Kanigara : Jurnal Pengabdian Kepada Masyarakat
Fakultas Pedagogi & Psikologi
Universitas PGRI Adi Buana Surabaya
http://jurnal.unipasby.ac.id/index.php/kanigara

# IMPLEMENTASI TEKNIS: TRANSFORMASI KEAMANAN DIGITAL SEKOLAH MELALUI PENDEKATAN DEFENSE-IN-DEPTH DAN ZERO-TRUST

**Feny Rita Fiantika[1]*, Dian Kusmaharti[2], Danang Prastyo[3], Wahyu Susiloningsih[4]**

[1,2,3,4]Pendidikan Guru Sekolah Dasar, Universitas PGRI Adi Buana, Surabaya, Indonesia

*Email: fenyfiantika@unipasby.ac.id

**Informasi Artikel**

**Kata kunci:**
**keamanan digital sekolah, Defense-in-Depth, Zero-Trust, keamanan siber, pengabdian masyarakat.**

**Diterima: 20-06-2026**
**Disetujui: 21-07-2026**
**Dipubikasikan: 27-07-2026**

**Keywords:**
**school digital security, Defense-in-Depth, Zero Trust, cybersecurity, community**

**Abstrak**

Transformasi digital pada sektor pendidikan telah meningkatkan pemanfaatan layanan berbasis cloud, Learning Management System (LMS), perangkat bergerak, dan sistem administrasi digital yang diikuti dengan meningkatnya risiko ancaman keamanan siber. Sebagian besar sekolah masih menghadapi keterbatasan dalam penerapan tata kelola keamanan digital, seperti belum optimalnya autentikasi pengguna, pembaruan sistem yang tidak terjadwal, rendahnya literasi keamanan siber, serta belum tersusunnya prosedur tanggap insiden. Kegiatan pengabdian kepada masyarakat ini bertujuan meningkatkan kapasitas sekolah dalam mengimplementasikan keamanan digital melalui pendekatan **Defense-in-Depth** dan **Zero-Trust Architecture**. Metode yang digunakan meliputi observasi awal, asesmen kebutuhan, pelatihan teknis, pendampingan implementasi, simulasi serangan phishing, evaluasi, dan monitoring terhadap kepala sekolah, guru, operator sekolah, serta tenaga teknologi informasi. Hasil kegiatan menunjukkan tersusunnya kebijakan keamanan digital sekolah, implementasi **Multi-Factor Authentication (MFA)** pada akun prioritas, penyusunan jadwal **Patch Management** mingguan, penerapan **Endpoint Protection**, pengenalan **Mobile Device Management (MDM)**, serta penyusunan **Incident Response Plan (IRP)**. Selain itu, terjadi peningkatan literasi keamanan siber dan kesadaran keamanan informasi di kalangan peserta. Implementasi kedua pendekatan tersebut memperkuat ketahanan organisasi melalui pengelolaan identitas digital, pengendalian hak akses, perlindungan perangkat, serta monitoring keamanan secara berkelanjutan. Program ini memberikan model implementasi keamanan digital yang aplikatif dan berkelanjutan bagi sekolah dalam mendukung transformasi pendidikan berbasis teknologi informasi.

***Abstact***

Digital transformation in the education sector has accelerated the adoption of cloud-based services, Learning Management Systems (LMS), mobile devices, and digital school management platforms, while simultaneously increasing cybersecurity risks. Many schools still face challenges in implementing effective cybersecurity governance, including weak user authentication, irregular system updates, limited cybersecurity awareness, and the absence of formal incident response procedures. This community service program aimed to strengthen schools' cybersecurity capacity through the implementation of **Defense-in-Depth** and **Zero Trust Architecture** approaches. The program employed initial observation, needs assessment, technical training, implementation assistance, phishing simulation, evaluation, and continuous monitoring involving school principals, teachers, school administrators, and information technology personnel. The

implementation resulted in the development of school digital security policies, deployment of **Multi-Factor Authentication (MFA)** for priority accounts, establishment of weekly **Patch Management** procedures, implementation of **Endpoint Protection**, introduction of **Mobile Device Management (MDM)**, and preparation of an **Incident Response Plan (IRP)**. Furthermore, participants demonstrated improved cybersecurity awareness and digital security literacy. The integration of Defense-in-Depth and Zero Trust approaches enhanced organizational cyber resilience through identity management, access control, endpoint protection, and continuous security monitoring. This program provides a practical and sustainable cybersecurity implementation model that can support secure digital transformation in educational institutions.

