



UPT. TEKNOLOGI INFORMASI DAN KOMUNIKASI

"Menjadikan Undana sebagai kampus digital dalam menghadapi era global dengan mengedepankan keamanan sistem informasi yang bersifat confidentiality, integrity dan availability."

 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	:	34/UN15.28/TU/2026
	Tanggal Pembuatan	:	10 Februari 2026
	Tanggal revisi	:	
	Tanggal Ewektif	:	11 Februari 2025
	Disahkan oleh	:	Kepala UPT. TIK  Arfan Y. Mauko. S.T., M.Cs NIP. 198005202008121003
	Nama SOP	:	Skrining Dalam Akses Data Dari Pihak Eksternal
Dasar Hukum		Kualifikasi Pelaksana	
1. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) sebagaimana telah diubah dengan UU Nomor 19 Tahun 2016. 2. Undang-undang Nomor 12 Tahun 2012 Pendidikan Tinggi 3. Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi 4. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor : 35 Tahun 2012 tentang Penyusunan Standart Operasional Prosedur 5. Keputusan Menteri Pendidikan , Kebudayaan, Riset dan Teknologi Nomor: 25 Tahun 2021 Tentang Organisasi dan Tata Kerja Universitas Nusa Cendana 6. Keputusan Rektor Undana Nomor 3 Tahun 2019 tentang Pedoman Penyelenggaraan Pendidikan di Universitas Nusa Cendana 7. Peraturan Pemerintah No. 82 Tahun 2012 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik 8. Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor : 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik.		1. Memiliki pengetahuan dan memahami undang-undang keterbukaan informasi publik. 2. Memiliki pengetahuan tentang keamanan sistem informasi 3. Memiliki ketrampilan pengelolaan <i>firewall</i>	
Keterkaitan		Peralatan dan Kelengkapan	
1. SOP Akses Data 2. SOP <i>Acceptable Usage</i>		1. ATK 2. Komputer/Laptop 3. Jaringan internet	
Peringatan		Pencatatan dan Pendataan	
Jika SOP ini tidak dilaksanakan akan berdampak Keamanan sistem informasi		1. Surat Permohonan 2. Lampiran berkas 3. Akses log	

I. Latar Belakang

Universitas Nusa Cendana memiliki data dan mengelola data strategis yang bersifat rahasia, terbatas, dan/atau publik meliputi data akademik, keuangan, penelitian, sumber daya manusia serta sistem informasi. Akses terhadap data tersebut oleh pihak eksternal berpotensi menimbulkan risiko keamanan informasi, pelanggaran privasi, kebocoran data dan penyalahgunaan informasi apabila tidak dikendalikan secara ketat. Karena itu Universitas Nusa Cendana wajib melindungi aset informasi dari ancaman internal maupun eksternal ISO 27001 secara tegas mengatur pengendalian akses pihak ketiga (*third party access control*) yang mensyaratkan proses penilaian risiko, verifikasi identitas serta pengendalian keamanan sebelum akses diberikan. Tanpa mekanisme skrining yang ketat, Undana berisiko mengalami kebocoran data, pelanggaran hukum serta kerugian reputasi. Oleh karena itu SOP ini disusun sebagai pedoman resmi untuk melakukan skrining akses data pihak eksternal yang mencakup pemeriksaan identitas, profil dan catatan kriminalitas guna menjamin kepatuhan terhadap peraturan perundang-undangan nasional maupun standar internasional.

SOP ini mengacu pada control :

- ✚ A.15.19 – *Information security in supplier relationships*
- ✚ A.5.20 – *Addressing information security within supplier agreements*
- ✚ A.5.15 – *Access control*
- ✚ A.5.16 – *Identity management*
- ✚ A.5.17 – *Authentication Information*
- ✚ A.5.18 – *Access rights*
- ✚ A.8.2 - *Information classification*
- ✚ A.8.5 – *Secure information transfer*

II. Tujuan

SOP ini bertujuan untuk:

- ✚ Mengimplemetasikan kontrol keamanan akses pihak eksternal sesuai ISO 27001:2022
- ✚ Menjamin hanya pihak eksternal sah, terpercaya dan berisiko rendah yang dapat mengakses data Universitas Nusa Cendana
- ✚ Melindungi kerahasiaan, integritas dan ketersediaan data Universitas Nusa Cendana

