membantu pihak manajemen rumah sakit dalam melakukan analisa dan pengambilan keputusan. Dengan memanfaatkan algoritma komputer, sistem perhitungan analisa baik dalam hal pelayanan, SDM ataupun kesehatan finansial rumah sakit itu sendiri. Hal ini sangat bermanfaat bagi manajemen untuk memutuskan strategi pengelolaan perusahaan yang tepat.

Memberikan kemudahan bagi masyarakat, lembaga dan instansi pemerintah dalam memperoleh informasi realtime mengenai rumah sakit yang bersangkutan. Dengan adanya sistem informasi ini mempermudah pihak lain dalam konsumsi data dan informasi yang selayaknya dipublikasikan.

## METODE PENELITIAN

Penelitian ini menggunakan metode penelitian kualitatif yang melibatkan analisis keamanan sistem manajemen informasi Rumah Sakit Umum Daerah Nabire. Menurut (Sugiyono, 2018) metode penelitian kualitatif adalah metode penelitian yang berlandaskan pada filsafat yang digunakan untuk meneliti pada kondisi ilmiah (eksperimen) dimana peneliti sebagai instrumen, teknik pengumpulan data dan di analisis yang bersifat kualitatif lebih menekan pada makna. Data pada penelitian ini dikumpulkan melalui wawancara dengan pihak terkait di Rumah Sakit Umum Daerah Nabire, observasi langsung terhadap sistem, serta analisis dokumen dan kebijakan terkait keamanan informasi. Wawancara digunakan untuk mendapatkan informasi dari pihak yang berpengalaman dalam sistem manajemen informasi rumah sakit. Data yang telah terkumpul kemudian dianalisis secara tematik.

## PEMBAHASAN

Sistem Informasi dalam layanan kesehatan dapat memberikan banyak manfaat yang potensial seperti meningkatkan kualitas pelayanan, mengurangi kesalahan medis, meningkatkan

pemantauan ketersediaan fasilitas, dan meningkatkan aksesibilitas informasi. Namun, penting untuk diwaspadai bahwa ada ancaman yang dapat mengganggu keamanan Sistem Informasi (Siagian, 2017). Potensi ancaman terhadap sistem manajemen informasi Rumah Sakit Umum Daerah Nabire meliputi:

1. Serangan Siber
   Rumah sakit dapat menjadi target serangan siber oleh pihak yang tidak bertanggung jawab seperti peretas atau hacker. Serangan ini dapat berupa serangan malware, ransomware, serangan DDoS (Distributed Denial of Service), atau serangan lainnya yang bertujuan untuk mengganggu, merusak, atau mencuri data sensitif.
2. Kebocoran Data
   Ancaman kebocoran data dapat terjadi baik akibat serangan siber maupun karena kelalaian atau kesalahan manusia (Putra & Masnun, 2022). Data medis dan informasi pribadi pasien yang tersimpan dalam sistem manajemen informasi rumah sakit dapat menjadi target pencurian atau disalahgunakan oleh pihak yang tidak berwenang.
3. Akses Tidak Sah
   Ancaman ini melibatkan pihak yang mencoba mendapatkan akses ilegal ke sistem manajemen informasi rumah sakit dengan tujuan mengambil, mengubah, atau merusak data (Hidayat, 2020). Hal ini bisa terjadi jika sistem tidak memiliki mekanisme keamanan yang memadai atau jika terdapat celah keamanan yang dieksploitasi.
4. Kecelakaan atau Bencana Alam
   Ancaman ini berkaitan dengan kejadian tak terduga seperti kebakaran, banjir, atau bencana alam lainnya yang dapat merusak infrastruktur dan perangkat yang digunakan dalam sistem manajemen informasi rumah sakit. Hal ini dapat menyebabkan kehilangan data dan gangguan pada operasional rumah sakit (Hidayat, 2020).

