



 KEMENTERIAN PENDIDIKAN TINGGI, RISET, SAINS DAN TEKNOLOGI UNIVERSITAS NUSA CENDANA UPT. TIK email : upt.tik@undana.ac.id, website : https://tik.undana.ac.id	Nomor Pos	:	07/UN15.28/TU/2026
	Tanggal Pembuatan	:	6 Januari 2026
	Tanggal revisi	:	
	Tanggal Ewektif	:	
	Disahkan oleh	:	Kepala UPT. TIK  Prof. Dr. Kalvein Rantelobo, ST.,MT NIP. 19710617 199903 1 003
	Nama SOP	:	Sistem Keamanan Informasi
Dasar Hukum		Kualifikasi Pelaksana	
1. Undang-undang Nomor 20 Tahun 2003 tentang Sistem Pendidikan Nasional 2. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor : 35 Tahun 2012 tentang Penyusunan Standart Operasional Prosedur 3. Keputusan Menteri Pendidikan , Kebudayaan, Riset dan Teknologi Nomor: 25 Tahun 2021 Tentang Organisasi dan Tata Kerja Universitas Nusa Cendana 4. Keputusan Rektor Undana Nomor 3 Tahun 2019 tentang Pedoman Penyelenggaraan Pendidikan di Universitas Nusa Cendana 5. Peraturan Pemerintah No. 82 Tahun 2012 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik 6. Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor : 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik.		1. S1 2. Mengetahui tugas dan fungsi 3. Memiliki kemampuan pada sistem keamanan jaringan dan sistem informasi	
Keterkaitan		Peralatan dan Kelengkapan	
1. SOP <i>Web filtering</i> 2. SOP Akses Data 3. SOP <i>Backup and restore</i>		1. ATK 2. Pakta integritas 3. Komputer/laptop	
Peringatan		Pencatatan dan Pendataan	
Jika SOP ini tidak dilaksanakan akan berdampak Keamanan jaringan dan sistem informasi		1. Akses log 2.	

I. Tujuan

Tujuan *Standard Operating Procedure* (SOP) Sistem Keamanan Informasi adalah

- ✚ Menjamin kerahasiaan, integritas dan ketersediaan data akademik, penelitian dan administrasi.
- ✚ Melindungi sistem informasi Undana dari ancaman internal maupun eksternal.
- ✚ Menetapkan standar keamanan sistem informasi yang konsisten bagi seluruh civitas akademika Undana.

II. Ruang Lingkup

Ruang lingkup SOP ini berlaku untuk :

- ✚ Seluruh staf baik tenaga pendidik maupun kependidikan, mahasiswa dan pihak ketiga yang mengakses sistem informasi di Undana.
- ✚ Seluruh sistem aplikasi dengan domain maupun subdomain Undana, jaringan kampus dan data penelitian.

III. Definisi

Beberapa definisi yang ada dalam SOP ini adalah :

- ✚ CIA Triad : *Confidentiality, Integrity, Availability*
- ✚ Insiden Keamanan : Segala bentuk pelanggaran atau ancaman terhadap sistem informasi Undana.
- ✚ User : Individu yang memiliki hak akses ke sistem perguruan tinggi.

IV. Tanggungjawab

Tanggungjawab dalam pelaksanaan SOP ini adalah :

- ✚ Kepala UPT. TIK bersama sub koordinator
- ✚ Team keamanan sistem informasi
- ✚ Civitas akademika melaksanakan tugas sesuai dengan SOP

V. Prosedur

Prosedur dalam pelaksanaan SOP ini sebagai berikut:

1. Pengelolaan akses

- ✚ Setiap user wajib memiliki akun baik berupa NIP, NIM, NIK ataupun email institusi
- ✚ Hak akses diberikan sesuai peran (mahasiswa, tenaga pendidik, tenaga kependidikan dan admin)
- ✚ Password wajib diperbaharui setiap 90 hari

2. Penggunaan Sistem

- + Dilarang menginstal software tidak resmi di perangkat kampus.
- + Wajib menggunakan VPN untuk akses jarak jauh
- + Jika VPN belum tersedia, maka akses jarak jauh tidak diperkenankan menggunakan jaringan publik
- + Data sensitif (nilai, penelitian, data pribadi) harus dienkripsi

3. Monitoring dan Audit

- + Log aktivitas sistem disimpan minimal 6 bulan
- + Audit keamanan dilakukan setiap semester oleh tim TIK
- + IDS/IPS digunakan untuk mendeteksi intrusi

