Jurnal Ilmiah Sistem Informasi dan Ilmu Komputer
Volume 5, Nomor 2, Juli 2025
p-ISSN: 2827-8135; e-ISSN: 2827-7953, Hal. 225-234
DOI: https://doi.org/10.55606/juisik.v5i2.1231
Available Online at: https://journal.sinov.id/index.php/juisik

Evaluasi Implementasi Keamanan Informasi pada Sistem Perpustakaan SMKN 1 Banyumas

Akbar Andhika Putra[1*], Sigit Setiyoko[2], Sabdo Bagus Andriyanto[3], Azmi Imtiyaz[4], Dwi Krisbiantoro[5]

[1-5]Universitas Amikom Purwokerto, Indonesia
Email: *dhikarizzz233@gmail.com[1], sigitsetiyoko9@gmail.com[2], sabdobagus35@gmail.com[3], azmiimtiyaz001@gmail.com[4], dwikris@amikompurwokerto.ac.id[5]

Alamat: Jl. Letjend Pol. Soemarto No.127, Watumas, Purwanegara, Kec. Purwokerto Utara, Kabupaten Banyumas, Jawa Tengah 53127
Korespondensi penulis: dhikarizzz233@gmail.com

Abstract. *The rapid adoption of digital technologies in educational environments has increased the need for secure information systems, particularly in school libraries. This study aims to evaluate the implementation of information security and data privacy within the library system at SMKN 1 Banyumas. A qualitative approach was used, involving direct observations, semi-structured interviews, and document analysis. The findings reveal that although role-based access control and manual data backups are in place, the system still operates over unencrypted HTTP, lacks two-factor authentication, and has no firewall or intrusion detection system. Furthermore, staff members have not received formal cybersecurity training. The study concludes with recommendations for implementing HTTPS, enhancing user authentication mechanisms, deploying network protection tools, and improving staff cybersecurity awareness. These measures are crucial for improving the security posture of educational digital services.*

Keywords: *school IT infrastructure, data security, cyber literacy, risk management, library information systems*

Abstrak. Adopsi teknologi digital yang pesat di lingkungan pendidikan telah meningkatkan kebutuhan akan sistem informasi yang aman, terutama pada layanan perpustakaan sekolah. Penelitian ini bertujuan mengevaluasi implementasi keamanan informasi dan perlindungan data dalam sistem perpustakaan di SMKN 1 Banyumas. Pendekatan kualitatif digunakan melalui observasi langsung, wawancara semi-terstruktur, dan analisis dokumentasi. Hasil menunjukkan bahwa sistem telah menerapkan kontrol akses berbasis peran dan pencadangan data manual, tetapi masih menggunakan protokol HTTP tanpa enkripsi, belum mendukung autentikasi dua faktor, serta belum memiliki firewall dan sistem deteksi intrusi. Selain itu, staf belum mendapatkan pelatihan keamanan siber secara formal. Penelitian ini merekomendasikan penerapan HTTPS, penguatan autentikasi pengguna, penerapan perlindungan jaringan, serta peningkatan literasi keamanan bagi staf perpustakaan. Langkah-langkah tersebut penting untuk meningkatkan keamanan layanan digital di institusi pendidikan.

Kata kunci: infrastruktur TI sekolah, keamanan data, literasi siber, manajemen risiko, sistem informasi perpustakaan

1. LATAR BELAKANG

Kemajuan teknologi informasi dalam lima tahun terakhir telah mengubah cara institusi pendidikan mengelola layanan, termasuk perpustakaan. Transformasi dari sistem manual menuju sistem digital memungkinkan pengelolaan koleksi, transaksi peminjaman, dan data pengguna dilakukan secara lebih cepat, efisien, dan terpusat. Digitalisasi perpustakaan juga mendukung transparansi layanan dan memberikan kemudahan akses informasi kepada siswa

Received: Mei 17, 2025; Revised: Mei 31, 2025; Accepted: Juni 09, 2025; Online Available: Juni 23, 2025

maupun tenaga pendidik. Namun, peningkatan ketergantungan pada sistem digital juga menimbulkan risiko baru, khususnya terkait ancaman terhadap keamanan informasi dan privasi data pengguna.

