**EDUSCOTECH**, Vol.6 No.1 Januari 2025
**ISSN**: 2716-0653 (Print) | 2716-0645 (Online)
**DOI**:https://doi.org/10.XXXX/eduscotech.xxxx.xxx

# Penyusunan dan Uji Terap SOP Penanganan Insiden Jaringan Sekolah

**Diterima:**
10 Desember 2024
**Revisi:**
10 Januari 2025
**Terbit:**
15 Januari 2025

**[1]Suparno, [2]Pirdaus Jihan Oktavianto**
*[1,2]Universitas Doktor Nugroho Magetan*
*[1,2]Magetan, Indonesia*
*E-mail: likparno@udn.ac.id*

***Abstract***— *The use of computer networks in schools plays a crucial role in supporting digital-based learning processes and administrative services. However, increasing reliance on networks also carries the risk of network incidents, both technical disruptions and security threats, which can hamper school operations. This study aims to develop and test a Standard Operating Procedure (SOP) for handling school network incidents as an effort to improve preparedness and the effectiveness of responses to network incidents. The research method used is applied research with a qualitative descriptive approach through case studies in school environments. The research stages include needs analysis, development of a network incident handling SOP, implementation testing of the SOP through incident simulations, and evaluation of its effectiveness. Data collection techniques were conducted through interviews, observation, and documentation, while data analysis was conducted using qualitative descriptive methods. The results show that the developed SOP provides clear and structured guidance for school technical teams in handling network incidents. The implementation testing of the SOP demonstrated improved response speed, handling accuracy, and consistency of actions during the network recovery process. Thus, the development and implementation of a network incident handling SOP has been proven to improve preparedness and more effective school network management.*

***Keywords:*** *SOP, Network Incident Handling, School Network, Network Management, Network Security.*

## I. PENDAHULUAN

Perkembangan pemanfaatan teknologi informasi dan komunikasi dalam dunia pendidikan telah menjadikan jaringan komputer dan akses internet sebagai bagian penting dalam menunjang proses pembelajaran, administrasi sekolah, dan kegiatan akademik lainnya. Peningkatan penggunaan jaringan nirkabel dan internet di sekolah memberikan kemudahan akses informasi, tetapi secara bersamaan membuka peluang terjadinya ancaman keamanan jaringan, seperti akses tidak sah, manipulasi data, serta gangguan sistem yang dapat menghambat kelancaran kegiatan pembelajaran. Penelitian di lingkungan sekolah menunjukkan bahwa jaringan nirkabel sangat rentan terhadap serangan seperti Man in the Middle (MitM), di mana pihak tidak berwenang dapat memantau atau memanipulasi komunikasi data yang berjalan dalam jaringan pendidikan [1].

Selain ancaman teknis, rendahnya literasi keamanan siber di kalangan guru dan siswa menjadi tantangan serius. Kurangnya pemahaman tentang penggunaan kata sandi yang kuat, autentikasi, dan perlindungan data pribadi meningkatkan risiko perilaku tidak aman yang dapat memicu penyalahgunaan akun serta eksploitasi sistem jaringan [2]. Ancaman tersebut bukan hanya berdampak pada ketersediaan layanan tetapi juga dapat mengancam kerahasiaan data akademik dan pribadi pengguna. Analisis keamanan jaringan di tingkat pendidikan menunjukkan kelemahan dalam sistem keamanan dapat menyebabkan gangguan serius dalam operasional

sehari-hari, sehingga dibutuhkan strategi pengamanan yang adaptif dan prosedur baku untuk menanggapi insiden [3]. Kajian tentang mekanisme keamanan juga menunjukkan penggunaan alat seperti firewall dan sistem proteksi jaringan lainnya dapat meningkatkan stabilitas serta efektivitas pengendalian ancaman keamanan jaringan di lingkungan pendidikan [4].

Insiden keamanan jaringan adalah kejadian tak terduga yang mengganggu operasional layanan TI dan mengancam kerahasiaan, integritas, serta ketersediaan sistem jaringan komputer. Dalam manajemen layanan TI, insiden didefinisikan sebagai gangguan atau penurunan kualitas layanan IT yang memerlukan penanganan cepat untuk mengembalikan layanan ke kondisi normal dan mencegah dampak lebih lanjut [5]. Standard Operating Procedure (SOP) penanganan insiden berisi langkah-langkah formal yang harus dijalankan secara konsisten oleh personel berwenang untuk menjamin penanganan insiden dilakukan sistematis, cepat, dan terdokumentasi, sesuai praktik terbaik atau standar global seperti ITIL [6]. Dalam organisasi pendidikan, manajemen insiden mencakup prosedur khusus untuk menangani gangguan pada layanan TI yang berdampak pada proses pembelajaran atau administrasi [7].

