MUDIR (Jurnal **MUDIR** (Jurnal Manajemen Pendidikan) P-ISSN : 2655-9331 E-ISSN : 2657-2230
Avalaible online at: **https://ejournal.unsuda.ac.id/index.php/mpi/index**
Volume 8, Nomor 1, Juli 2026 | DOI: https://doi.org/10.55352/mudir

EVALUASI KEAMANAN DAN MANAJEMEN DATA PADA SISTEM INFORMASI SEKOLAH DI ERA TRANSFORMASI DIGITAL

Siti Novi Coalliani[1], Arie Ekayudistira Kirana Tejawati[2], Syifa' Hanum Budiawati[3], Irmawati [4], Laili Komariyah[5], Yudo Dwiyono[6]
[1] *Universitas Mulawarman, Samarinda, Indonesia*
[2] *Universitas Mulawarman, Samarinda, Indonesia*
[3] *Universitas Mulawarman, Samarinda, Indonesia*
[4] *Universitas Mulawarman, Samarinda, Indonesia*
[5] *Universitas Mulawarman, Samarinda, Indonesia*
[6] *Universitas Mulawarman, Samarinda, Indonesia*

Email: sitinovi0511@gmail.com[1], ariekayudisthira@gmail.com[2], syifaummualif@gmail.com[3], irmawati231808@gmail.com[4], Laili.komariyah@fkip.unmul.ac.id[4], yudo.dwiyono@fkip.umnul.ac.id[5]

Abstrak: *Penelitian ini bertujuan untuk menganalisis penerapan keamanan dan manajemen data pada sistem informasi sekolah di era transformasi digital, dengan fokus pada upaya perlindungan data pendidikan serta efektivitas tata kelola digital. Metode yang digunakan adalah pendekatan kualitatif deskriptif berbasis data sekunder, yang bersumber dari laporan Badan Siber dan Sandi Negara (BSSN), publikasi Kementerian Pendidikan Dasar dan Menengah (Kemendikdasmen), serta publikasi ilmiah terkait kasus kebocoran data di sektor pendidikan Indonesia periode 2019–2023. Data dianalisis menggunakan kerangka kerja Confidentiality, Integrity, and Availability (CIA) Triad dan Data Governance Principle untuk menilai penerapan prinsip keamanan informasi dan tata kelola data di lingkungan sekolah. Hasil penelitian menunjukkan bahwa masih terdapat kelemahan signifikan dalam perlindungan data, terutama akibat kelalaian internal, kurangnya kebijakan keamanan yang komprehensif, serta lemahnya pengawasan terhadap sistem digital pendidikan. Dua aspek utama yang ditemukan berperan penting dalam memperkuat sistem keamanan informasi sekolah adalah kebijakan backup data yang berlapis dan terjadwal, serta manajemen akun pengguna berbasis role-based access control (RBAC). Penelitian ini berkontribusi dalam memperkaya literatur mengenai manajemen keamanan data pendidikan di Indonesia dan memberikan rekomendasi strategis bagi sekolah untuk membangun sistem informasi yang aman, akuntabel, dan berkelanjutan.*
Kata kunci: Keamanan Data; Manajemen Data; Sistem Informasi Sekolah; Tata Kelola Data; Transformasi Digital.

Abstract: This study aims to analyze the implementation of data security and management within school information systems in the era of digital transformation, focusing on the protection of educational data and the effectiveness of digital governance. The research employs a descriptive qualitative approach based on secondary data obtained from the National Cyber and Encryption Agency (BSSN), the Directorate General of Primary and Secondary Education (Kemendikdasmen), and scholarly publications related to data breach incidents in Indonesia's education sector between 2019 and 2023. Data were analyzed using the *Confidentiality, Integrity, and Availability (CIA) Triad* framework and the *Data Governance Principles* to assess the application of information security and data management standards in educational institutions. The findings reveal significant weaknesses in data protection, primarily due to internal negligence, the absence of comprehensive security policies, and inadequate oversight of digital education systems. Two critical components identified as essential for strengthening school

information security are multilayered and scheduled data backup policies, as well as user account management based on *role-based access control (RBAC)*. This study contributes to the growing body of literature on educational data security management in Indonesia and offers strategic recommendations for schools to develop information systems that are secure, accountable, and sustainable.
Keywords: Data Security; Data Management; School Information Systems; Data Governance; Digital Transformation.

Pendahuluan

Era transformasi digital telah membawa perubahan signifikan dalam dunia pendidikan, di mana teknologi informasi menjadi bagian integral dari sistem pengelolaan sekolah. Pemanfaatan teknologi digital mendorong efisiensi dalam administrasi, pembelajaran, serta komunikasi antara guru, siswa, dan orang tua. Sekolah-sekolah kini dituntut untuk beradaptasi dengan penggunaan sistem berbasis data dalam berbagai aspek manajemen pendidikan. Kondisi ini menunjukkan bahwa transformasi digital bukan sekadar tren, melainkan kebutuhan strategis untuk meningkatkan mutu layanan pendidikan di era modern (Ahyani & Dhuhani, 2024).

Perkembangan sistem informasi sekolah di Indonesia menunjukkan peningkatan yang pesat seiring dengan kebijakan digitalisasi pendidikan dari pemerintah. Berbagai aplikasi seperti Dapodik, e-rapor, dan platform manajemen akademik berbasis web telah diimplementasikan untuk mendukung pengelolaan data sekolah secara terintegrasi. Sistem ini berfungsi sebagai sarana utama dalam pengumpulan, penyimpanan, dan pelaporan data pendidikan di tingkat satuan pendidikan. Melalui penerapan sistem informasi tersebut, proses administrasi dan pengawasan pendidikan menjadi lebih efisien dan transparan (Ahyani & Dhuhani, 2024).