- ✚ Memenuhi kewajiban hukum terkait perlindungan data dan keamanan informasi
- ✚ Menjadi acuan bagi seluruh uni kerja di Universitas Nusa Cendana dalam pengelolaan akses data eksternal

III. Ruang Lingkup

SOP ini berlaku untuk

- ✚ Seluruh permohonan akses data oleh pihak eksternal
- ✚ Seluruh jenis data Universitas Nusa Cendana (publik, internal, terbatas dan rahasia)
- ✚ Seluruh sistem informasi, jaringan dan aplikasi yang dikelola Universitas Nusa Cendana
- ✚ Seluruh unit kerja yang terlibat dalam proses persetujuan dan pengolahan akses data

IV. Definisi

Beberapa definisi yang ada dalam SOP ini adalah :

- ✚ Pihak eksternal: Individu atau badan hukum diluar struktur organisasi Undana yang memerlukan akses data
- ✚ Skrining akses: Proses pemeriksaan administratif, hukum dan keamanan informasi sebelum pemberian akses data
- ✚ Identitas: Dokumen resmi yang membuktikan jadi diri pihak eksternal (KTP, Paspor, Akta Perusahaan)
- ✚ Profil pihak eksternal: Informasi latar belakang,, tujuan akses, afiliasi institusi, dan rekam jejak profesional
- ✚ Catatan kriminalitas: Dokumen resmi berupa SKCK atau surat pernyataan bebas tindak pidana
- ✚ Aset informasi: Data, sistem, aplikasi dan infrastruktur TI milik Undana

V. Penanggungjawab

Penanggungjawab dalam pelaksanaan SOP ini adalah :

- ✚ Wakil Rektor Bidang Perencanaan, Kerjasama dan Sistem Informasi
- ✚ Kepala UPT. TIK
- ✚ Administrator jaringan dan web server
- ✚ Unit Pengelola Data

VI. Prosedur

Prosedur dalam pelaksanaan SOP ini sebagai berikut:

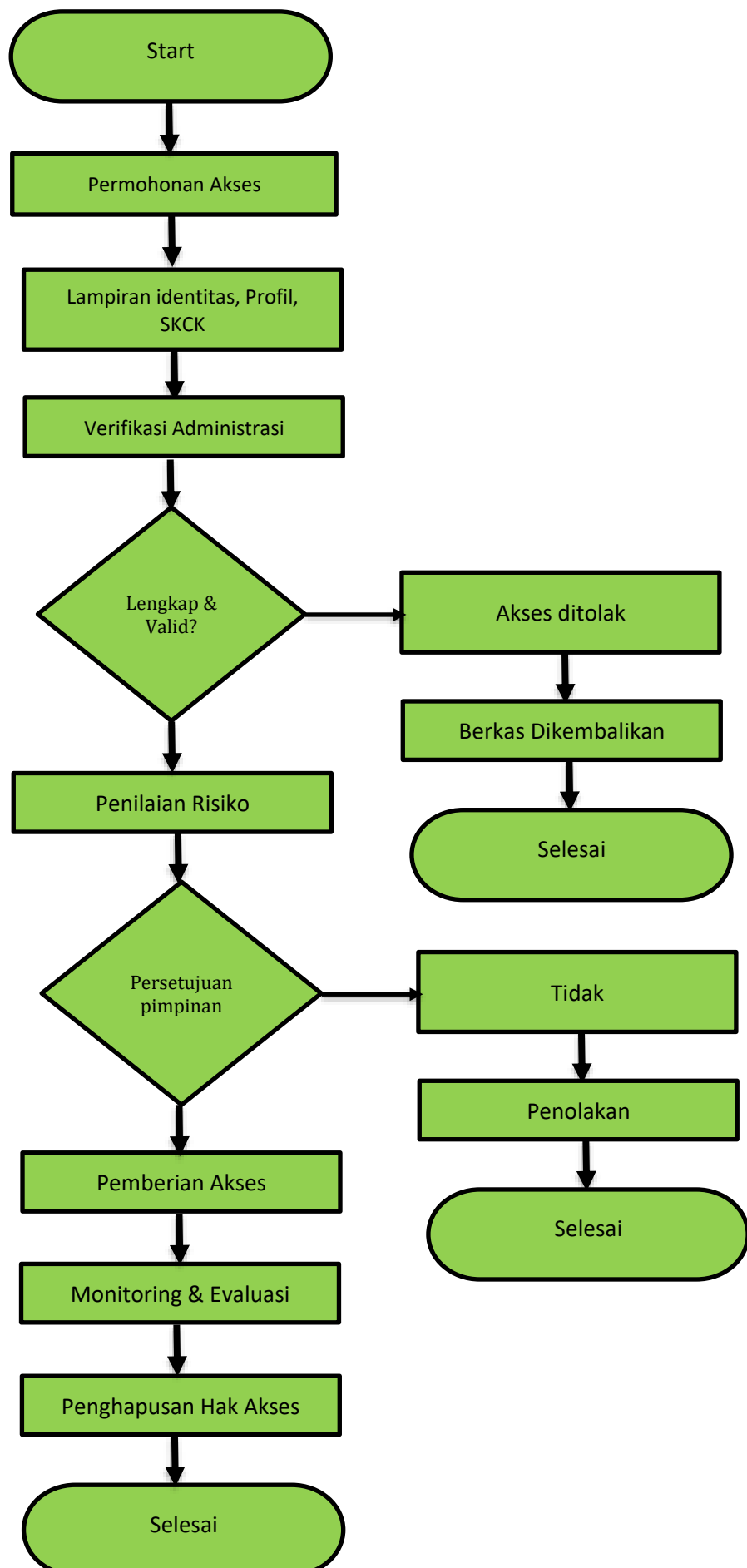
1. Pengajuan Permohonan Akses

- ✚ Pihak eksternal mengajukan permohonan tertulis kepada unit pengelola data
- ✚ Permohonan wajib melampirkan :

- ✓ Surat permohonan resmi
 - ✓ Identitas diri atau badan hukum
 - ✓ Profil lengkap
 - ✓ Dokumen kerjasama atau surat tugas
 - ✓ SKCK yang masih berlaku
 - ✓ Surat pernyataan kepatuhan keamanan informasi
 - ✓ Kesediaan menandatangani *Non-Disclosure Agreement* (NDA)
2. Verifikasi Administrasi
- ✚ Unit pengelola data melakukan verifikasi keabsahan dan kelengkapan dokumen
 - ✚ Dokumen yang tidak lengkap atau tidak valid dikembalikan
3. Penilaian Profil dan Risiko Keamanan
- ✚ Tim keamanan informasi melakukan
 - ✓ Penilaian tujuan dan urgensi akses
 - ✓ Klasifikasi data yang diminta
 - ✓ Analisis risiko berdasarkan profil dan catatan kriminalitas
 - ✚ Risiko ditetapkan sebagai :
 - ✓ Rendah
 - ✓ Sedang
 - ✓ Tinggi
 - ✚ Seluruh keputusan didokumentasikan
4. Pemberian dan Pengendalian Akses
- ✚ Unit pengolah data memberikan akses sesuai prinsip least privilege
 - ✚ Akses bersifat
 - ✓ Terbatas
 - ✓ Sementara
 - ✓ Diawasi dan dicatat (log aktivitas). Log aktivitas disimpan selama 1 tahun
 - ✚ Pihak eksternal wajib menandatangani NDA dan perjanjian keamanan data
5. Pemantauan dan Pencabutan Akses
- ✚ Aktivitas akses dimonitor secara berkala
 - ✚ Akses dicabut apabila
 - ✓ Masa akses berakhir
 - ✓ Terjadi pelanggaran
 - ✓ Kerjasama dihentikan

- ✚ Hak akses akan dicabut jika tidak digunakan dalam 24 jam
- ✚ Evaluasi akhir didokumentasikan

VII. Bagan Alur



VIII. Penutup

SOP Skrining Dalam Akses Data Dari Pihak Eksternal ini 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.