Dalam konteks perpustakaan sekolah, data yang dikelola mencakup identitas pengguna, rekam jejak peminjaman, hingga kredensial sistem yang sangat rentan apabila tidak dilindungi dengan baik. Ancaman seperti peretasan, penyadapan jaringan, maupun penyalahgunaan akun internal dapat terjadi ketika sistem informasi tidak dilengkapi dengan mekanisme pengamanan teknis seperti enkripsi, autentikasi ganda, firewall, serta sistem deteksi intrusi (IDS). Beberapa studi terkini, seperti yang dilakukan oleh Rahayu dan Nugroho (2023) serta Nursalam dan Wibowo (2021), mengungkap bahwa mayoritas sistem informasi perpustakaan di sekolah-sekolah Indonesia belum dilengkapi dengan komponen keamanan esensial. Hal ini diperparah oleh minimnya pelatihan keamanan digital bagi staf, serta rendahnya penerapan kebijakan manajemen risiko keamanan informasi.

Kondisi serupa ditemukan di SMKN 1 Banyumas. Sistem informasi perpustakaan di sekolah ini telah menerapkan kontrol akses berbasis peran (RBAC) dan melakukan pencadangan data secara manual, namun masih menggunakan protokol komunikasi HTTP tanpa enkripsi. Selain itu, belum diterapkan autentikasi dua faktor, dan belum tersedia firewall atau sistem IDS yang dapat mendeteksi ancaman secara real-time. Kelemahan lain yang mencolok adalah tidak tersedianya pelatihan keamanan siber untuk pustakawan maupun operator sistem, yang menjadikan potensi kesalahan manusia (human error) sebagai faktor risiko tambahan.

Melihat kondisi tersebut, penelitian ini menjadi relevan dan mendesak untuk dilakukan. Fokus dari studi ini adalah mengevaluasi sejauh mana sistem keamanan informasi diterapkan dalam lingkungan perpustakaan sekolah menengah kejuruan, dengan mengambil studi kasus di SMKN 1 Banyumas. Aspek kebaruan (novelty) dari penelitian ini terletak pada konteks kajiannya, yaitu sistem informasi perpustakaan sekolah vokasi yang masih jarang dieksplorasi dalam literatur keamanan informasi di Indonesia. Penelitian ini juga mengedepankan pendekatan kualitatif berbasis observasi langsung, wawancara semi-terstruktur, dan dokumentasi, guna menghasilkan pemetaan kondisi aktual yang mendalam. Tujuan utama dari penelitian ini adalah untuk menilai sejauh mana kebijakan dan teknologi keamanan informasi telah diterapkan, serta memberikan rekomendasi teknis dan kebijakan untuk meningkatkan keamanan sistem informasi di lingkungan pendidikan menengah.

2. KAJIAN TEORITIS

Keamanan informasi merupakan pendekatan strategis yang bertujuan untuk melindungi sistem dan data dari berbagai potensi ancaman yang dapat membahayakan aspek kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability) informasi. Dalam sistem perpustakaan digital, khususnya di lingkungan pendidikan, keamanan informasi menjadi pilar utama untuk menjamin bahwa layanan yang diberikan berjalan dengan aman dan dapat dipercaya oleh pengguna. Gangguan terhadap sistem tidak hanya berdampak pada operasional teknis, tetapi juga bisa menyebabkan pelanggaran privasi dan kerugian reputasi institusi.

ISO/IEC 27001:2013 merupakan standar internasional yang memberikan kerangka kerja dalam penerapan Sistem Manajemen Keamanan Informasi (SMKI). Standar ini mencakup komponen-komponen penting seperti kebijakan organisasi, identifikasi risiko, penilaian kerentanan, pengendalian teknis dan administratif, serta perbaikan berkelanjutan terhadap sistem yang ada. Penerapan standar ini memberikan acuan dalam menjaga keamanan informasi secara sistematis dan terukur di berbagai sektor, termasuk institusi pendidikan.