Ketergantungan sekolah terhadap data digital semakin meningkat seiring dengan perluasan penggunaan sistem informasi dalam kegiatan akademik dan administrasi. Data siswa, guru, kehadiran, nilai, serta informasi keuangan kini tersimpan dalam basis data digital yang menjadi aset penting bagi lembaga pendidikan. Pengelolaan data yang akurat dan aman sangat menentukan kelancaran proses pendidikan serta pengambilan keputusan di tingkat sekolah. Oleh karena itu, data digital tidak hanya berfungsi sebagai alat administratif, tetapi juga sebagai fondasi utama dalam mewujudkan tata kelola sekolah yang efektif dan modern (Mania et al., 2025).

Seiring meningkatnya penggunaan sistem digital di sekolah, muncul pula berbagai risiko dan ancaman terhadap keamanan data. Kasus kebocoran data, peretasan situs sekolah, serta penyalahgunaan informasi pribadi menjadi isu yang semakin sering terjadi di sektor pendidikan. Laporan Badan Siber dan Sandi Negara (BSSN) menunjukkan bahwa insiden keamanan siber di bidang pendidikan mengalami peningkatan dalam beberapa tahun terakhir. Kondisi ini menegaskan perlunya perhatian serius terhadap perlindungan data di lingkungan sekolah agar tidak menimbulkan kerugian bagi peserta didik maupun lembaga pendidikan (Mania et al., 2025).

Meskipun penggunaan sistem informasi sekolah terus berkembang, pengelolaan dan keamanan data di banyak sekolah masih tergolong lemah. Sebagian besar lembaga pendidikan belum memiliki kebijakan atau prosedur baku terkait pengelolaan data, seperti sistem backup, kontrol akses, dan enkripsi. Keterbatasan sumber daya manusia yang kompeten di bidang teknologi informasi juga menjadi kendala dalam menjaga keamanan data. Akibatnya, potensi terjadinya kebocoran, kehilangan, atau penyalahgunaan data semakin tinggi dan dapat mengganggu integritas sistem pendidikan secara keseluruhan (Shobri, 2024).

Penerapan regulasi perlindungan data pribadi di sektor pendidikan masih menghadapi berbagai tantangan. Meskipun pemerintah telah memberlakukan Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (PDP), banyak sekolah belum memiliki kapasitas dan pemahaman yang memadai untuk menyesuaikan diri dengan ketentuan tersebut. Keterbatasan infrastruktur teknologi, minimnya pelatihan bagi tenaga pendidik, serta rendahnya kesadaran akan pentingnya keamanan data menjadi hambatan utama. Akibatnya, implementasi regulasi belum berjalan optimal dan berpotensi menimbulkan celah dalam perlindungan data di lingkungan pendidikan (Mahameru et al., 2023).

Kesenjangan antara percepatan transformasi digital dan kesiapan keamanan data di sekolah menjadi persoalan yang semakin nyata. Sementara teknologi informasi terus berkembang pesat dan diterapkan secara luas, langkah-langkah perlindungan dan tata kelola datanya belum sepenuhnya mengikuti perkembangan tersebut. Banyak sekolah fokus pada efisiensi layanan digital tanpa memperhatikan aspek keamanan informasi yang memadai (Nugraha & Rochimat, 2025). Ketidakseimbangan ini dapat menimbulkan risiko tinggi terhadap kebocoran data serta menghambat terciptanya ekosistem pendidikan digital yang aman dan berkelanjutan.

Penelitian ini bertujuan untuk mengevaluasi tingkat keamanan dan manajemen data pada sistem informasi sekolah di Indonesia dalam konteks transformasi digital. Melalui analisis terhadap data historis dan kasus nyata

pelanggaran keamanan, penelitian ini berupaya mengidentifikasi faktor-faktor yang memengaruhi efektivitas perlindungan data di lingkungan pendidikan. Hasil evaluasi diharapkan dapat memberikan gambaran mengenai kesiapan sekolah dalam mengelola data secara aman dan sesuai dengan regulasi yang berlaku. Selain itu, penelitian ini juga bertujuan merumuskan rekomendasi strategis untuk memperkuat tata kelola dan keamanan data di sektor pendidikan.

Metode/Method (Huruf pertama kapital Book Antiqua 12pt)

Penelitian ini menggunakan pendekatan kualitatif deskriptif dengan memanfaatkan data sekunder historis yang relevan dengan keamanan dan manajemen data di sektor pendidikan. Pendekatan ini dipilih untuk memperoleh pemahaman mendalam terhadap fenomena keamanan data sekolah berdasarkan kasus nyata yang pernah terjadi di Indonesia. Penelitian difokuskan pada evaluasi kebijakan, praktik pengelolaan, serta kerentanan sistem informasi sekolah yang muncul selama proses transformasi digital. Dengan demikian, penelitian ini tidak hanya menjelaskan kondisi yang ada, tetapi juga memberikan interpretasi analitis terhadap efektivitas pengelolaan data di lingkungan pendidikan.

Variabel penelitian digunakan untuk memperjelas fokus kajian dan mempermudah proses analisis terhadap aspek yang diteliti. Dalam penelitian ini, variabel ditetapkan berdasarkan konsep utama yang berkaitan dengan sistem informasi sekolah di era transformasi digital. Dua variabel pokok yang dianalisis adalah keamanan data dan manajemen data, yang masing-masing memiliki definisi operasional dan indikator utama sebagai dasar pengukuran dan evaluasi.