4. Penanganan Insiden

- + Identifikasi insiden oleh *user* atau sistem monitoring
- + Pelaporan ke Helpdesk/TIM TIK
- + Analisis & Klasifikasi insiden (minor/major/critical)
- + Mitigasi (isolasi sistem, patching, restore backup)
- + Dokumentasi & Evaluasi untuk perbaikan SOP

5. Pengembangan Karier

- + Identifikasi pegawai berprestasi
- + Rekomendasi pelatihan lanjutan
- + Promosi jabatan atau rotasi kerja

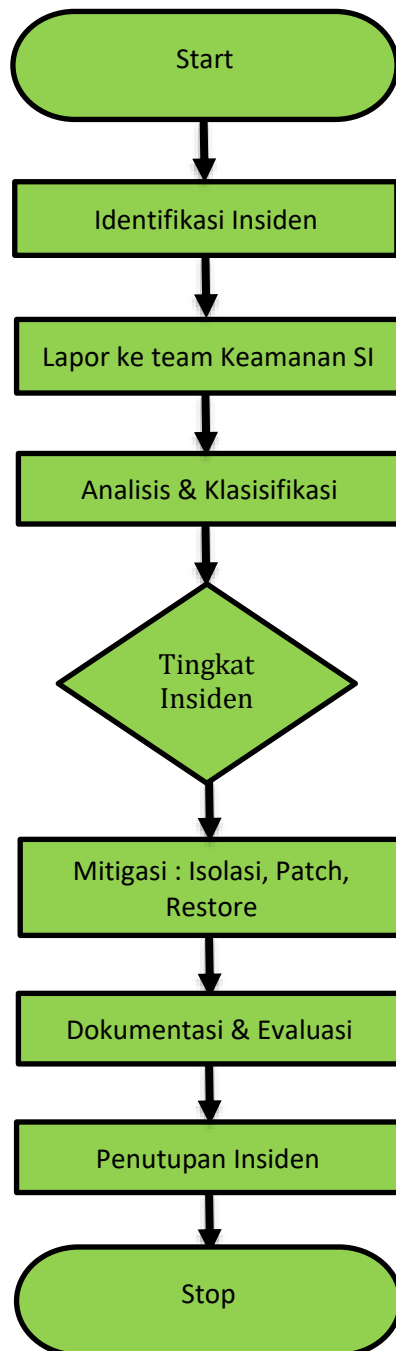
6. Backup dan Recovery

- + Backup harian (incremental) dan mingguan (full)
- + Recovery plan diuji minimal 2 kali setahun
- + Backup disimpan di lokasi berbeda (offsite/cloud)

7. Edukasi dan Pelatihan

- + Pelatihan keamanan informasi wajib diikuti seluruh staf setiap tahun
- + Sosialisasi kebijakan keamanan dilakukan pada mahasiswa baru

VI. Bagan Alur



VII. Tahapan Penanganan Insiden Keamanan Informasi

1. Identifikasi

- ✚ Insiden dikenali oleh *user* (misalnya dosen, mahasiswa, staf) atau oleh sistem monitoring
- ✚ Contoh: akses ilegal, malware, kebocoran data

2. Pelaporan

- ✚ *User* melaporkan insiden ke helpdesk/Tim TIK
- ✚ Sistem otomatis juga dapat mengirim alert ke team keamanan

3. Analisis dan Klasifikasi

Team keamanan melakukan analisis untuk menentukan tingkat insiden :

- ✚ Minor : Gangguan kecil, tidak berdampak luas
- ✚ Major : Berdampak pada sebagian sistem
- ✚ Critical : Mengancam data sensitif atau semua sistem

4. Mitigas

Tindakan cepat dilakukan :

- ✚ Minor : Perbaikan cepat (Reset password, update sistem)
- ✚ Isolasi sistem yang terdampak (Major/critical)
- ✚ Penerapan patch keamanan (Major/critical)
- ✚ *Restore backup* jika diperlukan (Major/critical)

5. Dokumentasi dan Evaluasi

- ✚ Semua langkah dicatat dalam laporan insiden
- ✚ Evaluasi dilakukan untuk memperbaiki SOP agar insiden serupa tidak terulang

6. Penutup

- ✚ Insiden dinyatakan selesai setelah mitigasi berhasil
- ✚ Sistem kembali beroperasi normal

VIII. Penutup

SOP Keamanan Sistem Informasi merupakan bagian integral dari penerapan Sistem Manajemen Keamanan Informasi berbasis ISO 27001 di Undana. SOP ini wajib dipatuhi oleh seluruh pihak terkait dan akan ditinjau secara berkala untuk memastikan kesesuaian dengan perkembangan teknologi, regulasi, dan kebutuhan institusi.