## PENDAHULUAN

Transformasi digital pada sektor pendidikan telah membawa perubahan yang sangat signifikan terhadap tata kelola sekolah. Berbagai aktivitas administrasi, pembelajaran, penilaian, komunikasi, hingga penyimpanan data kini dilakukan melalui sistem digital berbasis internet. Pemanfaatan Learning Management System (LMS), Cloud Computing, aplikasi administrasi sekolah, media pembelajaran digital, serta perangkat bergerak (mobile devices) telah meningkatkan efisiensi proses pendidikan sekaligus memperluas akses terhadap sumber belajar. Namun demikian, digitalisasi tersebut juga diikuti oleh meningkatnya kompleksitas ancaman keamanan siber yang dapat mengganggu keberlangsungan layanan pendidikan serta mengancam kerahasiaan, integritas, dan ketersediaan data sekolah (ENISA, 2023).

Dalam beberapa tahun terakhir, institusi pendidikan menjadi salah satu sektor yang paling sering menjadi sasaran serangan siber. Data Sophos menunjukkan bahwa lebih dari 80% institusi pendidikan tingkat dasar dan menengah pernah mengalami serangan ransomware dalam satu tahun terakhir (Sophos, 2023). Selain ransomware, sekolah juga menghadapi berbagai bentuk ancaman lain seperti phishing, malware, distributed denial of service (DDoS), pencurian identitas digital, eksploitasi kerentanan aplikasi, hingga penyalahgunaan akun pengguna. Ancaman tersebut tidak hanya menyebabkan kerugian finansial, tetapi juga berpotensi menghentikan proses pembelajaran, merusak reputasi institusi, serta menimbulkan pelanggaran terhadap perlindungan data pribadi peserta didik. Di Indonesia, percepatan implementasi transformasi digital melalui berbagai platform pembelajaran dan administrasi sekolah belum sepenuhnya diimbangi dengan peningkatan kapasitas keamanan siber pada tingkat satuan pendidikan. Sebagian besar sekolah masih menerapkan model keamanan tradisional yang berorientasi pada perlindungan jaringan (perimeter security), sementara pola akses pengguna telah berubah menjadi lebih dinamis melalui layanan cloud, perangkat pribadi (Bring Your Own Device/BYOD), serta pembelajaran jarak jauh. Kondisi tersebut menyebabkan batas keamanan jaringan menjadi semakin kabur sehingga pendekatan keamanan konvensional menjadi kurang efektif dalam menghadapi ancaman siber modern. Paradigma keamanan siber saat ini mengalami pergeseran menuju konsep **Defense-in-**