Tabel 1
Ruang Lingkup Penelitian

Variabel	Definisi Operasional	Indikator / Aspek Utama
Keamanan Data	Upaya sekolah dalam melindungi data digital dari ancaman kebocoran, akses tidak sah, atau kehilangan informasi dengan menerapkan prinsip keamanan siber yang sesuai dengan pedoman BSSN dan regulasi nasional.	1. Kebijakan backup data dan pemulihan sistem (*disaster recovery plan*). 2. Pengamanan akses melalui otentikasi dan enkripsi data. 3. Penanganan insiden siber dan audit sistem berkala.
Manajemen Data	Proses pengelolaan data sekolah secara digital agar tersimpan, terorganisir, dan mudah diakses dengan aman oleh pihak yang berwenang.	1. Kebijakan backup data, manajemen akun pengguna, dan proteksi kata sandi. 2. Pemanfaatan platform digital Dapodik 3. Penerapan pedoman keamanan data dari Kemendikbudristek dan BSSN.

Data penelitian dikumpulkan melalui studi dokumentasi dan studi pustaka terhadap berbagai sumber tepercaya seperti laporan tahunan Badan Siber dan Sandi Negara (BSSN), Kementerian Komunikasi dan Informatika (Kominfo), peraturan perundangan seperti UU Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, serta publikasi ilmiah terkait keamanan sistem informasi sekolah. Objek penelitian mencakup sistem informasi sekolah di Indonesia pada jenjang dasar hingga menengah, dengan periode pengamatan antara tahun 2020-2024. Analisis data dilakukan dengan menggunakan kerangka kerja Confidentiality, Integrity, and Availability (CIA) Triad dan NIST Cybersecurity Framework untuk menilai sejauh mana prinsip-prinsip keamanan dan tata kelola data diterapkan di lingkungan sekolah.

Proses analisis dilakukan melalui tahapan reduksi data, pengelompokan tema, dan interpretasi hasil. Setiap data historis tentang insiden keamanan dievaluasi berdasarkan jenis ancaman, penyebab, dampak, serta langkah mitigasi yang dilakukan oleh lembaga terkait. Hasil analisis kemudian diinterpretasikan secara deskriptif untuk menggambarkan kesiapan sekolah dalam menghadapi tantangan keamanan data di era digital. Dari hasil tersebut, penelitian ini diharapkan mampu memberikan kontribusi praktis berupa rekomendasi strategis bagi pengambil kebijakan dan satuan pendidikan dalam memperkuat tata kelola serta perlindungan data sekolah di masa mendatang.

Temuan dan Diskusi

Kasus-Kasus Kebocoran Data di Sektor Pendidikan Indonesia

Dalam era transformasi digital, sektor pendidikan di Indonesia menghadapi tantangan besar dalam menjaga keamanan dan integritas data. Berbagai sistem informasi sekolah dan kampus kini terhubung secara daring untuk mendukung efisiensi administrasi dan proses belajar, namun hal ini juga membuka peluang terjadinya ancaman siber seperti kebocoran data, peretasan situs, hingga penyalahgunaan informasi pribadi. Insiden-insiden tersebut mencerminkan belum optimalnya penerapan manajemen keamanan data dan tata kelola digital di lingkungan pendidikan. Untuk memahami skala dan pola permasalahan tersebut, berikut disajikan Tabel 1 tentang Kasus-Kasus Pelanggaran Keamanan Data di Sektor Pendidikan Indonesia Tahun 2019–2023, yang menggambarkan berbagai bentuk insiden, dampak, dan sumber rujukan yang relevan.

Tabel 2

Kasus-Kasus Pelanggaran Keamanan Data di Sektor Pendidikan Indonesia Tahun 2019–2023

No.	Tahun	Institusi / Sektor	Jenis Insiden / Deskripsi Singkat
1	2020	Kemendikbud	Dugaan kebocoran 1,3 juta data pengguna (NIK, nama, alamat) yang beredar di forum daring. Kemendikbud menyatakan data tersebut tidak berasal dari sistem Dapodik/PD Dikti.
2	2020	Kemendikbud (Guru Honorer)	File berisi 175.000 data guru honorer penerima BSU tersebar secara publik; Kemendikbud melakukan investigasi.
3	2020	EduCSIRT Kemendikbud	Sepanjang 2020 terdapat 20 laporan insiden keamanan siber (6 closed, 14 solved), mencakup defacement, phishing, dan malware. Laporan disampaikan melalui educsirt@kemdikbud.go.id
8	2022–2023	BSSN	Ratusan dugaan kebocoran data sektor pendidikan ditemukan dalam laporan tahunan BSSN. Termasuk serangan malware dan defacement.
9	2019–2022	Situs kampus dan sekolah di berbagai daerah	Gelombang defacement dan peretasan situs kampus/sekolah yang dijadikan target untuk penyebaran malware atau spam.

Pada tahun 2020, dua insiden besar terjadi di lingkungan Kementerian Pendidikan dan Kebudayaan (Kemendikbud). Kasus pertama adalah dugaan kebocoran 1,3 juta data pengguna yang beredar di forum daring, mencakup NIK, nama, dan alamat, yang diduga bersumber dari sistem pendidikan daring. Jenis ancaman yang terjadi kemungkinan besar berasal dari kebocoran internal atau human error, karena tidak ditemukan indikasi serangan siber besar seperti malware. Kasus kedua melibatkan tersebarnya 175.000 data guru honorer penerima BSU (Bantuan Subsidi Upah) ke publik, yang juga menunjukkan adanya kelemahan dalam tata kelola data dan kontrol akses internal. Dampaknya meliputi kebocoran data pribadi yang sensitif, potensi penyalahgunaan identitas, serta penurunan reputasi kelembagaan Kemendikbud sebagai pengelola data pendidikan nasional. Sebagai respons, Kemendikbud melakukan investigasi internal dan memperkuat koordinasi dengan BSSN serta EduCSIRT untuk meningkatkan keamanan siber di sektor pendidikan.

