SOP Backup dan Recovery Data

Kategori: IT & Sistem

No. Dokumen: SOP-0052

Tanggal Terbit: 20/04/2026

Sumber: GajiHub SOP — sop.gajihub.com

Prosedur standar untuk memastikan pencadangan dan pemulihan data perusahaan dilakukan secara aman, terjadwal, dan sesuai regulasi.

Tujuan

SOP ini bertujuan untuk memastikan seluruh data perusahaan terlindungi melalui proses pencadangan (backup) yang terstruktur dan pemulihan (recovery) yang efektif apabila terjadi kehilangan data, kerusakan sistem, atau bencana. Dengan adanya SOP ini, perusahaan dapat meminimalkan risiko kehilangan data penting, menjaga kelangsungan operasional bisnis, serta memastikan kepatuhan terhadap regulasi perlindungan data yang berlaku di Indonesia. SOP ini juga menjadi acuan bagi tim IT dalam menjalankan tugas secara konsisten, terdokumentasi, dan dapat diaudit.

Ruang Lingkup

SOP ini berlaku untuk seluruh sistem informasi, aplikasi, database, serta data penting yang dimiliki dan dikelola oleh perusahaan, baik yang berada di lingkungan on-premise maupun cloud. Ruang lingkup mencakup proses identifikasi data kritis, penjadwalan backup, pelaksanaan backup, penyimpanan media backup, pengujian pemulihan data, serta tindakan recovery dalam kondisi darurat. SOP ini juga mencakup seluruh karyawan yang memiliki akses terhadap data dan sistem, terutama tim IT, manajemen, serta pihak ketiga yang terlibat dalam pengelolaan infrastruktur teknologi.

Definisi

Istilah	Definisi
Backup Data	Proses membuat salinan data dari sistem utama untuk disimpan di lokasi lain sebagai cadangan.
Recovery Data	Proses pemulihan data dari media backup ketika data utama hilang, rusak, atau tidak dapat diakses.
Disaster Recovery	Strategi dan prosedur untuk memulihkan sistem IT dan data setelah terjadi gangguan besar atau bencana.

Istilah	Definisi
Media Backup	Perangkat atau layanan yang digunakan untuk menyimpan data cadangan seperti hard drive eksternal, tape, atau cloud storage.
RPO (Recovery Point Objective)	Batas maksimal kehilangan data yang dapat diterima dalam satuan waktu.
RTO (Recovery Time Objective)	Waktu maksimum yang dibutuhkan untuk memulihkan sistem setelah gangguan.

Tanggung Jawab

Pihak	Tanggung Jawab
Manajer IT	Menetapkan kebijakan backup dan recovery, menyetujui jadwal backup, serta memastikan kepatuhan terhadap SOP.
Tim IT Infrastruktur	Melaksanakan proses backup dan recovery sesuai prosedur serta memastikan keamanan dan integritas data.
Administrator Sistem	Mengelola konfigurasi sistem backup, melakukan monitoring, serta melakukan pengujian recovery secara berkala.
Karyawan Pengguna Sistem	Menyimpan data pada lokasi yang telah ditentukan dan tidak melakukan tindakan yang dapat mengganggu proses backup.
Vendor/Penyedia Layanan Cloud	Menyediakan layanan penyimpanan backup yang aman, andal, dan sesuai dengan SLA yang disepakati.

Prosedur

Tahap 1: Identifikasi dan Klasifikasi Data

Tahap ini bertujuan untuk menentukan data mana yang perlu dibackup berdasarkan tingkat kepentingannya terhadap operasional perusahaan.

1. Melakukan inventarisasi seluruh data dan sistem yang digunakan dalam perusahaan.
2. Mengklasifikasikan data berdasarkan tingkat kritikalitas (tinggi, sedang, rendah).
3. Menentukan prioritas backup berdasarkan kebutuhan bisnis dan risiko kehilangan data.

Penanggung Jawab: Manajer IT dan Administrator Sistem

Tahap 2: Perencanaan dan Penjadwalan Backup

Tahap ini mencakup penyusunan strategi backup termasuk metode, frekuensi, dan media yang digunakan.

1. Menentukan jenis backup (full, incremental, differential) sesuai kebutuhan.
2. Menyusun jadwal backup harian, mingguan, dan bulanan.
3. Menentukan lokasi penyimpanan backup baik onsite maupun offsite/cloud.

Penanggung Jawab: Manajer IT

Tahap 3: Pelaksanaan Backup Data

Tahap ini merupakan pelaksanaan proses backup sesuai dengan jadwal dan metode yang telah ditentukan.

1. Menjalankan proses backup secara otomatis atau manual sesuai jadwal.
2. Memastikan proses backup selesai tanpa error melalui monitoring sistem.
3. Mencatat hasil backup dalam log aktivitas backup.

Penanggung Jawab: Tim IT Infrastruktur

Tahap 4: Penyimpanan dan Pengamanan Backup

Tahap ini memastikan bahwa data backup disimpan dengan aman dan terlindungi dari akses tidak sah atau kerusakan.

1. Menyimpan backup di lokasi terpisah dari sistem utama (offsite/cloud).
2. Melakukan enkripsi data backup untuk menjaga kerahasiaan.
3. Mengatur hak akses terhadap media backup hanya untuk personel yang berwenang.

Penanggung Jawab: Administrator Sistem

Tahap 5: Pengujian Recovery Data

Tahap ini bertujuan untuk memastikan bahwa data backup dapat dipulihkan dengan baik ketika dibutuhkan.

1. Melakukan simulasi recovery secara berkala minimal setiap 3 bulan.
2. Menguji integritas dan kelengkapan data hasil recovery.
3. Mendokumentasikan hasil pengujian dan melakukan perbaikan jika ditemukan kendala.

Penanggung Jawab: Tim IT Infrastruktur

Tahap 6: Pelaksanaan Recovery Data

Tahap ini dilakukan ketika terjadi insiden kehilangan data atau gangguan sistem yang membutuhkan pemulihan.

1. Mengidentifikasi penyebab dan ruang lingkup kehilangan data.
2. Menentukan titik pemulihan (restore point) sesuai RPO.
3. Melakukan proses recovery dan memastikan sistem kembali normal sesuai RTO.

Penanggung Jawab: Administrator Sistem dan Manajer IT

Dokumen Terkait

- Kebijakan Keamanan Informasi Perusahaan
- Rencana Disaster Recovery (DRP)
- Standar Operasional IT Infrastruktur
- Formulir Permintaan Backup dan Recovery
- Log Aktivitas Sistem

Referensi

- Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi
- ISO/IEC 27001:2022 tentang Sistem Manajemen Keamanan Informasi
- Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik
- Peraturan Menteri Kominfo No. 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik