SOP Pelaporan Insiden Keamanan

Kategori: IT & Sistem

No. Dokumen: SOP-0168

Tanggal Terbit: 11/06/2026

Sumber: GajiHub SOP — sop.gajihub.com

Panduan terstruktur untuk mengidentifikasi, melaporkan, dan menindaklanjuti insiden keamanan secara cepat, akurat, dan terdokumentasi di lingkungan perusahaan.

Tujuan

SOP ini bertujuan untuk memastikan setiap insiden keamanan yang terjadi di lingkungan perusahaan dapat diidentifikasi, dilaporkan, ditangani, dan didokumentasikan secara sistematis, cepat, dan akurat. Dengan adanya prosedur ini, perusahaan dapat meminimalkan dampak negatif terhadap operasional, menjaga kerahasiaan, integritas, dan ketersediaan informasi, serta memenuhi kewajiban kepatuhan terhadap regulasi yang berlaku di Indonesia. SOP ini juga dirancang untuk meningkatkan kesadaran karyawan terhadap pentingnya keamanan serta memastikan adanya jalur komunikasi yang jelas dalam penanganan insiden.

Ruang Lingkup

SOP ini berlaku untuk seluruh karyawan, kontraktor, dan pihak ketiga yang memiliki akses terhadap sistem, jaringan, data, maupun fasilitas perusahaan. Ruang lingkup mencakup semua jenis insiden keamanan, termasuk namun tidak terbatas pada pelanggaran data, akses tidak sah, serangan siber, kehilangan perangkat, kebocoran informasi, dan ancaman fisik terhadap aset perusahaan. SOP ini mencakup seluruh tahapan mulai dari identifikasi insiden, pelaporan awal, eskalasi, investigasi, hingga penutupan dan evaluasi insiden.

Definisi

Istilah	Definisi
Insiden Keamanan	Setiap kejadian yang berpotensi atau telah mengganggu kerahasiaan, integritas, atau ketersediaan informasi dan sistem perusahaan.
Pelapor	Individu yang pertama kali menemukan atau mengetahui adanya insiden keamanan dan bertanggung jawab untuk melaporkannya.

Istilah	Definisi
Tim Keamanan Informasi	Tim yang bertanggung jawab atas pengelolaan, analisis, dan penanganan insiden keamanan di perusahaan.
Eskalasi	Proses peningkatan penanganan insiden kepada pihak yang memiliki kewenangan lebih tinggi sesuai tingkat keparahan insiden.
Root Cause Analysis	Proses identifikasi penyebab utama terjadinya insiden untuk mencegah kejadian serupa di masa depan.

Tanggung Jawab

Pihak	Tanggung Jawab
Seluruh Karyawan	Melaporkan setiap indikasi insiden keamanan secara segera sesuai prosedur yang ditetapkan dan menjaga kerahasiaan informasi.
Atasan Langsung	Memastikan laporan insiden diteruskan ke tim terkait dan memberikan dukungan awal dalam penanganan.
Tim Keamanan Informasi	Menerima, memverifikasi, menganalisis, dan menangani insiden serta melakukan dokumentasi dan pelaporan lanjutan.
Manajemen	Mengambil keputusan strategis terkait insiden besar serta memastikan kepatuhan terhadap regulasi dan kebijakan perusahaan.
Tim IT Support	Memberikan dukungan teknis dalam isolasi, pemulihan, dan investigasi sistem yang terdampak.

Prosedur

Tahap 1: Identifikasi Insiden Keamanan

Tahap awal untuk mengenali adanya potensi atau kejadian insiden keamanan melalui pengamatan langsung, sistem monitoring, atau laporan pihak ketiga.

1. Mengidentifikasi tanda-tanda insiden seperti aktivitas tidak biasa, akses ilegal, atau kehilangan data.
2. Mengumpulkan informasi awal seperti waktu kejadian, lokasi, sistem yang terdampak, dan kronologi singkat.
3. Menjaga kondisi sistem atau lokasi agar tidak terjadi perubahan yang dapat menghilangkan bukti penting.

Penanggung Jawab: Seluruh Karyawan dan Tim IT

Tahap 2: Pelaporan Awal Insiden

Tahap pelaporan insiden kepada pihak yang berwenang untuk memastikan respons cepat dan tepat.

1. Melaporkan insiden kepada atasan langsung atau tim keamanan informasi maksimal 1 jam setelah ditemukan.
2. Mengisi formulir pelaporan insiden secara lengkap dan akurat.
3. Mengirimkan bukti pendukung seperti screenshot, log, atau dokumentasi lainnya.

Penanggung Jawab: Pelapor

Tahap 3: Klasifikasi dan Eskalasi Insiden

Menentukan tingkat keparahan insiden dan melakukan eskalasi sesuai dengan dampak yang ditimbulkan.

1. Mengklasifikasikan insiden berdasarkan tingkat risiko (rendah, sedang, tinggi, kritis).
2. Menentukan prioritas penanganan berdasarkan dampak terhadap operasional bisnis.
3. Melakukan eskalasi kepada manajemen atau pihak eksternal jika diperlukan.

Penanggung Jawab: Tim Keamanan Informasi

Tahap 4: Penanganan dan Investigasi Insiden

Melakukan tindakan untuk mengendalikan, mengisolasi, dan menyelesaikan insiden serta mengidentifikasi penyebab utama.

1. Mengisolasi sistem atau area yang terdampak untuk mencegah penyebaran.
2. Melakukan analisis forensik dan pengumpulan bukti.
3. Menentukan akar penyebab insiden melalui root cause analysis.

Penanggung Jawab: Tim Keamanan Informasi dan IT Support

Tahap 5: Pemulihan dan Penutupan Insiden

Memastikan sistem kembali normal dan insiden ditutup dengan dokumentasi lengkap serta tindakan pencegahan.

1. Melakukan pemulihan sistem dan memastikan tidak ada ancaman lanjutan.
2. Mengkomunikasikan status penyelesaian kepada pihak terkait.
3. Menutup insiden secara resmi setelah verifikasi selesai.

Penanggung Jawab: Tim IT dan Tim Keamanan Informasi

Tahap 6: Evaluasi dan Pencegahan

Melakukan evaluasi pasca insiden untuk meningkatkan sistem keamanan dan mencegah kejadian serupa.

1. Melakukan rapat evaluasi dengan pihak terkait.
2. Menyusun rekomendasi perbaikan kebijakan dan sistem.
3. Melakukan sosialisasi dan pelatihan kepada karyawan terkait hasil evaluasi.

Penanggung Jawab: Manajemen dan Tim Keamanan Informasi

Dokumen Terkait

- Form Laporan Insiden Keamanan
- Matriks Risiko dan Dampak Insiden
- Kebijakan Keamanan Informasi Perusahaan
- Panduan Manajemen Akses Sistem
- Checklist Audit Keamanan Internal

Referensi

- Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE)
- Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik
- ISO/IEC 27001:2022 tentang Sistem Manajemen Keamanan Informasi
- Peraturan Menteri Komunikasi dan Informatika No. 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik
- NIST Cybersecurity Framework