Pada tahun 2020, tim EduCSIRT Kemendikbud menerima 20 laporan insiden keamanan siber yang meliputi defacement, phishing, dan serangan malware terhadap sistem pendidikan. Jenis ancaman utama berasal dari malware dan serangan eksternal, yang berpotensi menyebabkan gangguan layanan dan menurunkan kepercayaan publik terhadap keamanan sistem pendidikan digital. Sebagai respons, Kemendikbud menindaklanjuti laporan melalui kanal resmi seperti educsirt@kemdikbud.go.id serta memperkuat prosedur penanganan insiden. Selain itu, Badan Siber dan Sandi Negara (BSSN) turut menegaskan bahwa dalam laporan tahunannya terdapat ratusan insiden kebocoran di sektor pendidikan, meliputi serangan malware, defacement, dan phishing.

Rangkaian kasus kebocoran dan serangan siber di sektor pendidikan Indonesia dari tahun 2019 hingga 2023 menunjukkan bahwa keamanan data pendidikan masih menjadi tantangan serius dalam era transformasi digital. Berbagai insiden mulai dari kebocoran data siswa, defacement situs sekolah, hingga penyusupan konten ilegal di laman kampus memperlihatkan lemahnya kesadaran keamanan informasi dan pengelolaan infrastruktur digital. Sebagian besar kasus muncul akibat kombinasi antara human error, kelalaian dalam pemeliharaan sistem, dan kurangnya kebijakan keamanan yang komprehensif. Dampaknya bukan hanya pada hilangnya data pribadi, tetapi juga pada penurunan reputasi lembaga pendidikan yang seharusnya menjadi garda depan literasi digital dan pelindung data peserta didik.

Kondisi ini menegaskan pentingnya penerapan prinsip-prinsip tata kelola data (data governance) dan

keamanan siber (cybersecurity management) di lingkungan pendidikan. Institusi perlu beralih dari pendekatan reaktif menjadi pendekatan preventif dan adaptif, seperti melakukan security audit berkala, pembaruan sistem, enkripsi data, serta pelatihan keamanan digital bagi tenaga pendidik dan operator sekolah. Selain itu, kolaborasi antara pihak sekolah, Kementerian Pendidikan, dan lembaga seperti BSSN atau EduCSIRT sangat dibutuhkan untuk menciptakan sistem pertahanan digital yang lebih kuat dan terintegrasi. Dengan demikian, keamanan data di sektor pendidikan tidak hanya menjadi aspek teknis, tetapi juga bagian dari tanggung jawab etis dan kelembagaan dalam menjaga kepercayaan publik terhadap sistem informasi sekolah di Indonesia.

Manajemen Data Sekolah di Era Digital

Manajemen data di lingkungan sekolah memiliki peran yang sangat penting dalam mendukung efisiensi administrasi, transparansi informasi, serta pengambilan keputusan berbasis data. Dalam era digital, sekolah tidak lagi hanya mengandalkan dokumen fisik, tetapi telah beralih pada sistem informasi terintegrasi yang mencakup data pribadi siswa dan guru, nilai akademik, absensi, hingga laporan keuangan dan sarana prasarana. Setiap jenis data tersebut memiliki tingkat kerahasiaan dan sensitivitas yang berbeda, sehingga membutuhkan sistem pengelolaan yang aman dan terstruktur. Ketika data dikelola dengan baik, sekolah dapat meningkatkan kualitas layanan pendidikan, mempercepat proses administrasi, serta memperkuat akuntabilitas publik.

Namun, transformasi digital di sektor pendidikan juga membawa tantangan baru dalam hal keamanan dan keandalan sistem informasi. Banyak sekolah kini mengandalkan database terpusat, layanan cloud, serta platform pembelajaran daring untuk menyimpan dan mengakses data secara efisien. Meskipun sistem tersebut menawarkan kemudahan dalam pengelolaan dan kolaborasi, risiko kebocoran data dan akses tidak sah juga meningkat apabila tidak disertai kebijakan keamanan yang kuat. Oleh karena itu, sekolah perlu menerapkan standar manajemen data yang mencakup enkripsi, kontrol akses, serta sistem backup terjadwal, agar transformasi digital yang dijalankan tidak hanya efisien, tetapi juga aman dan berkelanjutan.

Manajemen data pada sistem informasi sekolah di era transformasi digital perlu dilaksanakan secara sistematis dan terintegrasi guna menjamin aspek keamanan, integritas, serta ketersediaan data pendidikan. Dalam konteks ini, satuan pendidikan tidak hanya berfungsi sebagai lembaga penyelenggara proses belajar mengajar, tetapi juga sebagai pengelola data strategis yang mencakup informasi pribadi peserta didik, pendidik, tenaga kependidikan, hingga dokumen administratif yang bersifat sensitif. Oleh karena itu, manajemen data menuntut adanya perencanaan, implementasi, dan pengawasan yang komprehensif terhadap proses penyimpanan, enkripsi, pengelolaan akses, serta pencadangan (backup) data. Berdasarkan hasil penelusuran dan telaah terhadap kebijakan pengelolaan data pendidikan, dapat diidentifikasi bahwa langkah-langkah yang perlu dilakukan oleh instansi pendidikan dalam menerapkan manajemen data pada sistem informasi sekolah di era transformasi digital dapat berfokus pada beberapa aspek utama, yaitu:

1. Kebijakan Backup Data

Kebijakan backup data pada sistem informasi kepegawaian sekolah merupakan aspek fundamental dalam menjaga keberlangsungan layanan digital pendidikan. Sistem ini umumnya menyimpan data penting seperti identitas guru dan tenaga kependidikan, riwayat jabatan, kehadiran, hingga dokumen kepegawaian. Berdasarkan Panduan Manajemen Risiko Keamanan Siber yang diterbitkan oleh BSSN, setiap lembaga pendidikan disarankan menerapkan kebijakan *redundancy* dan *disaster recovery plan* (DRP) sebagai bagian dari strategi mitigasi risiko kehilangan data. Backup yang terjadwal secara berkala—baik dalam bentuk *onsite* (lokal server sekolah) maupun *offsite* (penyimpanan awan atau cloud)—menjadi langkah preventif utama agar data kepegawaian tetap terlindungi dari ancaman seperti kegagalan perangkat keras, serangan ransomware, atau kesalahan manusia (*human error*).

Selain itu, Pedoman Tata Kelola Website BSSN memberikan acuan penting bagi sekolah yang menggunakan portal daring untuk layanan kepegawaian, seperti sistem presensi, pengajuan cuti, dan e-DUPAK (Daftar Usulan Penilaian Angka Kredit). Dokumen ini menekankan pentingnya sistem cadangan (backup server) dan pengamanan akses terhadap data personal pegawai melalui pengaturan otentikasi ganda serta enkripsi basis data. Dalam konteks ini, sekolah perlu memiliki SOP yang mengatur frekuensi backup, penyimpanan log aktivitas, serta mekanisme pemulihan sistem ketika terjadi serangan *defacement* atau *data breach*. Pendekatan ini sejalan dengan prinsip *confidentiality*, *integrity*, dan *availability* (CIA triad) yang menjadi pilar keamanan informasi di sektor publik.

Sementara itu, Kajian Ketahanan Siber: Manajemen Kerentanan BSSN menekankan pentingnya audit sistem secara berkala dan pemantauan terhadap kerentanan perangkat lunak yang digunakan dalam sistem kepegawaian sekolah. Audit tersebut meliputi evaluasi efektivitas kebijakan backup, keamanan akses, serta kesiapan sekolah dalam mengeksekusi *disaster recovery plan* apabila terjadi insiden. Dalam konteks tata kelola

pendidikan, kebijakan backup yang baik tidak hanya melindungi data administratif, tetapi juga membangun kepercayaan publik terhadap transparansi dan akuntabilitas pengelolaan kepegawaian digital. Dengan demikian, kombinasi kebijakan backup, sistem pemulihan bencana, serta penguatan ketahanan siber menjadi kerangka integral bagi sekolah untuk menjaga keberlanjutan sistem informasi di era transformasi digital.

Dengan demikian, sebagai acuan dalam menyusun kebijakan backup data pada sistem informasi kepegawaian sekolah, pedoman dari Badan Siber dan Sandi Negara (BSSN) memberikan kerangka kerja yang dapat diterapkan oleh satuan pendidikan untuk menjaga keamanan dan keberlanjutan data digital. Berdasarkan tiga dokumen utama yakni Pedoman Tata Kelola Website, Panduan Manajemen Risiko Keamanan Siber, dan Kajian Ketahanan Siber: Manajemen Kerentanan sekolah perlu membangun sistem pencadangan data yang terstruktur, berlapis, dan disertai dengan mekanisme pemulihan pasca insiden. Ringkasan langkah yang direkomendasikan dalam ketiga dokumen tersebut disajikan pada Tabel 3.

Tabel 3
Rekomendasi Kebijakan Backup Data Berdasarkan Pedoman Keamanan Siber BSSN untuk Sistem Informasi Kepegawaian Sekolah

Sumber : Dokumen BSSN	**Langkah yang Dilakukan Sekolah**
Pedoman Tata Kelola Keamanan Aplikasi Berbasis Web (2019)	1. Menyusun kebijakan backup data terjadwal untuk seluruh aplikasi berbasis web sekolah (seperti portal kepegawaian dan akademik). 2. Melakukan *hardening* server dan menerapkan pengendalian akses berbasis otorisasi pengguna. 3. Menyediakan mekanisme *incident response* terhadap insiden kehilangan atau modifikasi data.
Panduan Manajemen Risiko Keamanan Siber (2021)	1. Menetapkan prosedur *redundancy* dan *disaster recovery plan (DRP)* yang mencakup penyimpanan salinan data di lokasi berbeda (off-site/cloud). 2. Melakukan penilaian risiko rutin terhadap infrastruktur penyimpanan data sekolah. 3. Menyusun *business continuity plan (BCP)* yang memuat langkah pemulihan pasca serangan atau bencana.
Kajian Ketahanan Siber: Manajemen Kerentanan (2023)	1. Melakukan audit sistem secara berkala untuk mendeteksi kerentanan penyimpanan data kepegawaian. 2. Memperbarui sistem keamanan dan *patching* aplikasi. 3. Menjalankan proses *penetration testing* dan evaluasi efektivitas backup setelah setiap pembaruan sistem.

Kebijakan backup data pada sistem informasi kepegawaian sekolah harus dirancang secara komprehensif dengan mempertimbangkan aspek teknis, kelembagaan, dan keberlanjutan layanan digital. *Panduan Manajemen Risiko Keamanan Siber* menekankan pentingnya penerapan prinsip redundancy dan disaster recovery plan (DRP) untuk menjamin ketersediaan data meskipun terjadi gangguan sistem atau insiden siber. Sekolah diharapkan memiliki salinan data di lokasi yang berbeda (off-site backup) dan menyusun rencana kelangsungan layanan (business continuity plan) agar proses administrasi kepegawaian tetap berjalan tanpa kehilangan data penting. Sementara itu, Pedoman Tata Kelola Website mengarahkan agar setiap portal digital sekolah, termasuk sistem kepegawaian, menerapkan jadwal backup teratur, otorisasi pengguna yang ketat, dan mekanisme pelaporan insiden untuk memperkuat integritas sistem informasi.

