



IngatGuru
IngatIKIP Siliwangi

STANDARD OPERATING PROCEDURE KEAMANAN SISTEM & KONTROL AKSES



**BAGIAN
PENGEMBANGAN IT**

INSTITUT KEGURUAN DAN ILMU PENDIDIKAN
(IKIP) SILIWANGI



it.ikipsiliwangi.ac.id

INSTITUT KEGURUAN DAN ILMU PENDIDIKAN (IKIP) SILIWANGI
STANDARD OPERATING PROCEDURE
KEAMANAN SISTEM & KONTROL AKSES

Kode Dokumen	Versi	Tanggal Berlaku	Disusun Oleh	Disetujui Oleh
SOP-SD-010	1.0	November 2025 – November 2030	Bag. Pengembangan IT	Wakil Rektor Bidang SDM

TUJUAN

Menetapkan prosedur standar dalam pengelolaan keamanan sistem serta pengaturan hak akses pengguna guna mencegah kebocoran data, akses tidak sah, dan pelanggaran keamanan sistem.

RUANG LINGKUP

SOP ini berlaku untuk semua sistem aplikasi yang dikelola oleh tim IT, baik frontend, backend, mobile, database, DevOps, maupun sistem internal perusahaan.

DEFINISI

- **Akses Role-Based:** Pengaturan hak akses berdasarkan peran pengguna (misalnya admin, user, staf).
- **Audit Log:** Catatan digital yang merekam seluruh aktivitas pengguna dalam sistem.
- **Credential:** Informasi autentikasi berupa username, password, API key, token, dll.

PENANGGUNG JAWAB

- IT Security Officer
- Backend Developer / DevOps
- Project Manager
- Admin Sistem

PROSEDUR PELAKSANAAN

Tahapan	Uraian	Penanggung Jawab
Identifikasi Role & Akses	Menentukan jenis peran pengguna dan akses yang dibutuhkan untuk tiap sistem	PM + Dev + Security

INSTITUT KEGURUAN DAN ILMU PENDIDIKAN (IKIP) SILIWANGI
STANDARD OPERATING PROCEDURE
KEAMANAN SISTEM & KONTROL AKSES

Kode Dokumen	Versi	Tanggal Berlaku	Disusun Oleh	Disetujui Oleh
SOP-SD-010	1.0	November 2025 – November 2030	Bag. Pengembangan IT	Wakil Rektor Bidang SDM

Autentikasi Pengguna	Menerapkan sistem login aman: JWT, OAuth2, token-based authentication	Backend Dev
Otorisasi Role-Based	Membatasi akses berdasarkan peran (RBAC) dalam setiap endpoint atau halaman	Backend Dev
Enkripsi Credential & API Key	Menyimpan password, token, dan key dengan hash dan enkripsi kuat (bcrypt, AES-256)	Backend / DevOps
Penggunaan .env	Semua credential dan konfigurasi rahasia disimpan di file .env atau Secret Manager	DevOps
Audit Log Aktif	Sistem mencatat aktivitas login, update data, delete, dan transaksi kritikal	Backend Dev
Pengaturan Firewall & IP Whitelist	Membatasi akses sistem internal berdasarkan IP atau port tertentu	DevOps
Two-Factor Authentication (jika perlu)	Mengaktifkan 2FA pada akun sensitif (Admin, Finance, System Access)	IT Security
Review Akses Berkala	Melakukan audit akses user minimal 1 bulan sekali	PM + IT Security
Penonaktifan Akses Tidak Aktif	Akses yang tidak digunakan lebih dari 30 hari harus dinonaktifkan	Admin Sistem

DOKUMEN TERKAIT

- Role & Access Matrix
- Audit Log Report
- Template .env.example
- Kebijakan Keamanan Data
- SOP Git & Credential Handling

INSTITUT KEGURUAN DAN ILMU PENDIDIKAN (IKIP) SILIWANGI
STANDARD OPERATING PROCEDURE
KEAMANAN SISTEM & KONTROL AKSES

Kode Dokumen	Versi	Tanggal Berlaku	Disusun Oleh	Disetujui Oleh
SOP-SD-010	1.0	November 2025 – November 2030	Bag. Pengembangan IT	Wakil Rektor Bidang SDM

PENUTUP

SOP ini merupakan dasar perlindungan sistem terhadap risiko keamanan digital. Seluruh tim IT wajib mengikuti prosedur ini dalam setiap pengembangan maupun pemeliharaan sistem agar keamanan data dan aplikasi perusahaan tetap terjaga.