Beberapa penelitian mendukung pentingnya SOP manajemen insiden. Brigidta et al. (2024) menunjukkan penerapan SOP berbasis ITIL V3 meningkatkan konsistensi penanganan insiden dan dokumentasi di instansi pemerintah [8]. Aulia et al. (2025) menegaskan bahwa ketiadaan prosedur terstruktur menyebabkan ketidakkonsistenan, keterlambatan respon, dan kurangnya dokumentasi, sehingga SOP yang lengkap dan sistematis diperlukan [9]. Permatasari dan Yohannis (2025) menemukan bahwa tingkat kesadaran dan kesiapan organisasi dalam merespons insiden keamanan informasi masih rendah, sehingga pelatihan berkelanjutan dan SOP yang jelas diperlukan untuk meningkatkan kemampuan staf [10]. Sementara itu, Romadhon dan Salman (2025) menunjukkan bahwa penggunaan skenario serangan sebagai media pelatihan meningkatkan pemahaman praktis tim respon insiden terhadap langkah-langkah penanganan insiden siber secara sistematis dan terkoordinasi [11]. Oleh karena itu, sangat penting bagi sekolah untuk memiliki Standard Operating Procedure (SOP) penanganan insiden jaringan yang terstruktur, terdokumentasi, serta diuji secara praktis agar setiap insiden dapat direspon secara cepat, konsisten, dan efektif sesuai standar keamanan jaringan modern.

## II. METODE PENELITIAN

### A. Jenis Penelitian

Penelitian ini menggunakan jenis penelitian terapan (applied research) karena bertujuan untuk menghasilkan produk berupa Standar Operasional Prosedur (SOP) penanganan insiden jaringan sekaligus menguji penerapannya secara langsung di lingkungan sekolah. Penelitian terapan dipilih karena fokusnya tidak hanya pada pengembangan konsep atau teori, tetapi juga pada pemecahan masalah nyata yang dihadapi dalam pengelolaan dan penanganan insiden jaringan, sehingga hasil penelitian dapat memberikan manfaat praktis bagi operasional jaringan sekolah.

**ISSN**: 2716-0653 (Print) | 2716-0645 (Online)
**DOI**:https://doi.org/10.XXXX/eduscotech.xxxx.xxx

B. **Desain Penelitian**

Penelitian ini menggunakan pendekatan deskriptif kualitatif dengan metode studi kasus untuk menggambarkan proses penyusunan, uji terap, dan penerapan SOP. Tahapan penelitian meliputi analisis kebutuhan, penyusunan dokumen, uji terap melalui simulasi insiden jaringan, serta evaluasi efektivitas SOP. Metode studi kasus dipilih untuk memperoleh pemahaman mendalam mengenai praktik operasional tim TI dan tantangan dalam penanganan insiden jaringan.

**C. Teknik Pengumpulan Data**

Pengumpulan data dilakukan melalui beberapa metode. Pertama, wawancara dengan pihak-pihak yang terlibat dalam pengelolaan jaringan sekolah, seperti tim teknis atau pengelola TI, bertujuan untuk memperoleh informasi mengenai kondisi jaringan, jenis insiden yang sering terjadi, serta kebutuhan prosedur penanganan insiden. Kedua, observasi dilakukan selama uji terap SOP untuk memantau secara langsung proses penanganan insiden serta kepatuhan tim terhadap prosedur yang telah ditetapkan. Ketiga, dokumentasi dikumpulkan berupa catatan insiden, hasil simulasi, dan dokumen SOP sebagai bahan analisis dan verifikasi data.

**D. Teknik Analisis Data**

Analisis data dilakukan menggunakan teknik deskriptif kualitatif dengan cara mengelompokkan data sesuai tahapan SOP dan membandingkannya dengan pelaksanaan nyata saat uji terap. Hasil analisis ini digunakan untuk menilai efektivitas SOP, mengidentifikasi kendala yang muncul selama penerapan, serta menjadi dasar perbaikan dan penyempurnaan prosedur. Dengan demikian, metode analisis ini tidak hanya menilai implementasi SOP, tetapi juga memberikan masukan yang berguna untuk pengembangan prosedur yang lebih optimal.