Kajian Ketahanan Siber: Manajemen Kerentanan menyoroti pentingnya audit keamanan dan pemeliharaan sistem secara berkala untuk memastikan efektivitas kebijakan backup yang telah diterapkan. Melalui kegiatan seperti patching sistem, penetration testing, dan evaluasi efektivitas backup, sekolah dapat mendeteksi serta memperbaiki celah keamanan sebelum dimanfaatkan oleh pihak yang tidak berwenang. Pendekatan ini sejalan dengan prinsip *continuous improvement* dalam manajemen risiko siber, di mana keamanan data tidak bersifat statis tetapi harus diperbarui seiring perkembangan teknologi dan ancaman digital. Dengan demikian, kebijakan backup data tidak hanya berfungsi sebagai perlindungan teknis, tetapi juga menjadi bagian integral dari tata kelola keamanan informasi yang berkelanjutan di lingkungan pendidikan.

2. Manajemen Akun Pengguna

Manajemen akun pengguna pada sistem informasi sekolah merupakan aspek penting dalam menjaga keamanan, integritas, dan akuntabilitas data pendidikan. Dalam konteks sistem digital seperti, pengelolaan akun dilakukan dengan prinsip *role-based access control* (RBAC), yaitu pemberian hak akses sesuai dengan fungsi dan tanggung jawab masing-masing pengguna. Misalnya, admin atau operator sekolah memiliki akses penuh terhadap input dan pembaruan data, guru diberi hak untuk mengelola nilai dan absensi siswa, sementara siswa hanya dapat melihat hasil pembelajaran yang telah divalidasi. Struktur otorisasi ini dirancang untuk mencegah penyalahgunaan data, mengurangi risiko kesalahan input, serta memastikan setiap aktivitas digital dapat dilacak melalui sistem log pengguna. Adapun rincian kebijakan dan langkah yang perlu diterapkan sekolah dalam manajemen akun pengguna dapat dilihat pada tabel berikut.

Tabel 4
Manajemen Akun Pengguna pada Sistem Informasi Sekolah

Aspek	Pihak yang Terlibat	Langkah/Kebijakan yang Harus Dilakukan Sekolah	Informasi yang Dapat Disajikan
Kode Registrasi dan Akun Sekolah	Kepala Sekolah, Admin Dapodik, Petugas Pendataan	Sekolah wajib memiliki NPSN dan mengajukan permohonan kode registrasi ke Dinas Pendidikan; menyimpan kode registrasi secara rahasia dan tidak membagikannya ke pihak tidak berwenang.	Data sekolah terdaftar, NPSN, status validasi kode registrasi, riwayat perubahan akun.
Username dan Password	Petugas Pendataan, Dinas Pendidikan	Penetapan dan pergantian username serta password dilakukan melalui mekanisme resmi; wajib disertai SK penugasan. Password harus dienkripsi dan diperbarui secara berkala.	Data login pengguna, frekuensi perubahan password, log aktivitas pengguna.
Hak Akses Pengguna (Role Management)	Admin Sekolah, Guru, Operator Dapodik	Pembagian peran berdasarkan tanggung jawab: admin mengelola data utama, guru menginput nilai, TU mengelola data PTK dan sarpras; akses berbasis otorisasi.	Tabel hak akses tiap jabatan, jumlah pengguna aktif, jenis aktivitas yang dilakukan.
Keamanan Akses dan Validasi Data	Kepala Sekolah, Dinas Pendidikan	Setiap perubahan data diverifikasi oleh kepala sekolah; proses sinkronisasi hanya dilakukan setelah validasi internal dan penandatanganan SPTJM (Surat Pertanggungjawaban Mutlak).	Riwayat validasi data, jadwal sinkronisasi, dokumen SPTJM digital.
Pemulihan dan Pengelolaan Akun	Dinas Pendidikan, Operator Sekolah	Jika terjadi kehilangan akses atau kebocoran, sekolah harus segera melapor ke Dinas Pendidikan untuk reset akun; backup dilakukan sebelum sinkronisasi.	Data audit akses, laporan insiden keamanan akun, log pemulihan akun.

Manajemen akun pengguna dalam sistem informasi sekolah dirancang untuk menjamin keamanan serta integritas data pendidikan melalui pengaturan akses yang ketat dan terstruktur. Setiap pengguna sistem, mulai dari kepala sekolah hingga operator, diberikan hak akses yang berbeda sesuai dengan fungsi dan tanggung jawabnya. Mekanisme ini dikenal sebagai *role-based access control* (RBAC), yang bertujuan untuk meminimalkan risiko kesalahan input dan penyalahgunaan data (Wandri et al., 2025). Selain itu, setiap aktivitas pengguna terekam dalam log sistem sehingga memungkinkan proses audit dan penelusuran ketika terjadi perubahan atau anomali data. Kebijakan ini memperkuat transparansi tata kelola informasi di lingkungan sekolah sekaligus mendukung prinsip akuntabilitas digital yang ditekankan oleh Kemendikbudristek.