**Depth**, yaitu strategi pertahanan berlapis yang mengintegrasikan berbagai mekanisme pengamanan pada seluruh komponen sistem informasi. Strategi ini memastikan bahwa apabila satu lapisan keamanan berhasil ditembus, lapisan berikutnya masih mampu memberikan perlindungan terhadap aset digital organisasi (NIST, 2020). Implementasi Defense-in-Depth meliputi penguatan identitas digital, pengamanan perangkat (endpoint security), segmentasi jaringan, pengelolaan akses, monitoring keamanan, pencadangan data, serta peningkatan kesadaran pengguna melalui edukasi keamanan siber. Sejalan dengan konsep tersebut, pendekatan **Zero-Trust Architecture** berkembang sebagai paradigma baru dalam pengelolaan keamanan digital. Prinsip utama Zero-Trust adalah **"Never Trust, Always Verify"**, yaitu tidak memberikan kepercayaan secara otomatis kepada setiap pengguna, perangkat, maupun aplikasi, meskipun berada di dalam jaringan internal organisasi. Seluruh permintaan akses harus melalui proses autentikasi, otorisasi, dan validasi identitas secara berkelanjutan berdasarkan tingkat risiko yang dimiliki (NIST, 2020). Pendekatan ini dinilai lebih sesuai dengan karakteristik ekosistem pendidikan modern yang memanfaatkan layanan cloud, perangkat bergerak, serta akses jarak jauh. Berdasarkan hasil observasi awal terhadap sekolah mitra, ditemukan beberapa permasalahan utama yang menjadi fokus kegiatan pengabdian kepada masyarakat. Pertama, sebagian besar akun guru dan tenaga kependidikan masih menggunakan autentikasi berbasis kata sandi tunggal tanpa dukungan Multi-Factor Authentication (MFA). Kedua, proses pembaruan sistem operasi dan aplikasi belum dilakukan secara terjadwal sehingga meningkatkan risiko eksploitasi terhadap kerentanan perangkat lunak. Ketiga, perangkat komputer laboratorium maupun laptop guru belum seluruhnya dilengkapi dengan solusi Endpoint Detection and Response (EDR) yang mampu mendeteksi aktivitas malware secara real-time. Keempat, belum tersedia kebijakan Mobile Device Management (MDM) untuk mengendalikan penggunaan perangkat digital yang digunakan dalam proses pembelajaran. Selain itu, sekolah juga belum memiliki prosedur baku dalam menangani insiden keamanan siber melalui Incident Response Plan (IRP). Permasalahan tersebut menunjukkan bahwa peningkatan infrastruktur digital harus diikuti dengan peningkatan kapasitas sumber daya manusia dalam mengelola keamanan informasi. Keamanan siber bukan hanya menjadi tanggung jawab tenaga teknologi informasi, melainkan merupakan tanggung jawab seluruh warga sekolah yang melibatkan kepala sekolah, guru, tenaga kependidikan, peserta didik, serta orang tua. Oleh karena itu, kegiatan pengabdian kepada masyarakat perlu diarahkan tidak hanya pada penyediaan teknologi keamanan, tetapi juga pada penguatan budaya keamanan informasi (security awareness) melalui pelatihan, pendampingan teknis, simulasi serangan siber, dan penyusunan kebijakan keamanan digital sekolah.

SDN Gelam 2 Candi Sidoarjo merupakan sekolah yang sedang menyiapkan diri untuk menggunakan pembelajaran berbasis IT. Oleh karenanya sekolah tersebut memulai dengan menyiapkan SDM sekolah untuk belajar lebih banyak tentang teknologi dan siber. SDN Gelam 2

menggandeng dosen-dosen PGSD Universitas PGRI Adi Buana Surabaya dan Universitas Muhammadiyah Sidoarjo untuk melaksanakan kegiatan pendampingan bersama guru-guru Sekolah Dasar se-kecamatan Candi Sidoarjo. Kegiatan pengabdian masyarakat ini dirancang sebagai implementasi teknis transformasi keamanan digital sekolah melalui pendekatan **Defense-in-Depth** dan **Zero-Trust**. Program dilaksanakan dalam bentuk pelatihan intensif, pendampingan implementasi Multi-Factor Authentication (MFA), penyusunan kebijakan Patch Management, penerapan Endpoint Protection, pengenalan Mobile Device Management (MDM), penyusunan Incident Response Plan (IRP), serta simulasi mitigasi serangan phishing sebagai bagian dari peningkatan literasi keamanan siber. Seluruh materi dan tahapan implementasi mengacu pada **Panduan Implementasi Teknis: Transformasi Keamanan Digital Sekolah melalui Pendekatan Defense-in-Depth dan Zero-Trust** yang menjadi acuan utama kegiatan pengabdian. Melalui kegiatan pengabdian ini diharapkan sekolah mampu membangun sistem keamanan digital yang lebih tangguh, adaptif, dan berkelanjutan. Implementasi Defense-in-Depth dan Zero-Trust tidak hanya meningkatkan perlindungan terhadap aset digital sekolah, tetapi juga membentuk budaya keamanan informasi yang melibatkan seluruh warga sekolah sebagai bagian dari transformasi digital pendidikan yang aman, terpercaya, dan berkelanjutan.

