SOP Manajemen Password dan Hak Akses

Kategori: IT & Sistem

No. Dokumen: SOP-0053

Tanggal Terbit: 20/04/2026

Sumber: GajiHub SOP — sop.gajihub.com

Panduan pengelolaan password dan hak akses sistem untuk menjaga keamanan informasi dan mencegah akses tidak sah di lingkungan perusahaan.

Tujuan

SOP ini disusun untuk memastikan pengelolaan password dan hak akses terhadap sistem informasi perusahaan dilakukan secara aman, terkontrol, dan terdokumentasi dengan baik. Tujuan utama dari SOP ini adalah untuk melindungi data dan sistem dari akses tidak sah, mencegah kebocoran informasi, serta memastikan bahwa setiap pengguna hanya memiliki akses sesuai dengan peran dan tanggung jawabnya. Selain itu, SOP ini juga bertujuan untuk mendukung kepatuhan terhadap regulasi yang berlaku di Indonesia serta standar praktik terbaik dalam keamanan informasi, seperti ISO/IEC 27001. Dengan adanya SOP ini, perusahaan dapat meminimalkan risiko keamanan dan meningkatkan akuntabilitas dalam pengelolaan akses sistem.

Ruang Lingkup

SOP ini berlaku untuk seluruh karyawan, kontraktor, vendor, dan pihak ketiga lainnya yang memiliki akses ke sistem informasi perusahaan, baik secara internal maupun eksternal. Ruang lingkup mencakup seluruh sistem teknologi informasi, termasuk aplikasi bisnis, jaringan, database, perangkat keras, serta layanan berbasis cloud yang digunakan oleh perusahaan. SOP ini mengatur proses pembuatan, penggunaan, perubahan, dan penghapusan password serta pemberian, perubahan, dan pencabutan hak akses. Selain itu, SOP ini juga mencakup pengelolaan akun pengguna, audit akses, serta penanganan insiden terkait keamanan akses. Seluruh unit kerja wajib mematuhi prosedur ini tanpa pengecualian.

Definisi

Istilah	Definisi
Password	Kata sandi rahasia yang digunakan oleh pengguna untuk mengakses sistem atau aplikasi tertentu.
Hak Akses	Izin yang diberikan kepada pengguna untuk mengakses, melihat, atau memodifikasi data dan sistem tertentu sesuai dengan perannya.

Istilah	Definisi
User ID	Identitas unik yang digunakan untuk mengidentifikasi pengguna dalam suatu sistem.
Multi-Factor Authentication (MFA)	Metode autentikasi yang menggunakan lebih dari satu faktor verifikasi untuk meningkatkan keamanan akses.
Least Privilege	Prinsip pemberian hak akses minimum yang diperlukan pengguna untuk menjalankan tugasnya.

Tanggung Jawab

Pihak	Tanggung Jawab
Tim IT/Security	Mengelola sistem akses, membuat kebijakan keamanan, melakukan monitoring, serta memastikan implementasi SOP berjalan dengan baik.
Atasan Langsung	Menyetujui permintaan hak akses sesuai kebutuhan pekerjaan karyawan.
Pengguna/Karyawan	Menjaga kerahasiaan password dan menggunakan hak akses sesuai ketentuan yang berlaku.
Audit Internal	Melakukan audit berkala terhadap penggunaan hak akses dan kepatuhan terhadap SOP.

Prosedur

Tahap 1: Pembuatan dan Pengelolaan Akun Pengguna

Tahap ini mengatur proses pembuatan akun pengguna baru serta pengelolaannya selama siklus hidup karyawan atau pengguna dalam organisasi.

1. Pengguna baru diajukan oleh HR atau atasan langsung melalui formulir permintaan akses resmi.
2. Tim IT melakukan verifikasi data dan membuat User ID unik untuk setiap pengguna.
3. Hak akses awal diberikan berdasarkan peran kerja dengan prinsip least privilege.
4. Pengguna menerima kredensial awal dan diwajibkan mengganti password pada login pertama.