Sistem Dapodik juga menekankan pentingnya keamanan akses dan validasi data melalui verifikasi berlapis, termasuk kewajiban penggunaan kode registrasi resmi dan SPTJM (Surat Pertanggungjawaban Mutlak) sebelum sinkronisasi data ke server pusat. Langkah ini memastikan bahwa seluruh data yang dikirim merupakan hasil validasi internal dan memiliki legitimasi administratif. Di sisi lain, kebijakan pemulihan akun dan mekanisme pelaporan insiden ke Dinas Pendidikan menjadi bagian integral dari perlindungan data sekolah, khususnya untuk mencegah dan menanggulangi potensi kebocoran akun. Dengan demikian, manajemen akun pengguna dalam sistem Dapodik tidak hanya berfungsi sebagai sarana operasional, tetapi juga sebagai instrumen pengendalian

risiko dan penguatan keamanan siber di sektor pendidikan (Monia et al., 2025)

Diskusi

Penerapan teori keamanan data dalam konteks sistem informasi sekolah dapat dijelaskan melalui kerangka *Confidentiality, Integrity, and Availability (CIA) Triad*. Prinsip *confidentiality* menekankan pentingnya menjaga kerahasiaan data pribadi siswa, guru, dan staf agar tidak diakses oleh pihak yang tidak berwenang. Dalam praktiknya, banyak sekolah belum memiliki mekanisme enkripsi yang kuat atau kebijakan otentikasi ganda, sehingga risiko kebocoran informasi masih tinggi. Prinsip *integrity* menuntut agar data tidak dimodifikasi secara tidak sah selama proses pengolahan dan penyimpanan. Namun, beberapa kasus seperti perubahan nilai akademik tanpa izin atau manipulasi data kepegawaian menunjukkan lemahnya kontrol akses internal. Sementara itu, *availability* berkaitan dengan ketersediaan data saat dibutuhkan — aspek ini sering terganggu oleh serangan ransomware atau kegagalan sistem yang tidak memiliki rencana pemulihan (*disaster recovery plan*) yang baik (Munawar et al., 2022).

Prinsip-prinsip *data governance* memperluas cakupan pengelolaan keamanan data dengan menekankan tanggung jawab kelembagaan dalam menjaga kualitas, akurasi, dan kepatuhan terhadap regulasi perlindungan data pribadi (Michael & Parhusip, 2025). Berdasarkan pedoman BSSN dan panduan Kemendikbudristek, tata kelola data pendidikan seharusnya mencakup struktur organisasi keamanan informasi, kebijakan backup, dan mekanisme audit berkala. Namun, hasil penelitian menunjukkan bahwa sebagian besar sekolah masih menerapkan pendekatan yang bersifat reaktif terhadap insiden siber. Belum adanya unit khusus keamanan informasi di tingkat sekolah membuat pelaksanaan *risk management* dan *incident response* kurang optimal. Akibatnya, ketika terjadi kebocoran data atau peretasan situs, proses penanganan sering terlambat dan tidak terkoordinasi dengan baik.

Dalam perspektif teori tata kelola data, pengelolaan sistem informasi sekolah yang efektif seharusnya berlandaskan prinsip *accountability* dan *transparency*. Setiap entitas pengguna sistem — baik kepala sekolah, operator, maupun guru — harus memiliki peran dan tanggung jawab yang jelas dalam menjaga keamanan dan validitas data (Shobri, 2024). Hal ini dapat diwujudkan melalui penerapan sistem *role-based access control (RBAC)* yang sudah diatur dalam pedoman Dapodik. Dengan struktur otorisasi yang tepat, setiap akses data dapat dilacak, sehingga mengurangi potensi penyalahgunaan. Di sisi lain, proses validasi dan sinkronisasi data yang mewajibkan penandatanganan *Surat Pertanggungjawaban Mutlak (SPTJM)* juga mencerminkan penerapan prinsip *accountability* dalam manajemen data pendidikan.

Dari sisi teknis, teori keamanan data modern seperti *defense in depth* dan *redundancy principle* perlu diadopsi untuk memperkuat sistem informasi sekolah. Strategi *defense in depth* mengharuskan adanya lapisan perlindungan berjenjang — mulai dari firewall, enkripsi database, hingga kebijakan autentikasi ganda — agar serangan siber tidak langsung menembus sistem utama. Sementara itu, prinsip *redundancy* menuntut keberadaan cadangan sistem dan data (*backup*) baik secara lokal maupun berbasis *cloud* untuk memastikan kelangsungan layanan pendidikan digital (Aska et al., 2024). Panduan BSSN (2021) menegaskan bahwa sekolah harus memiliki *business continuity plan* (BCP) dan *disaster recovery plan* (DRP) untuk mengantisipasi kehilangan data akibat gangguan teknis atau serangan siber.

Hasil penelitian ini menunjukkan bahwa efektivitas keamanan dan manajemen data di sektor pendidikan masih bergantung pada kesiapan institusi dalam menerapkan prinsip-prinsip tersebut secara konsisten. Sekolah yang memiliki kebijakan backup terjadwal, sistem audit berkala, dan otorisasi pengguna yang ketat terbukti lebih siap menghadapi ancaman siber dibanding sekolah yang hanya mengandalkan inisiatif individu. Selain itu, dukungan kelembagaan dari Kementerian Pendidikan dan koordinasi dengan BSSN sangat penting untuk membangun *cyber resilience* nasional di bidang pendidikan. Penerapan teori dan kebijakan secara terpadu akan membantu mewujudkan sistem informasi sekolah yang aman, transparan, dan berkelanjutan.

Dengan demikian, integrasi antara teori keamanan data dan prinsip tata kelola data menjadi dasar penting dalam evaluasi sistem informasi sekolah di era transformasi digital. Keamanan tidak hanya dimaknai sebagai perlindungan teknis terhadap serangan, tetapi juga sebagai proses tata kelola yang mencakup kebijakan, budaya organisasi, dan tanggung jawab etis terhadap data pendidikan. Implementasi yang berkelanjutan atas prinsip CIA Triad dan *data governance framework* dapat memperkuat posisi sekolah sebagai lembaga yang tidak hanya mengelola pembelajaran digital, tetapi juga menjaga kepercayaan publik melalui pengelolaan data yang aman, andal, dan profesional.