## METODE

Pengabdian dilaksanakan dalam lima tahapan utama yang saling berkesinambungan, yaitu observasi awal, asesmen kebutuhan, pelatihan teknis, pendampingan implementasi, serta evaluasi dan monitoring. Rangkaian kegiatan dirancang untuk membantu sekolah membangun sistem keamanan digital yang komprehensif berdasarkan prinsip **Defense-in-Depth** dan **Zero-Trust Architecture**, sehingga setiap lapisan sistem informasi memperoleh perlindungan secara menyeluruh.

### Lokasi, Waktu, dan Sasaran Pengabdian

Kegiatan pengabdian dilaksanakan pada sekolah mitra yang telah/sedang proses menyiapkan penerapan sistem pembelajaran digital, Learning Management System (LMS), layanan cloud, serta jaringan internet sebagai pendukung proses pembelajaran dan administrasi sekolah. Pelaksanaan kegiatan berlangsung selama **satu bulan**, yang terdiri atas tahap persiapan, pelaksanaan, pendampingan, dan evaluasi.

Sasaran kegiatan meliputi:

1. Kepala sekolah sebagai pengambil kebijakan keamanan digital sekolah.
2. Guru sebagai pengguna utama layanan pembelajaran digital.
3. Operator sekolah sebagai pengelola sistem administrasi berbasis teknologi informasi.
4. Tenaga Teknologi Informasi (IT Support) sebagai pelaksana implementasi teknis keamanan siber.

Pemilihan sasaran tersebut didasarkan pada peran strategis masing-masing dalam membangun budaya keamanan informasi (*security awareness*) di lingkungan sekolah.

## HASIL DAN PEMBAHASAN

Pelaksanaan kegiatan pengabdian kepada masyarakat menghasilkan berbagai luaran yang menunjukkan peningkatan kapasitas sekolah dalam mengelola keamanan digital secara sistematis. Seluruh rangkaian kegiatan dilaksanakan berdasarkan tahapan observasi, pelatihan, pendampingan implementasi, simulasi keamanan siber, serta monitoring dan evaluasi. Implementasi dilakukan dengan mengacu pada prinsip **Defense-in-Depth** dan **Zero-Trust Architecture** sehingga penguatan keamanan tidak hanya difokuskan pada infrastruktur teknologi, tetapi juga pada tata kelola organisasi dan peningkatan kompetensi sumber daya manusia.

### Penyusunan Kebijakan Keamanan Digital Sekolah

Salah satu luaran utama kegiatan pengabdian adalah tersusunnya **Kebijakan Keamanan Digital Sekolah** yang menjadi pedoman bagi seluruh warga sekolah dalam memanfaatkan teknologi informasi secara aman dan bertanggung jawab. Sebelum pelaksanaan kegiatan, sekolah belum memiliki dokumen kebijakan yang mengatur standar pengelolaan akun digital, penggunaan perangkat pribadi, mekanisme pencadangan data, maupun prosedur penanganan insiden keamanan siber. Kondisi tersebut menyebabkan setiap pengguna menerapkan praktik keamanan yang berbeda sehingga meningkatkan risiko terjadinya kebocoran data.

Melalui pendampingan teknis, sekolah berhasil menyusun dokumen kebijakan yang mencakup pengelolaan identitas digital, penggunaan kata sandi yang kuat, pengaturan hak akses berdasarkan tugas dan fungsi pengguna, mekanisme pembaruan perangkat lunak, prosedur pencadangan data, serta tata cara pelaporan insiden keamanan informasi. Penyusunan kebijakan ini menjadi fondasi utama dalam membangun tata kelola keamanan digital yang terstandarisasi sehingga seluruh aktivitas digital sekolah memiliki pedoman operasional yang jelas.