Penentuan kontrol keamanan setelah identifikasi ancaman, evaluasi kerentanan merupakan langkah penting dalam menjaga keamanan sistem informasi dan data di RSUD Nabire. Beberapa langkah yang dapat dilakukan dalam penentuan kontrol keamanan adalah sebagai berikut:

1. Kebijakan Keamanan
   Penetapan kebijakan keamanan yang jelas dan komprehensif untuk RSUD Nabire. Kebijakan ini mencakup aspek-aspek seperti kebijakan akses pengguna, kebijakan penggunaan kata sandi, kebijakan privasi dan perlindungan data, serta kebijakan terkait keamanan fisik. Kebijakan ini harus dipahami dan diikuti oleh seluruh personel RSUD.
2. Penggunaan Perangkat Lunak Keamanan
   Penggunaan perangkat lunak keamanan yang tepat untuk melindungi sistem informasi dan data di RSUD. Ini termasuk penggunaan firewall, sistem deteksi intrusi, antivirus, enkripsi data, dan alat pengamanan lainnya. Perangkat lunak keamanan harus diperbarui secara teratur untuk mengatasi ancaman keamanan terbaru (Alghifary, 2023).
3. Pengawasan dan Pemantauan
   Tindakan pengawasan dan pemantauan secara berkala terhadap aktivitas pengguna dan sistem informasi di RSUD. Ini dapat dilakukan dengan menggunakan alat pemantauan jaringan dan log aktivitas sistem. Pengawasan ini membantu mendeteksi aktivitas

mencurigakan atau tidak sah serta memungkinkan respons cepat terhadap ancaman keamanan.

4. Pelatihan Keamanan
   Pelatihan keamanan kepada seluruh personel RSUD untuk meningkatkan kesadaran akan praktik keamanan yang baik. Pelatihan ini mencakup penggunaan kata sandi yang kuat, keamanan email, pengenalan phishing, serta tindakan pencegahan lainnya. Dengan meningkatkan pemahaman tentang keamanan, personel RSUD akan dapat mengidentifikasi dan menghindari ancaman keamanan potensial.
5. Manajemen Akses Pengguna
   Penerapan sistem manajemen akses pengguna yang baik untuk mengontrol akses ke sistem informasi dan data di RSUD. Ini termasuk memberikan hak akses yang tepat berdasarkan peran dan tanggung jawab, serta melaksanakan kebijakan pembatasan akses jika diperlukan.

Kemudian, setelah langkah kontrol keamanan perlu adanya evaluasi terhadap kerentanan sistem. Evaluasi kerentanan sistem manajemen informasi Rumah Sakit Umum Daerah Nabire dilakukan untuk mengetahui sejauh mana kerentanan tersebut dapat dimanfaatkan oleh pihak yang tidak berwenang. Evaluasi ini melibatkan penilaian terhadap kelemahan keamanan yang ada dalam infrastruktur teknologi informasi, kebijakan keamanan, dan proses operasional rumah sakit. Beberapa langkah yang dapat dilakukan dalam evaluasi kerentanan adalah analisis Kerentanan Infrastruktur TI yang melibatkan penilaian terhadap sistem jaringan, server, perangkat lunak, dan perangkat keras yang digunakan dalam sistem manajemen informasi rumah sakit. Pada analisis ini, dilakukan identifikasi kerentanan yang mungkin ada, seperti kelemahan konfigurasi, penggunaan versi perangkat lunak yang rentan, atau kekurangan keamanan pada firewall atau sistem deteksi intrusi.