Salah satu prinsip utama yang banyak diterapkan dalam sistem informasi adalah Role-Based Access Control (RBAC), yaitu model pengelolaan akses berdasarkan peran pengguna. RBAC memungkinkan pengelolaan hak akses yang terstruktur dan mencegah akses tidak sah dari pihak-pihak yang tidak memiliki wewenang. Ahmad dan Purwanto (2022) menekankan bahwa penerapan RBAC dalam sistem informasi sekolah memberikan peningkatan signifikan terhadap pengendalian akses pengguna.

Selanjutnya, autentikasi dua faktor (2FA) juga menjadi mekanisme penting dalam menjamin identitas pengguna sistem. Sistem ini menggabungkan dua jenis validasi, biasanya berupa sesuatu yang diketahui pengguna (seperti sandi) dan sesuatu yang dimiliki (seperti kode OTP). Dalam praktiknya, banyak institusi pendidikan belum menerapkan 2FA secara menyeluruh. Penelitian oleh Sari dan Putra (2022) mengungkap bahwa ketidakhadiran mekanisme 2FA pada sistem perpustakaan sekolah menjadikan sistem lebih rentan terhadap peretasan akun dan serangan berbasis rekayasa sosial.

Selain autentikasi, keamanan transmisi data juga krusial. Penggunaan protokol HTTPS dengan dukungan enkripsi data menjadi praktik standar dalam pengamanan informasi yang ditransmisikan melalui jaringan. Rahayu dan Nugroho (2023) menunjukkan bahwa sebagian besar sistem berbasis web di sekolah belum menggunakan HTTPS secara konsisten, yang meningkatkan risiko penyadapan data oleh pihak ketiga. Untuk mendukung perlindungan

sistem secara menyeluruh, teknologi seperti firewall dan Intrusion Detection System (IDS) diperlukan untuk mengawasi lalu lintas jaringan dan mendeteksi potensi ancaman secara dini.

Namun, keberhasilan implementasi teknologi keamanan juga sangat bergantung pada kesiapan sumber daya manusia. Rendahnya literasi keamanan digital dan minimnya pelatihan siber di lingkungan sekolah membuat sistem informasi menjadi rawan terhadap human error. Nursalam dan Wibowo (2021) menekankan bahwa pelanggaran keamanan sering kali berasal dari kelalaian pengguna, seperti penggunaan sandi yang lemah, kurangnya kesadaran terhadap phishing, atau kebiasaan berbagi akun.

Berdasarkan uraian di atas, dapat disimpulkan bahwa landasan teori keamanan informasi dalam penelitian ini mencakup kombinasi antara kerangka kerja teknis (seperti ISO/IEC 27001, RBAC, 2FA, HTTPS, firewall, IDS) dan faktor manusia sebagai elemen kunci dalam penguatan sistem. Seluruh konsep ini menjadi fondasi dalam menganalisis tingkat kesiapan dan penerapan keamanan informasi pada sistem perpustakaan digital SMKN 1 Banyumas, serta menjadi rujukan dalam menyusun rekomendasi pengembangan sistem yang lebih aman dan adaptif terhadap tantangan digital.

3. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan rancangan studi kasus, yang bertujuan untuk mengkaji secara mendalam implementasi keamanan informasi dalam sistem perpustakaan digital di SMKN 1 Banyumas. Pendekatan ini dipilih untuk menggali fenomena secara kontekstual dan holistik, dengan melibatkan proses observasi langsung dan interaksi dengan subjek serta lingkungan tempat sistem informasi digunakan.

Populasi dalam penelitian ini mencakup seluruh pihak yang terlibat dalam pengelolaan dan penggunaan sistem informasi perpustakaan sekolah, seperti pustakawan, operator sistem, serta pengguna aktif lainnya. Teknik pemilihan informan dilakukan secara purposive sampling, yaitu berdasarkan kriteria keterlibatan langsung dalam proses operasional sistem. Dalam hal ini, tiga informan kunci diwawancarai, terdiri atas satu pustakawan, satu staf operator sistem, dan satu tenaga pendidik pengguna aktif layanan perpustakaan digital.

Data dikumpulkan melalui tiga teknik utama: observasi partisipatif, wawancara semi-terstruktur, dan studi dokumentasi. Observasi dilakukan untuk melihat langsung bagaimana sistem perpustakaan diakses dan dikelola, serta mengidentifikasi komponen-komponen keamanan yang diterapkan. Wawancara digunakan untuk menggali pandangan, pengalaman,

serta kendala yang dihadapi informan terkait praktik keamanan informasi. Sedangkan dokumentasi dilakukan terhadap kebijakan internal sekolah, konfigurasi teknis sistem, dan catatan log sistem jika tersedia.

Seluruh data dianalisis menggunakan model interaktif dari Miles dan Huberman yang terdiri dari tiga tahap utama: reduksi data, penyajian data, dan penarikan kesimpulan. Analisis dilakukan secara iteratif dan berkesinambungan selama proses pengumpulan data berlangsung. Validitas hasil diperkuat melalui triangulasi sumber, yaitu membandingkan temuan dari observasi, wawancara, dan dokumen sebagai upaya memastikan konsistensi dan akurasi data.

Model penelitian ini bersifat eksploratif dan tidak melibatkan pengujian statistik seperti uji-F atau uji-t, karena tujuan utama adalah memperoleh pemahaman mendalam terhadap kondisi aktual sistem keamanan informasi. Simbol atau terminologi seperti RBAC (Role-Based Access Control), 2FA (Two-Factor Authentication), HTTPS, firewall, dan IDS digunakan dalam analisis untuk mewakili fitur teknis yang menjadi objek evaluasi dalam konteks studi ini.

4. HASIL DAN PEMBAHASAN

1. Proses Pengumpulan Data dan Lokasi Penelitian

Penelitian ini dilaksanakan di lingkungan Perpustakaan SMKN 1 Banyumas selama periode April hingga Mei 2025. Pengumpulan data dilakukan dengan pendekatan triangulasi, yaitu melalui observasi langsung terhadap alur kerja sistem informasi perpustakaan, wawancara semi-terstruktur dengan tiga informan utama (pustakawan, operator sistem, dan guru pengguna aktif), serta pengumpulan dokumentasi terkait kebijakan, konfigurasi sistem, dan struktur organisasi. Tujuan dari pendekatan ini adalah untuk memperoleh gambaran menyeluruh dari sisi teknis, manajerial, dan kesiapan sumber daya manusia dalam pengelolaan keamanan informasi perpustakaan digital.

2. Evaluasi Penerapan Fitur Keamanan Informasi

Berdasarkan hasil observasi dan wawancara, diketahui bahwa sebagian fitur dasar keamanan informasi telah diterapkan, namun masih banyak kekurangan dari segi teknis lanjutan dan kebijakan kelembagaan. Rangkuman hasil evaluasi terhadap fitur keamanan yang diterapkan dalam sistem dapat dilihat pada tabel berikut:

Tabel 1. Evaluasi Fitur Keamanan Sistem Informasi Perpustakaan SMKN 1 Banyumas

No	Fitur Keamanan	Status Implementasi	Keterangan
1	Role-Based Access Control (RBAC)	Sudah diterapkan	Hak akses dibedakan antara petugas dan pengguna biasa
2	Logging Aktivitas Pengguna	Sudah diterapkan	Pencatatan aktivitas dasar login dan akses pengguna
3	Pencadangan Data	Manual (mingguan)	Pencadangan dilakukan manual oleh operator
4	Protokol HTTPS	Belum diterapkan	Masih menggunakan HTTP yang tidak mendukung enkripsi
5	Autentikasi Dua Faktor (2FA)	Belum diterapkan	Hanya menggunakan kombinasi username dan password
6	Firewall	Belum tersedia	Tidak ada proteksi terhadap akses jaringan luar
7	Intrusion Detection System (IDS)	Belum tersedia	Belum ada sistem untuk mendeteksi aktivitas mencurigakan
8	Pelatihan Keamanan Siber	Belum tersedia	Belum pernah diadakan pelatihan formal bagi staf perpustakaan

Sumber: (Data Primer, 2025)

3. Keterkaitan Temuan dengan Teori dan Studi Sebelumnya

Hasil evaluasi menunjukkan adanya ketidaksesuaian antara praktik keamanan yang diterapkan dengan standar internasional ISO/IEC 27001:2013. Sistem masih minim dalam hal penerapan kontrol teknis tingkat lanjut, seperti autentikasi multi-faktor, proteksi jaringan, serta

enkripsi komunikasi. Hal ini memperbesar potensi risiko seperti kebocoran data, penyusupan jaringan, dan pencurian akun.

Temuan ini sejalan dengan penelitian Sari dan Putra (2022), yang menyebutkan bahwa sebagian besar perpustakaan sekolah di Indonesia masih berada pada tahap dasar dalam pengelolaan keamanan informasi. Selain itu, hasil ini juga menguatkan studi Nursalam dan Wibowo (2021), yang menekankan bahwa rendahnya literasi digital dan ketiadaan pelatihan keamanan menjadi akar dari banyak kelemahan sistem yang berbasis teknologi di sekolah.

4. Implikasi Teoritis dan Praktis

Secara teoritis, penelitian ini memperkuat pentingnya pendekatan multidimensi dalam pengelolaan keamanan informasi, yang tidak hanya menekankan pada teknologi, tetapi juga pada regulasi internal dan kesiapan pengguna. Sistem informasi perpustakaan yang aman memerlukan sinergi antara kebijakan kelembagaan, penguatan teknis, serta pelatihan SDM.

Secara praktis, hasil penelitian memberikan dasar bagi pengambilan kebijakan penguatan keamanan informasi di lingkungan sekolah. Beberapa langkah strategis yang direkomendasikan meliputi:

- Implementasi protokol HTTPS untuk mengamankan pertukaran data antar pengguna dan server.
- Penambahan autentikasi dua faktor guna mencegah pembobolan akun berbasis sandi lemah.
- Pengadaan perangkat lunak firewall dan IDS untuk memantau dan mengendalikan lalu lintas jaringan.
- Pelatihan literasi keamanan informasi bagi seluruh staf dan operator sistem secara berkala.

Dengan langkah-langkah tersebut, diharapkan sistem informasi perpustakaan di SMKN 1 Banyumas dapat meningkatkan ketahanannya terhadap ancaman digital dan menjadi model pengelolaan keamanan informasi yang adaptif dan berkelanjutan.

5. KESIMPULAN DAN SARAN

Berdasarkan hasil analisis dan temuan penelitian, dapat disimpulkan bahwa sistem informasi perpustakaan di SMKN 1 Banyumas telah menunjukkan upaya awal dalam penerapan keamanan informasi, khususnya melalui implementasi kontrol akses berbasis peran (RBAC) dan pencadangan data secara rutin. Meskipun demikian, sistem ini masih menghadapi sejumlah kelemahan yang signifikan, terutama pada aspek teknis. Beberapa fitur penting seperti protokol komunikasi terenkripsi (HTTPS), autentikasi dua faktor (2FA), firewall, dan sistem deteksi intrusi (IDS) belum diterapkan. Selain itu, belum tersedianya pelatihan keamanan siber bagi staf perpustakaan menunjukkan perlunya penguatan literasi keamanan informasi di lingkungan sekolah.

Oleh karena itu, diperlukan upaya perbaikan yang mencakup peningkatan infrastruktur keamanan digital, penerapan kebijakan keamanan informasi berbasis standar, serta pelatihan berkala bagi seluruh pengguna dan pengelola sistem. Langkah-langkah ini penting untuk meningkatkan ketahanan sistem terhadap ancaman digital, sekaligus menjamin perlindungan data pengguna perpustakaan secara menyeluruh.

Penelitian ini memiliki keterbatasan pada ruang lingkup yang hanya mencakup satu institusi dan menggunakan pendekatan kualitatif. Oleh sebab itu, penelitian lanjutan disarankan untuk melibatkan lebih banyak objek kajian di berbagai sekolah dan mengombinasikan pendekatan kuantitatif guna memperluas validitas dan generalisasi temuan terhadap sistem keamanan informasi di institusi pendidikan.

UCAPAN TERIMA KASIH

Penulis mengucapkan apresiasi kepada SMKN 1 Banyumas atas kesempatan dan dukungan yang diberikan selama proses penelitian berlangsung, khususnya dalam pelaksanaan observasi dan pengumpulan data di lingkungan perpustakaan sekolah. Terima kasih juga disampaikan kepada para staf perpustakaan dan pengelola sistem informasi yang telah bersedia menjadi responden serta memberikan informasi yang relevan dan mendalam. Artikel ini disusun sebagai bagian dari kegiatan penelitian lapangan yang bertujuan untuk mengkaji aspek keamanan informasi di institusi pendidikan menengah. Penulis juga menyampaikan penghargaan kepada semua pihak yang telah berkontribusi, baik melalui bimbingan, koreksi, maupun saran dalam proses penyusunan dan penyempurnaan naskah ini.

DAFTAR REFERENSI

Ahmad, I., & Purwanto, R. (2022). Evaluasi keamanan informasi pada aplikasi sekolah digital. *Jurnal Ilmiah Informatika, 8*(3), 98–104.

Aripradono, S., Hidayat, R., & Cahyono, D. (2024). Firewall dan sistem otentikasi ganda untuk sekolah digital: Studi kasus SMK. *Jurnal Keamanan Siber Indonesia, 5*(1), 33–40.

Cahyaningrum, M. (2022). Meningkatkan keamanan sistem informasi sekolah melalui autentikasi berlapis. *Jurnal Teknologi Informasi Pendidikan, 9*(2), 58–66.

Cahyanto, B., Nurhidayati, L., & Wulandari, D. (2025). Efektivitas multi-factor authentication dalam sistem informasi pendidikan. *Jurnal Sistem Informasi dan Teknologi, 11*(2), 71–79.

Fitria, S. L., & Aziz, M. R. (2025). Tantangan digitalisasi perpustakaan sekolah di daerah terpencil. *Jurnal Informasi Pendidikan Digital, 4*(1), 25–33.

Gunawan, A., & Iskandar, A. (2022). Model evaluasi keamanan sistem informasi berbasis risiko pada lembaga pendidikan. *Jurnal Teknologi dan Manajemen Informasi, 10*(1), 55–63.

International Organization for Standardization. (2013). *ISO/IEC 27001:2013 - Information security management systems – Requirements*.

Laudon, K. C., & Laudon, J. P. (2020). *Management information systems: Managing the digital firm* (16th ed.). Pearson.

Nafisah, I. (2022). Peran literasi digital dalam penguatan sistem perpustakaan sekolah. *Jurnal Teknologi Pendidikan Digital, 6*(1), 41–49.

Nursalam, A., & Wibowo, F. (2021). Manajemen risiko keamanan data sekolah. *Jurnal Manajemen Sistem Informasi, 9*(4), 200–210.

Prasetyo, D. (2023). Pengaruh autentikasi multi-faktor terhadap keamanan sistem akademik. *Jurnal Teknologi Digital, 5*(2), 111–118.

Rahayu, E., & Nugroho, A. (2023). Evaluasi HTTPS pada layanan berbasis web sekolah. *Jurnal Keamanan Jaringan, 3*(1), 45–52.

Rahmat, A., & Suryawan, I. (2022). Kebijakan keamanan informasi di Sekolah Menengah Kejuruan. *Jurnal Kebijakan Pendidikan dan Teknologi, 8*(2), 123–132.

Republik Indonesia. (2018). *Pedoman perlindungan data pribadi*.

Santoso, B., & Mukhlis, A. (2024). Analisis kerentanan sistem informasi perpustakaan sekolah. *Jurnal Sistem Informasi Pendidikan, 10*(1), 11–20.

Sari, R. P., & Putra, A. A. (2022). Analisis risiko keamanan sistem informasi perpustakaan sekolah. *Jurnal Sistem Informasi dan Keamanan Siber, 7*(1), 22–30.

Setiawan, D. (2021). *Keamanan informasi: Konsep dan implementasi dalam organisasi*. Andi Offset.

Stallings, W. (2018). *Cryptography and network security: Principles and practice* (7th ed.). Pearson Education.

Wulandari, D., & Prabowo, R. (2021). Literasi digital dan kesadaran keamanan informasi di lingkungan sekolah. *Jurnal Komunikasi Digital dan Edukasi, 3*(1), 61–68.

Yusuf, H., & Karim, A. (2020). Efektivitas implementasi otentikasi ganda dalam sistem akademik sekolah. *Jurnal Teknologi Informasi dan Keamanan*, *6*(2), 99–106.