### Implementasi Multi-Factor Authentication (MFA)

Hasil kegiatan menunjukkan bahwa sekolah berhasil menerapkan **Multi-Factor Authentication (MFA)** pada akun administrator, kepala sekolah, operator, dan guru yang memiliki akses terhadap sistem informasi sekolah. Sebelum pendampingan, sebagian besar akun masih menggunakan autentikasi berbasis kata sandi tunggal sehingga sangat rentan terhadap serangan phishing maupun pencurian kredensial. Pendampingan dilakukan melalui aktivasi aplikasi autentikator berbasis perangkat bergerak, konfigurasi autentikasi dua faktor pada Google Workspace maupun Microsoft 365 Education, serta pelatihan penggunaan kode pemulihan (recovery code). Implementasi MFA memberikan lapisan keamanan tambahan karena setiap proses autentikasi tidak hanya memerlukan kata sandi, tetapi juga memerlukan verifikasi identitas melalui perangkat yang dimiliki pengguna. Penerapan MFA secara signifikan meningkatkan keamanan

identitas digital sekolah. Walaupun kata sandi pengguna berhasil diketahui pihak lain, akses ke sistem tetap tidak dapat dilakukan tanpa proses verifikasi kedua. Kondisi ini sejalan dengan prinsip **Zero-Trust**, yaitu tidak memberikan kepercayaan secara otomatis kepada setiap permintaan akses sebelum dilakukan proses autentikasi dan otorisasi secara menyeluruh.

**Implementasi Patch Management dan Vulnerability Management**

Hasil pendampingan juga menunjukkan tersusunnya **jadwal pembaruan sistem (weekly patch management)** sebagai bagian dari pengelolaan kerentanan (vulnerability management). Sebelum kegiatan berlangsung, pembaruan sistem operasi maupun aplikasi dilakukan secara tidak terjadwal sehingga banyak perangkat menggunakan versi perangkat lunak yang telah memiliki celah keamanan. Melalui kegiatan pengabdian, sekolah berhasil menyusun kebijakan pembaruan mingguan yang mencakup sistem operasi, aplikasi pembelajaran, browser, antivirus, serta aplikasi administrasi sekolah. Tim teknologi informasi sekolah juga memperoleh panduan mengenai prioritas pembaruan berdasarkan tingkat risiko keamanan sehingga proses patching dapat dilakukan secara sistematis. Implementasi patch management terbukti meningkatkan kesiapan sekolah dalam mengurangi peluang eksploitasi terhadap kerentanan perangkat lunak yang umum dimanfaatkan oleh pelaku serangan siber. Selain meningkatkan keamanan, pembaruan berkala juga memberikan dampak positif terhadap stabilitas dan performa perangkat yang digunakan dalam proses pembelajaran.

**Implementasi Endpoint Protection dan Mobile Device Management**

Pendampingan implementasi menghasilkan peningkatan perlindungan terhadap perangkat yang digunakan di lingkungan sekolah melalui penerapan **Endpoint Protection** dan **Mobile Device Management (MDM)**. Seluruh komputer laboratorium dan perangkat administrasi dipastikan menggunakan perangkat lunak antivirus yang selalu diperbarui serta memiliki kemampuan mendeteksi malware secara real-time. Selain itu, sekolah mulai menerapkan kebijakan pengelolaan perangkat bergerak yang digunakan dalam pembelajaran. Melalui Mobile Device Management, administrator dapat mengendalikan distribusi aplikasi, melakukan pembatasan akses terhadap situs yang tidak sesuai, mengatur waktu penggunaan perangkat, serta melakukan penghapusan data secara jarak jauh apabila perangkat hilang atau dicuri. Implementasi kedua mekanisme tersebut memperkuat lapisan perlindungan perangkat (endpoint layer) dalam strategi **Defense-in-Depth**, sehingga setiap perangkat yang terhubung ke jaringan sekolah tetap berada dalam pengawasan administrator.