Kesimpulan

Berdasarkan hasil penelitian, dapat disimpulkan bahwa keamanan dan manajemen data pada sistem informasi sekolah di era transformasi digital masih menghadapi berbagai tantangan, terutama dalam hal kesiapan

kelembagaan dan penerapan kebijakan keamanan yang komprehensif. Dua variabel utama, yakni keamanan data dan manajemen data, menunjukkan bahwa perlindungan data sekolah belum sepenuhnya berjalan efektif akibat lemahnya kebijakan backup, kontrol akses, serta kesadaran keamanan digital di tingkat satuan pendidikan. Meskipun berbagai pedoman seperti dari BSSN dan Kemendikbudristek telah menyediakan standar keamanan dan tata kelola data, implementasinya di lapangan masih terbatas pada aspek teknis dan belum menyentuh dimensi tata kelola menyeluruh. torisasi untuk menciptakan sistem informasi sekolah yang aman, transparan, dan berkelanjutan.

Hasil analisis memperlihatkan bahwa penerapan kebijakan backup dengan prinsip *redundancy* dan *disaster recovery plan* sebagaimana diatur dalam pedoman BSSN, serta pengelolaan akun berbasis *role-based access control (RBAC)* dalam sistem Dapodik, menjadi komponen kunci dalam menjaga integritas dan keberlanjutan sistem informasi sekolah. Penerapan kedua aspek ini memperkuat perlindungan data pribadi siswa, guru, dan tenaga kependidikan, sekaligus mendukung transparansi dan akuntabilitas lembaga pendidikan di era digital. Dengan demikian, keberhasilan transformasi digital di sektor pendidikan tidak hanya ditentukan oleh inovasi teknologi, tetapi juga oleh sejauh mana sekolah mampu menerapkan tata kelola data yang aman, beretika, dan berkelanjutan sesuai standar nasional keamanan siber.

Referensi

Ahyani, E., & Dhuhani, E. M. (2024). Transformasi Digital dalam Manajemen Perkantoran Pendidikan : Sebuah Kajian Literatur. *Jurnal Visionary : Penelitian Dan Pengembangan Dibidang Administrasi Pendidikan*, *12*(April), 205–215. https://e-journal.undikma.ac.id/index.php/visionary

Aska, M. F., Putta, D., & Magdalena, C. J. (2024). *Strategi Efektif Untuk Implementasi Keamanan Siber di Era Digital*. *5*(2), 187–200.

Badan Siber dan Sandi Negara. (2019). *Pedoman tata kelola keamanan aplikasi berbasis web* (Versi 1). BSSN.

Badan Siber dan Sandi Negara. (2021). *Peraturan Kepala BSSN Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis*. BSSN.

Mahameru, D. E., Nurhalizah, A., Wildan, A., Haikal, M., & Rahmadia, M. H. (2023). Implementasi UU Perlindungan Data Pribadi Terhadap Keamanan Informasi Identitas di Indonesia. *Jurnal Esensi Hukum*, *5*(2), 115–131.

Mania, M. A., Giu, sra Y., & Nurpriatna, A. (2025). Transformasi Digital Madrasah Aliyah: Evaluasi Efektivitas Sim Dalam Meningkatkan Kinerja Akademik Dan Manajemen. *Epistemic : Jurnal Ilmiah Pendidikan*, *4*(1), 34–55. https://doi.org/https://doi.org/10.70287/epistemic.v4i1.358

Michael, & Parhusip, J. (2025). Integrasi Prinsip Etika Profesional dalam Data Governance untuk Mendukung Keamanan dan Akurasi Informasi di Era Digital. *Journal of Multidisciplinary Inquiry in Science Technology and Educational Research*, *2*(1), 828–834. https://doi.org/https://doi.org/10.32672/mister.v2i1.2570

Monia, F. A., Hanafi, I., Rahmi, A., & Fadilah, I. (2025). Keamanan Data Dalam Sistem Manajemen. *Jurnal Manajemen Pendidikan*, *10*(1), 1–15. https://ejurnal.stkip-pessel.ac.id/index.php/jmp

Munawar, Z., Putri, N. I., Kharisma, I. L., Insany, G. P., & Mogi, I. K. A. (2022). *Keamanan Sistem Informasi (Prinsip Dasar, Teori, dan Rekayasa Penerapan Konsep)* (I). Kaizen Media Publishing.

Nurhidayat, T., dkk. (2023). *Kajian ketahanan siber: manajemen kerentanan*. Politeknik Siber dan Sandi Negara Press.

Nugraha, M. S., & Rochimat, H. (2025). Efektivitas Penerapan Sistem Informasi Manajemen Pendidikan Berbasis Cloud dalam Meningkatkan Efisiensi Administrasi Sekolah Menengah. *Jurnal Global Ilmiah*, *2*(4), 1–9.

Shobri, M. (2024). Peran Sistem Informasi Manajemen Pendidikan dalam Meningkatkan. *AKSI: Jurnal Manajemen Pendidikan Islam*, *2*(2), 78–88. https://doi.org/https://doi.org/10.37348/aksi.v2i2.302

Wandri, R., Fadhilla, M., Rachmat, P., Daulay, S., Hanafiah, A., & Fiqri, D. (2025). *Optimalisasi Pengelolaan Data Sekolah Melalui Sistem Informasi Sekolah Berbasis*.