

# SOP Pengelolaan Penyimpanan Rekaman CCTV

**Kategori:** IT & Sistem

**No. Dokumen:** SOP-0176

**Tanggal Terbit:** 11/06/2026

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

*Pedoman standar untuk pengelolaan, penyimpanan, dan pengamanan rekaman CCTV agar sesuai regulasi dan menjaga integritas data perusahaan.*

## Tujuan

SOP ini disusun untuk memberikan panduan yang jelas, sistematis, dan terstandarisasi dalam pengelolaan penyimpanan rekaman CCTV di lingkungan perusahaan. Tujuannya adalah untuk memastikan bahwa seluruh rekaman CCTV disimpan dengan aman, terstruktur, mudah diakses oleh pihak berwenang, serta terlindungi dari kehilangan, kerusakan, atau penyalahgunaan. Selain itu, SOP ini juga bertujuan untuk memastikan kepatuhan terhadap peraturan perundang-undangan yang berlaku di Indonesia, khususnya terkait perlindungan data pribadi dan keamanan informasi.

## Ruang Lingkup

SOP ini berlaku untuk seluruh aktivitas yang berkaitan dengan pengelolaan penyimpanan rekaman CCTV di perusahaan, termasuk proses perekaman, penyimpanan, pengarsipan, pemeliharaan, hingga penghapusan data rekaman. Ruang lingkup mencakup seluruh perangkat CCTV, server penyimpanan, media backup, serta personel yang memiliki akses terhadap sistem CCTV. SOP ini juga berlaku bagi seluruh unit kerja yang menggunakan atau membutuhkan akses terhadap rekaman CCTV untuk kepentingan operasional, keamanan, maupun investigasi internal.

## Definisi

Istilah	Definisi
CCTV	Closed Circuit Television, yaitu sistem kamera pengawas yang digunakan untuk memantau aktivitas di area tertentu.
Rekaman CCTV	Data video hasil perekaman dari perangkat CCTV yang disimpan dalam media digital.
Server Penyimpanan	Perangkat keras atau sistem yang digunakan untuk menyimpan rekaman CCTV secara terpusat.

Istilah	Definisi
Retensi Data	Jangka waktu penyimpanan data sebelum dilakukan penghapusan atau pemusnahan.
Akses Terbatas	Hak akses yang hanya diberikan kepada personel tertentu yang berwenang.

## Tanggung Jawab

Pihak	Tanggung Jawab
Manajer IT	Bertanggung jawab atas pengelolaan sistem penyimpanan CCTV secara keseluruhan serta memastikan keamanan dan ketersediaan data.
Tim IT	Melakukan instalasi, pemeliharaan, backup, dan pengelolaan teknis sistem penyimpanan CCTV.
Security Supervisor	Mengawasi penggunaan CCTV dan memastikan rekaman digunakan sesuai kebutuhan keamanan.
Manajemen	Menetapkan kebijakan terkait retensi data dan akses terhadap rekaman CCTV.
Pengguna Berwenang	Mengakses rekaman CCTV sesuai izin dan menjaga kerahasiaan data.

## Prosedur

### Tahap 1: Pengaturan Sistem Penyimpanan

Tahap ini mencakup konfigurasi awal sistem penyimpanan untuk memastikan data CCTV tersimpan dengan aman dan terstruktur.

- Menentukan kapasitas penyimpanan sesuai kebutuhan operasional dan jumlah kamera CCTV.
- Mengatur server atau perangkat penyimpanan dengan sistem redundansi untuk menghindari kehilangan data.
- Mengkonfigurasi format penyimpanan dan kualitas rekaman sesuai standar perusahaan.

**Penanggung Jawab:** Tim IT

### Tahap 2: Pengelolaan Rekaman Harian

Proses pengelolaan rekaman yang dilakukan secara rutin setiap hari untuk memastikan rekaman tersimpan dengan baik.

- Memastikan seluruh kamera berfungsi dan merekam sesuai jadwal.

2. Melakukan pengecekan kapasitas penyimpanan secara berkala.
3. Mencatat log aktivitas sistem dan kejadian penting yang terekam.

**Penanggung Jawab:** Security Supervisor

### **Tahap 3: Pengamanan dan Akses Data**

Menjamin bahwa hanya pihak yang berwenang yang dapat mengakses rekaman CCTV.

1. Menetapkan hak akses berdasarkan peran dan tanggung jawab.
2. Menggunakan sistem autentikasi seperti username dan password yang kuat.
3. Mencatat setiap aktivitas akses dan pengunduhan rekaman.

**Penanggung Jawab:** Manajer IT

### **Tahap 4: Backup dan Retensi Data**

Tahap ini memastikan data rekaman CCTV memiliki cadangan dan disimpan sesuai kebijakan retensi.

1. Melakukan backup data secara berkala ke media penyimpanan eksternal atau cloud.
2. Menentukan periode retensi data sesuai kebijakan perusahaan (misalnya 30-90 hari).
3. Melakukan penghapusan otomatis atau manual terhadap data yang sudah melewati masa retensi.

**Penanggung Jawab:** Tim IT

### **Tahap 5: Pemeliharaan dan Audit Sistem**

Melakukan pemeliharaan rutin dan audit untuk memastikan sistem berjalan optimal.

1. Melakukan pengecekan perangkat keras dan perangkat lunak secara berkala.
2. Melakukan audit akses dan penggunaan rekaman CCTV.
3. Menyusun laporan hasil audit dan rekomendasi perbaikan.

**Penanggung Jawab:** Manajer IT

### **Tahap 6: Penghapusan dan Pemusnahan Data**

Tahap akhir dalam siklus pengelolaan data untuk memastikan data yang tidak diperlukan dihapus dengan aman.

1. Mengidentifikasi data yang telah melewati masa retensi.
2. Melakukan penghapusan data menggunakan metode yang aman.
3. Mendokumentasikan proses penghapusan sebagai bukti kepatuhan.

**Penanggung Jawab:** Tim IT

- Kebijakan Keamanan Informasi Perusahaan
- Kebijakan Perlindungan Data Pribadi
- Manual Sistem CCTV
- Prosedur Penanganan Insiden Keamanan

## Referensi

- Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi
- Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) beserta perubahannya
- Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik
- ISO/IEC 27001 tentang Sistem Manajemen Keamanan Informasi