Pengetahuan karyawan Rumah Sakit Umum Daerah Nabire dalam mengelola keamanan sistem manajemen informasi mencakup pemahaman tentang kebijakan keamanan yang telah ditetapkan oleh rumah sakit. Mereka memahami aturan dan pedoman yang mengatur penggunaan sistem informasi, termasuk penggunaan kata sandi, akses terbatas, dan tindakan keamanan lainnya. Karyawan memiliki pengetahuan tentang kebijakan yang mengatur penggunaan sistem informasi rumah sakit, seperti kebijakan tentang penggunaan perangkat lunak, penggunaan jaringan, dan kebijakan terkait privasi dan kerahasiaan data. Dengan pemahaman ini, karyawan dapat mengikuti prosedur yang ditetapkan dan memastikan bahwa mereka mematuhi kebijakan keamanan yang telah ditetapkan oleh rumah sakit. Mereka memahami pentingnya menjaga kerahasiaan data pasien dan informasi sensitif lainnya, serta melaksanakan langkah-langkah keamanan yang diperlukan untuk melindungi sistem informasi dari ancaman yang mungkin timbul. Selain itu, karyawan juga memahami pentingnya penggunaan kata sandi yang kuat dan mengikuti praktik keamanan yang direkomendasikan, seperti mengganti kata sandi secara teratur, tidak membagikan kata sandi dengan orang lain, dan menjaga kerahasiaan kata sandi. Mereka memahami bahwa akses ke sistem informasi harus dibatasi hanya kepada mereka yang berwenang, dan pemantauan

terhadap aktivitas sistem dilakukan untuk mendeteksi potensi ancaman keamanan.

Sikap (Attitude) karyawan Rumah Sakit Umum Daerah Nabire dalam mengelola keamanan sistem manajemen informasi adalah sikap yang proaktif dan memiliki kesadaran yang tinggi terhadap pentingnya menjaga keamanan informasi. Mereka menyadari bahwa kerahasiaan data pasien dan informasi sensitif lainnya merupakan tanggung jawab mereka sebagai tenaga medis dan administratif di rumah sakit. Karyawan memiliki sikap yang disiplin terhadap kebijakan keamanan yang telah ditetapkan.

Mereka memahami bahwa kebijakan keamanan ada untuk melindungi data dan informasi penting dari akses yang tidak sah atau penyalahgunaan (Winarti, 2015). Karyawan berkomitmen untuk mematuhi aturan dan pedoman keamanan yang ditetapkan oleh rumah sakit dan bertindak dengan itikad baik untuk menjaga kerahasiaan dan integritas sistem informasi. Contoh sikap proaktif adalah ketika karyawan secara aktif melaporkan potensi celah keamanan yang mereka temukan kepada pihak yang berwenang, seperti menginformasikan jika terdapat kerentanan dalam sistem atau jika mereka mendeteksi aktivitas mencurigakan. Mereka juga dapat memberikan saran atau rekomendasi untuk meningkatkan keamanan sistem informasi di rumah sakit.

Sikap disiplin terlihat dalam tindakan karyawan untuk selalu menjaga kerahasiaan kata sandi pribadi mereka dan tidak membocorkannya kepada pihak lain. Mereka mengikuti prosedur yang telah ditetapkan, seperti mengganti kata sandi secara berkala dan tidak menggunakan kata sandi yang mudah ditebak. Selain itu, karyawan juga mematuhi kebijakan akses terbatas, hanya mengakses informasi yang relevan dengan tugas dan tanggung jawab mereka. Dengan sikap proaktif dan disiplin ini, karyawan Rumah Sakit Umum Daerah Nabire menjunjung tinggi kepentingan keamanan informasi dan berperan aktif dalam menjaga kerahasiaan dan integritas sistem manajemen informasi rumah sakit.

Perilaku (Behavior) karyawan Rumah Sakit Umum Daerah Nabire dalam mengelola keamanan sistem manajemen informasi adalah implementasi tindakan keamanan dalam aktivitas sehari-hari mereka. Mereka memiliki kesadaran yang tinggi akan pentingnya menjaga keamanan informasi dan bertindak secara proaktif untuk melindungi data dan sistem informasi rumah sakit. Berikut adalah beberapa contoh perilaku yang diimplementasikan oleh karyawan:

1. Penggunaan kata sandi yang kuat

   Karyawan menggunakan kata sandi yang kompleks dan unik untuk mengakses sistem informasi. Karyawan tidak menggunakan kata sandi yang mudah ditebak dan secara rutin mengubah kata sandi mereka untuk menjaga keamanan.
2. Penguncian perangkat saat tidak digunakan

   Karyawan menyadari pentingnya mengunci perangkat mereka, seperti komputer atau ponsel, saat tidak digunakan, hal ini mencegah akses tidak sah ke informasi yang sensitif jika perangkat tersebut jatuh ke tangan yang salah.
3. Melaporkan insiden keamanan

   Karyawan memiliki keberanian untuk melaporkan insiden keamanan yang mereka temui kepada pihak yang berwenang, hal ini memungkinkan tindakan perbaikan yang cepat diambil

untuk mencegah kerugian lebih lanjut.