## III. HASIL DAN PEMBAHASAN

**A. Penyusunan SOP Penanganan Insiden Jaringan**

Penelitian ini menghasilkan dokumen Standar Operasional Prosedur (SOP) penanganan insiden jaringan yang disusun berdasarkan studi literatur, kebutuhan operasional sekolah, dan kondisi aktual jaringan. SOP tersebut mencakup beberapa tahapan penting yaitu identifikasi dan pelaporan insiden, analisis awal penyebab gangguan, klasifikasi insiden berdasarkan tingkat dampak, prosedur penanganan sesuai jenis insiden, mekanisme eskalasi apabila insiden tidak dapat ditangani pada level awal, serta proses pemulihan dan dokumentasi pasca-insiden. Penyusunan SOP bertujuan memberikan pedoman terstruktur bagi tim teknis sekolah agar merespons insiden secara sistematis dan konsisten, sehingga risiko gangguan layanan berkurang serta operasional jaringan tetap stabil.

**B. Uji Terapan SOP di Sekolah**

Uji terapan SOP dilakukan melalui simulasi insiden jaringan, meliputi gangguan koneksi internet, kesalahan konfigurasi perangkat, dan simulasi serangan denial of service. Hasil uji terap menunjukkan bahwa tim teknis mampu mendeteksi dan melaporkan insiden lebih cepat

dibandingkan sebelum adanya SOP. Selain itu, langkah penanganan menjadi lebih terarah dan tidak bersifat trial and error, karena seluruh tindakan mengacu pada prosedur yang telah ditetapkan dalam SOP. Hal ini menunjukkan bahwa SOP berperan penting dalam mempercepat respons dan mengurangi ketidakpastian dalam menangani insiden.

**C. Evaluasi Efektivitas SOP**

Efektivitas SOP dievaluasi berdasarkan waktu respon terhadap insiden, kecepatan pemulihan layanan, dan tingkat kepatuhan tim TI terhadap prosedur. Hasil evaluasi menunjukkan waktu respon meningkat secara signifikan, dengan identifikasi sumber masalah yang lebih cepat. Proses pemulihan layanan berjalan lebih terstruktur dan terdokumentasi dengan baik, sehingga memudahkan evaluasi pasca-insiden. Kepatuhan tim TI terhadap SOP juga menunjukkan hasil positif, meskipun masih diperlukan pembiasaan agar seluruh tahapan dapat dijalankan secara optimal dan konsisten.

**D. Pembahasan**

Hasil penelitian penyusunan dan penerapan SOP memberikan dampak positif terhadap kesiapsiagaan serta manajemen jaringan di lingkungan sekolah. SOP berperan sebagai panduan operasional yang membantu tim TI merespons insiden secara cepat, konsisten, dan terdokumentasi, sejalan dengan prinsip manajemen jaringan yang menekankan pentingnya prosedur baku dalam menjaga stabilitas dan keamanan sistem. Namun, masih terdapat kendala seperti kebutuhan pelatihan lanjutan bagi tim teknis serta peningkatan sistem pencatatan log insiden. Dengan demikian, keberhasilan penerapan SOP tidak hanya bergantung pada dokumen, tetapi juga pada kompetensi sumber daya manusia serta evaluasi dan pembaruan prosedur secara berkelanjutan.

## KESIMPULAN DAN SARAN

Penelitian ini menunjukkan bahwa Standar Operasional Prosedur (SOP) penanganan insiden jaringan yang terstruktur dan terdokumentasi dengan baik sangat penting untuk mendukung keberlangsungan operasional jaringan di lingkungan sekolah. SOP yang disusun mampu memberikan panduan yang sistematis bagi tim TI dalam melakukan deteksi, penanganan, serta pemulihan insiden jaringan secara cepat dan terarah. Hasil uji terap menunjukkan bahwa penerapan SOP meningkatkan kesiapsiagaan serta konsistensi tindakan tim TI, sehingga potensi gangguan layanan dapat diminimalkan. Dengan demikian, aktivitas pembelajaran berbasis teknologi dapat berlangsung secara optimal tanpa terganggu oleh masalah jaringan.

