

# SOP Keamanan Data dan Informasi Perusahaan

Kategori: IT & Sistem

No. Dokumen: SOP-0051

Tanggal Terbit: 20/04/2026

Sumber: GajiHub SOP — [sop.gajihub.com](https://sop.gajihub.com)

*Pedoman terstruktur untuk melindungi data dan informasi perusahaan dari risiko kebocoran, penyalahgunaan, dan ancaman siber.*

## Tujuan

SOP ini bertujuan untuk menetapkan standar dan prosedur yang jelas dalam melindungi data dan informasi perusahaan dari berbagai ancaman, baik internal maupun eksternal. Dengan adanya SOP ini, perusahaan diharapkan mampu menjaga kerahasiaan, integritas, dan ketersediaan data (CIA triad), serta meminimalkan risiko kebocoran data, serangan siber, dan penyalahgunaan informasi. Selain itu, SOP ini juga bertujuan untuk memastikan kepatuhan terhadap peraturan perundang-undangan yang berlaku di Indonesia, termasuk Undang-Undang Perlindungan Data Pribadi, serta meningkatkan kesadaran dan tanggung jawab seluruh karyawan dalam menjaga keamanan informasi perusahaan.

## Ruang Lingkup

SOP ini berlaku untuk seluruh karyawan, manajemen, kontraktor, serta pihak ketiga yang memiliki akses terhadap sistem, jaringan, dan data perusahaan. Ruang lingkup mencakup seluruh jenis data, baik dalam bentuk digital maupun fisik, termasuk data pelanggan, data karyawan, data keuangan, serta informasi strategis perusahaan. SOP ini juga mencakup pengelolaan perangkat keras, perangkat lunak, jaringan, serta sistem informasi yang digunakan dalam operasional perusahaan, termasuk penggunaan perangkat pribadi (BYOD) dan akses jarak jauh. Penerapan SOP ini berlaku di seluruh lokasi operasional perusahaan tanpa pengecualian.

## Definisi

Istilah	Definisi
Data Sensitif	Data yang bersifat rahasia dan memiliki risiko tinggi apabila bocor, seperti data pribadi, data keuangan, dan informasi strategis perusahaan.
Keamanan Informasi	Upaya melindungi informasi dari akses tidak sah, penggunaan, pengungkapan, gangguan, modifikasi, atau penghancuran.

Istilah	Definisi
Akses Kontrol	Mekanisme pembatasan akses terhadap sistem atau data hanya kepada pihak yang berwenang.
Insiden Keamanan	Setiap kejadian yang mengancam kerahasiaan, integritas, atau ketersediaan informasi.
Backup Data	Proses pencadangan data untuk menghindari kehilangan data akibat kerusakan atau serangan.

## Tanggung Jawab

Pihak	Tanggung Jawab
Direksi	Menetapkan kebijakan keamanan informasi dan memastikan implementasi SOP berjalan secara efektif di seluruh perusahaan.
Departemen IT	Mengelola sistem keamanan, melakukan monitoring, serta menangani insiden keamanan informasi.
Seluruh Karyawan	Mematuhi kebijakan keamanan data dan menjaga kerahasiaan informasi yang diakses dalam pekerjaan.
Tim Keamanan Informasi	Melakukan audit, evaluasi risiko, serta pengembangan sistem keamanan informasi secara berkelanjutan.

## Prosedur

### Tahap 1: Klasifikasi dan Identifikasi Data

Tahap ini bertujuan untuk mengidentifikasi dan mengklasifikasikan data berdasarkan tingkat sensitivitas dan risiko guna menentukan perlakuan keamanan yang sesuai.

- Mengidentifikasi seluruh jenis data yang dimiliki perusahaan, termasuk data pelanggan, karyawan, keuangan, dan operasional.
- Mengklasifikasikan data menjadi kategori seperti publik, internal, rahasia, dan sangat rahasia.
- Menetapkan label dan kebijakan perlindungan sesuai dengan klasifikasi data yang telah ditentukan.

**Penanggung Jawab:** Departemen IT dan Tim Keamanan Informasi

### Tahap 2: Pengendalian Akses dan Otentikasi

Tahap ini mengatur mekanisme pemberian dan pengelolaan akses terhadap sistem dan data agar hanya dapat digunakan oleh pihak yang berwenang.

1. Menerapkan sistem autentikasi seperti password kuat, multi-factor authentication (MFA), dan manajemen identitas pengguna.
2. Memberikan akses berdasarkan prinsip least privilege sesuai kebutuhan pekerjaan.
3. Melakukan review dan audit akses secara berkala untuk memastikan tidak ada akses yang tidak sah.

**Penanggung Jawab:** Departemen IT

### **Tahap 3: Perlindungan Sistem dan Infrastruktur**

Tahap ini berfokus pada pengamanan perangkat keras, perangkat lunak, dan jaringan perusahaan dari ancaman siber dan kerusakan.

1. Menginstal dan memperbarui antivirus, firewall, serta sistem keamanan lainnya secara berkala.
2. Melakukan patching dan update sistem operasi serta aplikasi secara rutin.
3. Mengamankan jaringan dengan enkripsi, VPN, dan segmentasi jaringan untuk membatasi akses.

**Penanggung Jawab:** Departemen IT

### **Tahap 4: Pengelolaan Backup dan Pemulihan Data**

Tahap ini memastikan bahwa data perusahaan dapat dipulihkan dengan cepat jika terjadi kehilangan, kerusakan, atau serangan.

1. Melakukan backup data secara berkala sesuai dengan kebijakan yang ditetapkan (harian, mingguan, bulanan).
2. Menyimpan backup di lokasi yang aman, termasuk penyimpanan offsite atau cloud.
3. Melakukan uji pemulihan data secara berkala untuk memastikan keandalan sistem backup.

**Penanggung Jawab:** Departemen IT

### **Tahap 5: Penanganan Insiden Keamanan Informasi**

Tahap ini mengatur langkah-langkah yang harus dilakukan ketika terjadi insiden keamanan untuk meminimalkan dampak dan mencegah kejadian berulang.

1. Mengidentifikasi dan melaporkan insiden keamanan kepada tim terkait secara segera.
2. Melakukan investigasi dan mitigasi untuk mengendalikan dampak insiden.
3. Menyusun laporan insiden dan melakukan evaluasi untuk perbaikan sistem keamanan.

**Penanggung Jawab:** Tim Keamanan Informasi dan Departemen IT

### **Tahap 6: Pelatihan dan Kesadaran Keamanan Informasi**

Tahap ini bertujuan untuk meningkatkan kesadaran dan pemahaman seluruh karyawan terhadap pentingnya keamanan data.

1. Menyelenggarakan pelatihan keamanan informasi secara berkala untuk seluruh karyawan.

2. Memberikan sosialisasi terkait ancaman siber seperti phishing, malware, dan social engineering.
3. Melakukan evaluasi pemahaman karyawan melalui tes atau simulasi keamanan.

**Penanggung Jawab:** Departemen HR dan IT

## Dokumen Terkait

- Kebijakan Keamanan Informasi Perusahaan
- Form Klasifikasi dan Inventaris Data
- Form Laporan Insiden Keamanan
- Kebijakan Penggunaan Sistem IT
- Prosedur Backup dan Recovery Data

## Referensi

- Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi
- Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) beserta perubahannya
- Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik
- ISO/IEC 27001:2013 tentang Sistem Manajemen Keamanan Informasi
- Peraturan Menteri Kominfo terkait perlindungan data dan keamanan informasi