Penting untuk menjaga keamanan sistem manajemen informasi rumah sakit dengan menerapkan langkah-langkah perlindungan yang tepat. Beberapa langkah yang dapat dilakukan antara lain enkripsi data dengan menggunakan teknik enkripsi untuk melindungi data sensitif agar tidak dapat diakses oleh pihak yang tidak berwenang. Pembaruan Perangkat Lunak dengan rutin melakukan pembaruan perangkat lunak dan sistem operasi untuk mengatasi kerentanan keamanan yang baru teridentifikasi. Penggunaan Kata Sandi yang Kuat dengan menerapkan kebijakan penggunaan kata sandi yang kuat dan kompleks, serta mengganti kata sandi secara berkala. Akses terbatas dengan memberikan akses terbatas hanya kepada personel yang membutuhkan informasi tersebut, dengan menggunakan sistem otentikasi dan otorisasi yang tepat. Pemantauan sistem dengan melakukan pemantauan secara aktif terhadap sistem informasi untuk mendeteksi aktivitas mencurigakan atau serangan yang mungkin terjadi. Pelatihan keamanan dengan melakukan pelatihan keamanan kepada staf rumah sakit untuk meningkatkan kesadaran tentang praktik keamanan yang baik dan tindakan pencegahan terhadap serangan siber. Implementasi langkah-langkah perlindungan tersebut, rumah sakit dapat menjaga keamanan sistem manajemen informasinya, melindungi data sensitif pasien, dan mencegah kebocoran informasi yang dapat merugikan rumah sakit dan pasien.

**KESIMPULAN**

Pengetahuan karyawan dalam mengelola keamanan sistem manajemen informasi meliputi pemahaman aturan dan pedoman yang mengatur penggunaan sistem informasi. Mereka memahami kebijakan dan prosedur yang telah ditetapkan oleh rumah sakit terkait penggunaan sistem informasi, termasuk aturan terkait penggunaan kata sandi, akses terbatas, kebijakan penggunaan perangkat lunak, dan prosedur keamanan lainnya. Mereka memahami pentingnya menjaga kerahasiaan dan integritas data serta menghindari praktik-praktik yang dapat membahayakan keamanan informasi. Pada dimensi sikap, karyawan memiliki kesadaran yang tinggi terhadap pentingnya menjaga keamanan informasi. Mereka menyadari bahwa kerahasiaan dan integritas data merupakan aspek kritis dalam menjaga keberlangsungan dan reputasi rumah sakit. Mereka menganggap keamanan informasi sebagai tanggung jawab bersama dan memiliki komitmen untuk melaksanakan tindakan keamanan yang sesuai dengan kebijakan yang telah ditetapkan. Kemudian, pada dimensi perilaku, karyawan menunjukkan kesadaran yang tinggi akan pentingnya menjaga keamanan informasi dan bertindak secara proaktif untuk melindungi data dan sistem informasi rumah sakit. Mereka melaksanakan tindakan keamanan yang diperlukan dalam aktivitas sehari-hari mereka, seperti menggunakan kata sandi yang kuat, mengunci perangkat saat tidak digunakan, menggunakan koneksi internet yang aman, dan berhati-hati dalam berbagi informasi. Mereka juga memiliki kesadaran untuk melaporkan insiden keamanan yang terjadi agar dapat segera ditindaklanjuti dan diatasi.

**DAFTAR PUSTAKA**


Adair, J. (2008). Kepemimpinan Yang Memotivasi. Gramedia Pustaka Utama.

Algiffary, A., Herdiansyah, M. I., & Kunang, Y. N. (2023). Audit Keamanan Sistem Informasi Manajemen Rumah Sakit Dengan Framework Cobit 2019 Pada Rsud Palembang Bari. Journal Of Applied Computer Science And Technology, 4(1), 19-26.

