

SOP Keamanan Kantor

Kategori: K3 (Keselamatan)

No. Dokumen: SOP-0118

Tanggal Terbit: 24/04/2026

Sumber: GajiHub SOP — sop.gajihub.com

Prosedur standar untuk memastikan keamanan lingkungan kantor, meliputi pengendalian akses, pengawasan, dan penanganan keadaan darurat.

Tujuan

SOP ini disusun untuk memastikan terciptanya lingkungan kerja yang aman, tertib, dan terlindungi dari berbagai potensi ancaman baik internal maupun eksternal. Tujuan utama dari SOP ini adalah memberikan panduan yang jelas dan sistematis terkait pengamanan fisik kantor, perlindungan aset perusahaan, serta keselamatan seluruh karyawan dan tamu. Dengan adanya SOP ini, diharapkan seluruh pihak yang terlibat dapat menjalankan tugasnya secara terkoordinasi dan sesuai standar yang berlaku, sehingga meminimalisir risiko kehilangan, kerusakan, maupun gangguan keamanan lainnya di lingkungan kerja.

Ruang Lingkup

SOP ini berlaku untuk seluruh area kantor perusahaan, termasuk area kerja, ruang server, ruang arsip, area parkir, dan fasilitas pendukung lainnya. SOP ini mencakup pengaturan akses masuk dan keluar, pengawasan aktivitas di lingkungan kantor, pengamanan aset dan dokumen penting, serta penanganan keadaan darurat seperti kebakaran, pencurian, dan gangguan keamanan lainnya. Seluruh karyawan, petugas keamanan (security), tamu, serta pihak ketiga yang berada di lingkungan kantor wajib mematuhi prosedur yang telah ditetapkan dalam SOP ini.

Definisi

Istilah	Definisi
Keamanan Kantor	Serangkaian upaya dan tindakan yang dilakukan untuk melindungi lingkungan kerja dari ancaman yang dapat mengganggu operasional perusahaan.
Petugas Keamanan (Security)	Personel yang ditunjuk oleh perusahaan untuk menjaga dan mengawasi keamanan di lingkungan kantor.
Kontrol Akses	Sistem atau prosedur yang digunakan untuk mengatur siapa saja yang diperbolehkan masuk atau keluar dari area tertentu.

Istilah	Definisi
Tamu	Individu dari luar perusahaan yang memasuki area kantor untuk kepentingan tertentu dan harus mendapatkan izin.
Keadaan Darurat	Situasi yang mengancam keselamatan manusia atau aset perusahaan yang memerlukan tindakan segera.

Tanggung Jawab

Pihak	Tanggung Jawab
Manajemen Perusahaan	Menetapkan kebijakan keamanan, menyediakan sumber daya, serta melakukan evaluasi terhadap efektivitas SOP keamanan kantor.
Petugas Keamanan	Melaksanakan pengawasan, patroli, pengendalian akses, serta penanganan awal terhadap insiden keamanan.
Karyawan	Mematuhi seluruh prosedur keamanan, menjaga barang pribadi dan aset perusahaan, serta melaporkan kejadian mencurigakan.
HRD/GA	Mengelola administrasi keamanan, termasuk kartu akses, data karyawan, serta koordinasi dengan vendor keamanan.

Prosedur

Tahap 1: Pengendalian Akses Masuk dan Keluar

Tahap ini bertujuan untuk memastikan bahwa hanya pihak yang berwenang yang dapat memasuki area kantor.

1. Setiap karyawan wajib menggunakan kartu identitas atau akses (ID Card) saat memasuki dan berada di area kantor.
2. Tamu wajib melapor ke resepsionis atau petugas keamanan untuk registrasi dan mendapatkan kartu tamu.
3. Petugas keamanan melakukan verifikasi identitas dan tujuan kunjungan sebelum memberikan izin masuk.
4. Akses ke area terbatas seperti ruang server atau arsip hanya diberikan kepada pihak yang memiliki otorisasi khusus.
5. Setiap aktivitas keluar masuk dicatat dalam sistem atau buku log keamanan.

Penanggung Jawab: Petugas Keamanan dan Resepsionis

Tahap 2: Patroli dan Pengawasan Area

Patroli dilakukan secara rutin untuk memastikan kondisi keamanan di seluruh area kantor tetap terjaga.

1. Petugas keamanan melakukan patroli secara berkala sesuai jadwal yang telah ditentukan.
2. Seluruh area diperiksa, termasuk pintu, jendela, ruang kerja, dan fasilitas umum.
3. Petugas mencatat hasil patroli dalam laporan harian.
4. Apabila ditemukan kejanggalan atau potensi risiko, segera dilaporkan kepada atasan.
5. Penggunaan CCTV dimonitor secara aktif untuk mendukung pengawasan.

Penanggung Jawab: Petugas Keamanan

Tahap 3: Pengamanan Aset dan Dokumen

Tahap ini bertujuan untuk melindungi aset fisik dan informasi perusahaan dari kehilangan atau penyalahgunaan.

1. Seluruh aset perusahaan harus terdata dan diberi label identifikasi.
2. Dokumen penting disimpan di tempat yang aman seperti lemari terkunci atau ruang arsip khusus.
3. Akses terhadap dokumen sensitif dibatasi hanya untuk pihak yang berwenang.
4. Karyawan dilarang membawa keluar aset perusahaan tanpa izin resmi.
5. Dilakukan audit aset secara berkala untuk memastikan keberadaan dan kondisi aset.

Penanggung Jawab: HRD/GA dan Karyawan

Tahap 4: Penanganan Keadaan Darurat

Prosedur ini mengatur langkah-langkah yang harus diambil dalam situasi darurat untuk meminimalkan dampak kerugian.

1. Petugas keamanan segera mengidentifikasi jenis keadaan darurat yang terjadi.
2. Aktifkan alarm atau sistem peringatan jika diperlukan.
3. Evakuasi karyawan sesuai jalur evakuasi yang telah ditentukan.
4. Hubungi pihak berwenang seperti pemadam kebakaran atau kepolisian jika diperlukan.
5. Buat laporan kejadian setelah situasi terkendali.

Penanggung Jawab: Petugas Keamanan dan Tim Tanggap Darurat

Tahap 5: Pelaporan dan Evaluasi Keamanan

Tahap ini bertujuan untuk memastikan adanya perbaikan berkelanjutan terhadap sistem keamanan kantor.

1. Setiap insiden keamanan harus dilaporkan secara tertulis kepada manajemen.
2. Dilakukan evaluasi berkala terhadap sistem dan prosedur keamanan.
3. Manajemen memberikan rekomendasi perbaikan berdasarkan hasil evaluasi.
4. Pelatihan keamanan diberikan kepada karyawan secara berkala.

5. Dokumentasi seluruh laporan dan evaluasi disimpan dengan baik untuk keperluan audit.

Penanggung Jawab: Manajemen dan HRD/GA

Dokumen Terkait

- Formulir Registrasi Tamu
- Laporan Patroli Keamanan
- Daftar Inventaris Aset
- Laporan Insiden Keamanan
- Checklist Inspeksi Keamanan

Referensi

- Undang-Undang No. 1 Tahun 1970 tentang Keselamatan Kerja
- Peraturan Menteri Tenaga Kerja No. PER.04/MEN/1987 tentang Panitia Pembina K3
- Peraturan Kapolri No. 24 Tahun 2007 tentang Sistem Manajemen Pengamanan Organisasi, Perusahaan dan/atau Instansi
- ISO 45001:2018 Sistem Manajemen Kesehatan dan Keselamatan Kerja
- ISO 27001:2022 Sistem Manajemen Keamanan Informasi