**Peningkatan Literasi Keamanan Siber**

Aspek lain yang mengalami peningkatan adalah **literasi keamanan siber** seluruh peserta kegiatan. Pelatihan tidak hanya memberikan pemahaman mengenai konsep dasar keamanan digital, tetapi juga membangun kemampuan praktis dalam mengenali berbagai bentuk ancaman siber yang sering terjadi di lingkungan pendidikan. Materi pelatihan meliputi identifikasi email

phishing, teknik social engineering, pengelolaan kata sandi yang aman, perlindungan data pribadi, penggunaan autentikasi multifaktor, serta praktik penggunaan layanan cloud secara aman. Selanjutnya dilakukan simulasi serangan phishing untuk mengukur kemampuan peserta dalam membedakan komunikasi resmi dengan pesan yang bersifat manipulatif. Hasil simulasi menunjukkan peningkatan kemampuan peserta dalam mengenali karakteristik tautan mencurigakan, memahami pentingnya verifikasi identitas pengirim, serta melaporkan dugaan serangan kepada administrator sekolah. Kondisi tersebut menunjukkan bahwa peningkatan kesadaran keamanan (security awareness) menjadi salah satu faktor penting dalam memperkuat sistem pertahanan digital sekolah karena sebagian besar serangan siber memanfaatkan kelemahan manusia sebagai titik masuk utama.

**Penyusunan Incident Response Plan (IRP)**

Luaran penting lainnya adalah tersusunnya **Incident Response Plan (IRP)** sebagai prosedur baku dalam menangani insiden keamanan informasi. Sebelum kegiatan pengabdian, sekolah belum memiliki mekanisme penanganan yang sistematis apabila terjadi kebocoran data, infeksi malware, maupun serangan ransomware. Melalui pendampingan, sekolah berhasil menyusun alur penanganan insiden yang terdiri atas tahap identifikasi, isolasi perangkat terdampak, pelaporan kepada pimpinan sekolah, pemulihan data melalui sistem pencadangan, dokumentasi insiden, serta evaluasi pasca kejadian. Adanya prosedur ini meningkatkan kesiapan organisasi dalam meminimalkan dampak operasional apabila terjadi gangguan keamanan siber.

## KESIMPULAN

kegiatan pengabdian kepada masyarakat menunjukkan bahwa penerapan pendekatan **Defense-in-Depth** dan **Zero-Trust Architecture** merupakan strategi yang efektif dalam mendukung transformasi keamanan digital di lingkungan sekolah. Pendekatan ini mampu membangun sistem pertahanan keamanan siber yang lebih komprehensif melalui penerapan perlindungan berlapis yang mencakup aspek kebijakan, teknologi, proses bisnis, serta peningkatan kapasitas sumber daya manusia. Implementasi keamanan tidak lagi hanya berorientasi pada perlindungan jaringan (perimeter security), tetapi juga menempatkan identitas digital, perangkat pengguna, aplikasi, data, dan aktivitas pengguna sebagai komponen utama yang harus diamankan secara berkesinambungan. Kegiatan pengabdian menghasilkan berbagai luaran yang mendukung penguatan tata kelola keamanan digital sekolah, antara lain tersusunnya kebijakan keamanan digital sekolah, implementasi **Multi-Factor Authentication (MFA)** pada akun prioritas, penyusunan mekanisme **Patch Management** secara berkala, penerapan **Endpoint Protection**, pengenalan **Mobile Device Management (MDM)**, serta tersusunnya **Incident Response Plan (IRP)** sebagai pedoman penanganan insiden keamanan siber. Luaran tersebut memberikan fondasi awal bagi sekolah dalam membangun sistem keamanan informasi yang lebih terstruktur,

terdokumentasi, dan sesuai dengan praktik terbaik keamanan siber. Pendampingan teknis yang dilakukan selama kegiatan juga memberikan dampak positif terhadap peningkatan kompetensi kepala sekolah, guru, operator sekolah, dan tenaga teknologi informasi dalam memahami serta mengimplementasikan prinsip-prinsip keamanan digital. Melalui pelatihan, praktik langsung, dan simulasi serangan phishing, peserta menunjukkan peningkatan kemampuan dalam mengenali ancaman siber, mengelola identitas digital secara aman, menerapkan autentikasi multifaktor, serta melaksanakan prosedur tanggap darurat apabila terjadi insiden keamanan informasi. Kondisi tersebut menunjukkan bahwa peningkatan literasi keamanan siber merupakan faktor penting dalam membangun budaya keamanan informasi (*security awareness*) di lingkungan sekolah. Selain meningkatkan kapasitas individu, kegiatan ini juga memperkuat ketahanan organisasi (*organizational cyber resilience*). Penerapan prinsip **Zero-Trust** mendorong sekolah untuk menerapkan verifikasi identitas secara berkelanjutan terhadap seluruh pengguna dan perangkat sebelum diberikan akses ke sistem informasi. Sementara itu, strategi **Defense-in-Depth** memastikan bahwa setiap lapisan keamanan saling melengkapi sehingga kegagalan pada satu mekanisme perlindungan tidak secara langsung menyebabkan terganggunya seluruh sistem. Integrasi kedua pendekatan tersebut mampu mengurangi risiko kebocoran data, penyalahgunaan akun, serangan malware, ransomware, maupun berbagai ancaman siber lainnya yang berpotensi mengganggu keberlangsungan proses pembelajaran. Berdasarkan hasil pelaksanaan pengabdian, pendekatan **Defense-in-Depth** dan **Zero-Trust** layak direkomendasikan sebagai model transformasi keamanan digital bagi satuan pendidikan, khususnya sekolah yang sedang mengembangkan ekosistem pembelajaran berbasis teknologi informasi. Keberhasilan implementasi model ini sangat dipengaruhi oleh komitmen pimpinan sekolah, kesiapan sumber daya manusia, dukungan infrastruktur teknologi informasi, serta keberlanjutan program pelatihan dan pendampingan. Sebagai tindak lanjut, sekolah disarankan untuk melakukan evaluasi keamanan siber secara berkala, memperbarui kebijakan keamanan informasi sesuai perkembangan teknologi dan regulasi, memperluas implementasi autentikasi multifaktor pada seluruh pengguna, meningkatkan pemanfaatan sistem monitoring keamanan secara real-time, serta menyelenggarakan program literasi keamanan siber secara berkesinambungan bagi seluruh warga sekolah. Dengan demikian, transformasi digital pendidikan tidak hanya menghasilkan layanan pembelajaran yang lebih efektif dan efisien, tetapi juga mampu menciptakan lingkungan digital yang aman, tangguh, dan berkelanjutan dalam menghadapi dinamika ancaman siber di masa mendatang.

**UCAPAN TERIMAKASIH**

Terima kasih kepada seluruh mitra sekolah SDN Gelam 2 Candi Sidoarjo, tim Universitas PGRI Adi Buana Surabaya dan pihak yang mendukung kegiatan pengabdian.

**DAFTAR PUSTAKA**

Cybersecurity and Infrastructure Security Agency. (2023). *Cross-Sector Cybersecurity Performance Goals*. U.S. Department of Homeland Security.

European Union Agency for Cybersecurity. (2023). *ENISA Threat Landscape 2023*.

Hasan, M. (2024). *Enhancing Enterprise Security with Zero Trust Architecture*. *arXiv*. https://doi.org/10.48550/arXiv.2410.18291

Kim, H., Kim, Y., & Kim, S. (2024). *A Study on the Security Requirements Analysis to Build a Zero Trust-Based Remote Work Environment*. *arXiv*. https://doi.org/10.48550/arXiv.2401.03675

Microsoft. (2024). *Microsoft Digital Defense Report 2024*.

National Institute of Standards and Technology. (2020). *Planning a Zero Trust Architecture: A Starting Guide for Federal Administrators (NIST CSWP 20)*. https://doi.org/10.6028/NIST.CSWP.20

Oz, H., Aris, A., Levi, A., & Uluagac, A. S. (2021). A Survey on Ransomware: Evolution, Taxonomy, and Defense Solutions. *ACM Computing Surveys*. https://doi.org/10.48550/arXiv.2102.06249

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero Trust Architecture (NIST Special Publication 800-207)*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

Sophos. (2023). *The State of Ransomware in Education 2023*.

Mavroudis, V. (2024). *Zero-Trust Network Access (ZTNA)*. *arXiv*. https://doi.org/10.48550/arXiv.2410.20611