Amelia, A. R., Skm, M. K., Rusydi, A. R., & Skm, M. K. (2021). Sistem Informasi Kesehatan (Kajian Covid-19 Melalui Sistem Informasi Kesehatan). Deepublish.

Fitri, E. S. (2023). Evaluasi Kematangan Teknologi Informasi Pada Domain Service Operation Menggunakan Framework Information Technology Infrastructure Library (Studi Kasus Rumah Sakit Umum Tipe C Di Kota Malang) (Doctoral Dissertation, Universitas Islam Negeri Maulana Malik Ibrahim).

Handiwidjojo, W. (2015). Sistem Informasi Manajemen Rumah Sakit. Jurnal Eksplorasi Karya Sistem Informasi Dan Sains, 2(2).

Handiwidjojo, W. (2015). Sistem Informasi Manajemen Rumah Sakit. Jurnal Eksplorasi Karya Sistem Informasi Dan Sains, 2(2).

Hidayat, F. (2020). Konsep Dasar Sistem Informasi Kesehatan. Deepublish.

Hidayat, F. (2020). Konsep Dasar Sistem Informasi Kesehatan. Deepublish.

Kruger, H.A., Kearney W., D. (2006). A Prototype For Assessing Information Security Awareness. Computer & Security Volume 25 : 289-29.

Nussy, M. D. (2023). Analisis Pengelolaan Risiko Teknologi Informasi Pt. Krakatau Daya Listrik Cilegon Dengan Menggunakan Framework Iso 31000: 2018 (Doctoral Dissertation).

Putra, C. A., & Masnun, M. A. (2022). Analisis Pertanggungjawaban Rumah Sakit Terkait Potensi Kebocoran Data Rekam Medis Elektronik Akibat Cyber Crime. Novum: Jurnal Hukum, 9(2), 191-200.

Putri, S. I., St, S., Akbar, P. S., & St, S. (2019). Sistem Informasi Kesehatan. Uwais Inspirasi Indonesia.

Rusman, A. D. P., & Suwardoyo, U. (2022). Penerapan Sistem Informasi Berbasis It Pengolahan Data Rekam Medis Untuk Peningkatan Pelayanan Di Rumah Sakit. Penerbit Nem.

Setyawan, D. (2016). Analisis Implementasi Pemanfaatan Sistem Informasi Manajemen Rumah Sakit (Simrs) Pada Rsud Kardinah Tegal. Ijcit (Indonesian Journal On Computer And Information Technology), 1(2).

Siagian, S. (2017). Analisis Ancaman Keamanan Pada Sistem Informasi Manajemen Di Rumah Sakit Rimbo Medica Jambi 2015. Scientia Journal, 4(4).

Sujudi, A. (2011). Menjadi Seniman Organisasi: Seni Mengelola "Healthcare Industry. Pt. Rayyana Komunikasindo.

Suryantoko, S., Agnes, A., & Faisol, A. (2020). Penerapan Sistem Informasi Manajemen Rumah Sakit Guna Meningkatkan Mutu Pelayanan Di Rumkital Marinir Cilandak. Jurnal Manajemen Dan Administrasi Rumah Sakit

Indonesia (Marsi), 4(2), 155-165.

Whitman, M. E., & Mattord, H. J. (2012). Threats To Information Security Revisited. Journal Of Information System Security, 8(1).

Winarti, I. (2015). Pengaruh Kompetensi Auditor Internal Terhadap Keamanan Informasi (Survey Pada Perusahaan Bumn Industri Strategis Kota Bandung) (Doctoral Dissertation, Universitas Widyatama).

Windriya, D. R. (2013). Ta: Audit Keamanan Sistem Informasi Pada Instalasi Sistem Informasi Manajemen Rsud Bangil Berdasarkan Iso 27002 (Doctoral Dissertation, Stikom Surabaya).

Yaumi, M. (2016). Pendidikan Karakter: Landasan, Pilar & Implementasi. Prenada Media.