SOP Penanganan Insiden Keamanan Siber

Kategori: IT & Sistem

No. Dokumen: SOP-0054

Tanggal Terbit: 20/04/2026

Sumber: GajiHub SOP — sop.gajihub.com

Panduan terstruktur untuk mendeteksi, merespons, dan memulihkan insiden keamanan siber secara cepat dan efektif di lingkungan perusahaan.

Tujuan

SOP ini bertujuan untuk memberikan pedoman yang sistematis dan terstandarisasi dalam menangani insiden keamanan siber di lingkungan perusahaan. Dengan adanya SOP ini, perusahaan diharapkan mampu merespons insiden secara cepat, tepat, dan terkoordinasi sehingga dampak kerugian dapat diminimalkan. Selain itu, SOP ini juga bertujuan untuk memastikan kepatuhan terhadap peraturan perundang-undangan di Indonesia terkait perlindungan data dan keamanan sistem elektronik, serta meningkatkan kesiapan organisasi dalam menghadapi ancaman siber yang semakin kompleks.

Ruang Lingkup

SOP ini berlaku untuk seluruh unit kerja di perusahaan yang menggunakan, mengelola, atau memiliki akses terhadap sistem informasi dan data elektronik. Ruang lingkup mencakup seluruh jenis insiden keamanan siber, termasuk namun tidak terbatas pada peretasan, malware, phishing, kebocoran data, serangan DDoS, dan penyalahgunaan akses internal. SOP ini juga mencakup proses identifikasi, pelaporan, analisis, mitigasi, pemulihan, hingga evaluasi pasca-insiden, serta melibatkan seluruh karyawan, tim IT, manajemen, dan pihak ketiga yang terkait.

Definisi

Istilah	Definisi
Insiden Keamanan Siber	Peristiwa yang mengancam kerahasiaan, integritas, atau ketersediaan sistem informasi dan data perusahaan.
Tim Respons Insiden	Tim yang ditunjuk oleh perusahaan untuk menangani dan merespons insiden keamanan siber.
Malware	Perangkat lunak berbahaya yang dirancang untuk merusak, mengganggu, atau memperoleh akses tidak sah ke sistem.

Istilah	Definisi
Data Pribadi	Setiap data tentang individu yang teridentifikasi atau dapat diidentifikasi secara langsung maupun tidak langsung.
Forensik Digital	Proses pengumpulan dan analisis bukti digital untuk investigasi insiden keamanan.

Tanggung Jawab

Pihak	Tanggung Jawab
Manajemen Puncak	Menyetujui kebijakan keamanan siber, menyediakan sumber daya, dan memastikan kepatuhan terhadap regulasi.
Tim IT/Keamanan Informasi	Melakukan deteksi, analisis, mitigasi, dan pemulihan insiden serta menjaga keamanan sistem.
Karyawan	Melaporkan indikasi insiden keamanan siber dan mematuhi kebijakan keamanan perusahaan.
Tim Legal dan Kepatuhan	Memastikan penanganan insiden sesuai dengan hukum dan regulasi yang berlaku di Indonesia.
Vendor/Pihak Ketiga	Mendukung proses penanganan insiden sesuai dengan perjanjian kerja sama dan standar keamanan.

Prosedur

Tahap 1: Identifikasi dan Deteksi Insiden

Tahap awal untuk mengenali adanya potensi atau kejadian insiden keamanan siber melalui sistem monitoring maupun laporan pengguna.

1. Melakukan pemantauan sistem secara real-time menggunakan tools keamanan seperti SIEM atau antivirus.
2. Menerima dan mencatat laporan dari karyawan atau pengguna terkait aktivitas mencurigakan.
3. Mengidentifikasi indikator kompromi seperti akses tidak sah, lonjakan trafik, atau perubahan sistem yang tidak wajar.

Penanggung Jawab: Tim IT/Keamanan Informasi

Tahap 2: Pelaporan dan Eskalasi

Tahap pelaporan insiden kepada pihak terkait dan eskalasi sesuai tingkat keparahan insiden.

1. Mencatat detail insiden dalam form laporan insiden secara lengkap dan akurat.
2. Mengklasifikasikan tingkat keparahan insiden berdasarkan dampak dan urgensi.
3. Melaporkan insiden kepada manajemen dan tim terkait sesuai jalur komunikasi yang telah ditetapkan.

Penanggung Jawab: Tim IT dan Karyawan Pelapor

Tahap 3: Analisis dan Investigasi

Tahap untuk menganalisis penyebab insiden dan mengumpulkan bukti digital untuk keperluan investigasi.

1. Melakukan analisis forensik terhadap sistem yang terdampak untuk menemukan sumber serangan.
2. Mengumpulkan dan mengamankan bukti digital tanpa merusak integritas data.
3. Mengidentifikasi kerentanan yang dimanfaatkan oleh pelaku dan dampak yang ditimbulkan.

Penanggung Jawab: Tim IT/Forensik Digital

Tahap 4: Penanganan dan Mitigasi

Tahap untuk menghentikan insiden dan mencegah penyebaran dampak lebih lanjut.

1. Mengisolasi sistem yang terdampak dari jaringan untuk mencegah penyebaran.
2. Menghapus malware atau akses tidak sah dari sistem.
3. Melakukan patching atau perbaikan pada celah keamanan yang ditemukan.

Penanggung Jawab: Tim IT/Keamanan Informasi

Tahap 5: Pemulihan Sistem

Tahap untuk mengembalikan sistem ke kondisi normal dan memastikan operasional berjalan kembali.

1. Melakukan pemulihan data dari backup yang aman dan terbaru.
2. Memastikan sistem telah bersih dari ancaman sebelum diaktifkan kembali.
3. Melakukan pengujian sistem untuk memastikan tidak ada gangguan lanjutan.

Penanggung Jawab: Tim IT

Tahap 6: Evaluasi dan Pelaporan Akhir

Tahap evaluasi pasca-insiden untuk meningkatkan sistem dan mencegah kejadian serupa.

1. Menyusun laporan akhir insiden yang mencakup kronologi, dampak, dan tindakan yang diambil.
2. Melakukan evaluasi terhadap efektivitas respons dan prosedur yang digunakan.
3. Menyusun rekomendasi perbaikan dan melakukan sosialisasi kepada seluruh pihak terkait.

Penanggung Jawab: Tim IT dan Manajemen

Dokumen Terkait

- Form Laporan Insiden Keamanan Siber
- Kebijakan Keamanan Informasi Perusahaan
- Dokumen Backup dan Recovery Data
- Matriks Klasifikasi Insiden
- Checklist Audit Keamanan IT

Referensi

- Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi
- Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik
- Peraturan Menteri Kominfo No. 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik
- ISO/IEC 27001:2013 Sistem Manajemen Keamanan Informasi
- NIST Cybersecurity Framework