Penanggung Jawab: Tim IT

Tahap 2: Kebijakan Password

Tahap ini mengatur standar keamanan password yang harus dipatuhi oleh seluruh pengguna untuk menjaga keamanan sistem.

1. Password harus terdiri dari minimal 8 karakter dengan kombinasi huruf besar, huruf kecil, angka, dan simbol.
2. Password wajib diganti secara berkala minimal setiap 90 hari.
3. Pengguna dilarang menggunakan password yang sama dengan akun pribadi atau sebelumnya.
4. Sistem harus menerapkan mekanisme penguncian akun setelah 5 kali percobaan login gagal.

Penanggung Jawab: Tim IT/Security

Tahap 3: Pemberian dan Perubahan Hak Akses

Tahap ini mengatur proses pemberian akses baru serta perubahan hak akses akibat perubahan peran atau kebutuhan pekerjaan.

1. Permintaan akses diajukan melalui sistem atau formulir resmi dan disetujui oleh atasan langsung.
2. Tim IT melakukan evaluasi kebutuhan akses berdasarkan prinsip least privilege.
3. Hak akses diberikan sesuai persetujuan dan dicatat dalam sistem manajemen akses.
4. Perubahan akses harus didokumentasikan dan diverifikasi ulang oleh pihak terkait.

Penanggung Jawab: Tim IT dan Atasan Langsung

Tahap 4: Pemantauan dan Audit Akses

Tahap ini bertujuan untuk memastikan bahwa penggunaan hak akses sesuai dengan kebijakan dan tidak terjadi penyalahgunaan.

1. Tim IT melakukan monitoring aktivitas login dan penggunaan sistem secara berkala.
2. Audit akses dilakukan minimal setiap 6 bulan oleh tim audit internal.
3. Hak akses yang tidak lagi relevan harus segera dicabut atau disesuaikan.
4. Setiap anomali atau aktivitas mencurigakan harus dilaporkan dan ditindaklanjuti.

Penanggung Jawab: Tim IT dan Audit Internal

Tahap 5: Penonaktifan dan Penghapusan Akses

Tahap ini mengatur pencabutan akses bagi pengguna yang sudah tidak memiliki hubungan kerja atau tidak lagi membutuhkan akses.

1. HR menginformasikan kepada tim IT terkait karyawan yang resign atau berpindah posisi.
2. Tim IT segera menonaktifkan akun pengguna maksimal 1x24 jam setelah pemberitahuan.
3. Seluruh akses ke sistem, email, dan aplikasi dicabut secara menyeluruh.
4. Data pengguna diarsipkan sesuai kebijakan retensi data perusahaan.

Penanggung Jawab: Tim IT dan HR

Tahap 6: Penanganan Insiden Keamanan Akses

Tahap ini mengatur langkah-langkah yang harus dilakukan jika terjadi pelanggaran atau insiden terkait keamanan password dan hak akses.

1. Pengguna wajib segera melaporkan dugaan kebocoran password atau akses tidak sah kepada tim IT.
2. Tim IT melakukan investigasi dan mengamankan akun yang terdampak.
3. Password di-reset dan akses ditinjau ulang untuk mencegah kejadian berulang.
4. Insiden didokumentasikan dan dilaporkan kepada manajemen untuk evaluasi lebih lanjut.

Penanggung Jawab: Tim IT/Security

Dokumen Terkait

- Kebijakan Keamanan Informasi Perusahaan
- Form Permintaan dan Perubahan Hak Akses
- Form Offboarding dan Onboarding Karyawan
- Checklist Audit Sistem Informasi
- Laporan Insiden Keamanan IT

Referensi

- ISO/IEC 27001:2022 - Information Security Management Systems
- Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik
- UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi
- Peraturan Menteri Kominfo No. 5 Tahun 2020 tentang Penyelenggara Sistem Elektronik
- NIST Cybersecurity Framework

Template ini dihasilkan oleh GajiHub SOP (sop.gajihub.com) — © 2026 PT Kledo Berhati Nyaman