Berdasarkan temuan penelitian, sekolah disarankan untuk menjadikan SOP sebagai dokumen resmi yang diterapkan secara berkelanjutan dalam pengelolaan jaringan. Selain itu, pelatihan dan sosialisasi rutin perlu dilakukan agar seluruh prosedur dalam SOP dapat dipahami dan dijalankan dengan benar saat terjadi insiden. Evaluasi dan pembaruan SOP sebaiknya dilakukan secara berkala untuk menyesuaikan dengan perkembangan teknologi dan jenis ancaman jaringan yang terus berubah. Penelitian selanjutnya dapat dikembangkan dengan cakupan yang

**ISSN**: 2716-0653 (Print) | 2716-0645 (Online)
**DOI**:https://doi.org/10.XXXX/eduscotech.xxxx.xxx

lebih luas, misalnya melalui pengujian SOP di beberapa sekolah sekaligus atau integrasi SOP dengan sistem manajemen keamanan informasi, sehingga hasil yang diperoleh menjadi lebih komprehensif dan aplikatif.

## DAFTAR PUSTAKA

[1] A. Aman, "Pengujian Keamanan Jaringan Nirkabel Melalui Simulasi Serangan Man In The Middle Attack di Sekolah XYZ," Digital Transformation Technology (Digitech), vol. 3, no. 2, pp. 824–831, 2023.

[2] D. A. Perkasa and B. Setiawan, "Measuring Information Security Awareness Level of High School Students," MALCOM, vol. 4, no. 4, pp. 1301–1308, 2024.

[3] A. Saraun, A. S. M. Lumenta, and D. F. Sengkey, "An Analysis of WLAN Security at the Minahasa Regency Office of Educational Affairs," Jurnal Teknik Informatika, vol. 17, no. 1, pp. 19–26, 2021.

[4] N. Dwipoyono, Khairil, and A. Sudarsono, "Penerapan Firewall pada Sistem Keamanan Jaringan Komputer di Sekolah SMK Negeri 5 Seluma," Jurnal Media Infotama, vol. 19, no. 2, pp. 454–464, 2023.

[5] Y. M. Maulana, "Model Analisis Incident Management pada Layanan Teknologi Informasi Berdasarkan Framework Information Technology Infrastructure Library V3," Jurnal Saintekom, vol. 13, no. 2, pp. 123–135, 2023.

[6] F. A. Andira, N. Hadian, and H. Hidayat, "Manajemen Insiden Customer Telkom Berbasis Service Desk Menggunakan Framework ITIL V3," Jurnal Ilmu Pengetahuan dan Teknologi Informasi (JIPTI), vol. 6, no. 1, pp. 47–60, 2025.

[7] M. K. Ilyasa and R. Bisma, "Analisis Manajemen Insiden dan Masalah Layanan IT pada Balitbang Jatim," JEISBI, vol. 3, no. 1, pp. 50–58, 2022.

[8] O. T. Brigidta, S. Mukaromah, and A. Faroqi, "Penyusunan Standar Operasional Prosedur Insiden Manajemen Menggunakan Framework ITIL Versi 3 (Studi Kasus: Dinas Koperasi dan UKM Provinsi Jawa Timur)," BRIDGE, vol. 2, no. 2, pp. 98–108, 2024.

[9] K. Aulia, S. Mukaromah, V. R. Aulia, and E. Hardiyanto, "Pengembangan SOP Manajemen Insiden TI Berdasarkan Framework ITIL V3 pada BPS Provinsi Jawa Timur," Jurnal TEKNO KOMPAK, vol. 19, no. 2, pp. 183–195, 2025.

[10] A. N. S. Permatasari and A. R. Yohannis, "Evaluation of Cybersecurity Awareness and Training for Digital Branch Frontliners at Bank XYZ," Journal of Computer Networks, Architecture and High Performance Computing, vol. 7, no. 3, pp. 672–683, 2025.

[11] F. W. Romadhon and M. Salman, "Pengembangan Skenario Serangan Siber untuk Pelatihan Tim Tanggap Insiden Siber Pemerintah Daerah Menggunakan Framework MITRE ATT&CK dan Cyber Kill Chain," Jurnal Pendidikan dan Teknologi Indonesia (JPTI), vol. 5, no. 5, pp. 1265–1279, 2025.