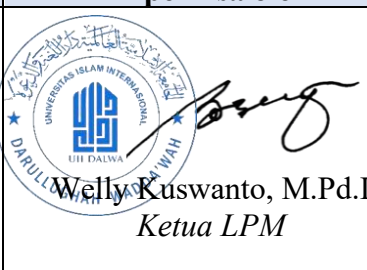


STANDAR OPERASIONAL PROSEDUR (SOP)

KEAMANAN DATA DAN INFORMASI BERBASIS TEKNOLOGI INFORMASI DAN KOMUNIKASI (TIK)

Kode Dokumen	20/SOP/LPM/TIK/25	No. Revisi : 01
Tanggal Berlaku	15/05/2027	Jumlah Halaman : 03

Disusun oleh	Diperiksa oleh	Disahkan oleh
 Novianto Puji Raharjo, M.I.Kom. <i>Kepala Unit TIK</i>	 Welly Kuswanto, M.Pd.I <i>Ketua LPM</i>	 Kuzairi, M.Pd. <i>Ketua BAAK</i>

I. Tujuan

Standar Operasional Prosedur (SOP) ini disusun sebagai pedoman bagi seluruh unit kerja di lingkungan Universitas Islam Internasional Darullughah Wadda'wah dalam menjaga keamanan, kerahasiaan, integritas, dan ketersediaan data serta informasi akademik dan non-akademik yang dikelola melalui sistem berbasis Teknologi Informasi dan Komunikasi (TIK), guna mendukung tata kelola pendidikan yang akuntabel dan memenuhi ketentuan perundang-undangan yang berlaku, termasuk untuk kebutuhan pelaporan dan akreditasi program studi.

II. Ruang lingkup

SOP ini berlaku untuk seluruh proses pengelolaan data dan informasi yang mencakup:

- Data akademik (KRS, KHS, nilai, presensi, kurikulum, capaian pembelajaran);
- Data kepegawaian dosen dan tenaga kependidikan;
- Data kemahasiswaan dan alumni;
- Data keuangan dan aset yang terhubung dengan sistem informasi terintegrasi;
- Infrastruktur jaringan, server, dan aplikasi pendukung layanan akademik.

III. Definisi

1. Keamanan Data: Kondisi terjaganya data dari akses, perubahan, pengungkapan, atau penghapusan yang tidak sah.
2. Hak Akses Berjenjang (Role-Based Access Control): Pengaturan kewenangan akses sistem berdasarkan peran pengguna (mahasiswa, dosen, operator, pimpinan).

3. Audit Trail: Catatan sistem yang merekam setiap aktivitas perubahan data, termasuk pelaku, waktu, dan jenis perubahan.
4. Backup Data: Proses pencadangan data secara berkala untuk memastikan ketersediaan data apabila terjadi kehilangan atau kerusakan.
5. Insiden Keamanan Data: Kejadian yang mengancam atau menyebabkan pelanggaran terhadap kerahasiaan, integritas, atau ketersediaan data.

IV. Kebijakan Umum

1. Setiap pengguna sistem informasi wajib memiliki akun resmi dengan otentikasi yang terenkripsi dan tidak boleh dibagikan kepada pihak lain.
2. Hak akses terhadap data ditetapkan sesuai peran dan kewenangan masing-masing pengguna (role-based access control).
3. Seluruh aktivitas perubahan data pada sistem harus tercatat secara otomatis dalam log audit (audit trail) yang tidak dapat diubah oleh pengguna biasa.
4. Data akademik wajib diverifikasi secara berjenjang sebelum dinyatakan final pada setiap akhir semester.
5. Pencadangan data (backup) dilakukan secara berkala sesuai jadwal yang ditetapkan oleh Unit TIK dan disimpan pada media/lokasi terpisah dari server utama.
6. Setiap insiden keamanan data wajib dilaporkan dan ditangani sesuai prosedur tanggap insiden dalam waktu paling lambat 1x24 jam sejak diketahui.
7. Evaluasi terhadap efektivitas kebijakan keamanan data dilakukan secara berkala minimal 1 (satu) kali per semester

V. Prosedur Keamanan Data Dan Informasi Berbasis Teknologi Informasi Dan Komunikasi

Pengelolaan akun dan hak akses

1. Unit TIK menerbitkan akun resmi bagi setiap dosen, tenaga kependidikan, dan mahasiswa baru berdasarkan data yang diverifikasi oleh bagian akademik/kepegawaian.
2. Setiap akun diberikan hak akses sesuai peran (mahasiswa, dosen, operator prodi, pimpinan) yang ditinjau ulang setiap awal semester
3. Akun yang tidak lagi aktif (mahasiswa lulus/mengundurkan diri, pegawai purna tugas) dinonaktifkan oleh Unit TIK paling lambat 7 hari kerja setelah menerima pemberitahuan resmi.
4. Verifikasi dan Validasi Data Akademik
5. Dosen menginput nilai dan presensi melalui sistem informasi akademik sesuai jadwal yang ditetapkan.
6. Operator akademik prodi melakukan verifikasi kelengkapan dan konsistensi data yang diinput.
7. Ketua Program Studi melakukan validasi akhir sebelum data dikunci pada sistem menjelang penutupan semester.
8. Data yang telah dikunci hanya dapat diubah melalui mekanisme koreksi resmi yang tercatat dalam log audit dan disetujui oleh Ketua Program Studi.

Pencadangan (Backup) dan Pemulihan Data

1. Unit TIK melaksanakan pencadangan data secara mingguan sesuai jadwal yang ditetapkan dalam kalender operasional TIK.
2. Hasil pencadangan disimpan pada server cadangan yang terpisah secara fisik/logis dari server utama.
3. Unit TIK melakukan uji pemulihan data (restore test) secara berkala minimal 1 semester untuk memastikan data cadangan dapat digunakan.
4. Hasil uji pemulihan didokumentasikan dalam laporan internal Unit TIK.

Penanganan Insiden Keamanan Data

1. Pengguna yang menemukan indikasi insiden keamanan data (kebocoran, akses tidak sah, kerusakan sistem) wajib segera melapor kepada Unit TIK melalui kanal resmi TIK UII Dalwa.
2. Unit TIK melakukan identifikasi awal, isolasi sumber masalah, dan mitigasi dampak dalam waktu paling lambat 1x24 jam.
3. Unit TIK menyampaikan laporan insiden kepada pimpinan UPPS disertai rencana tindak lanjut.
4. Evaluasi pasca-insiden dilakukan untuk memperbaiki prosedur dan mencegah kejadian serupa terulang.

Monitoring dan Evaluasi

1. Unit TIK melakukan pemantauan rutin terhadap kinerja sistem, termasuk tingkat ketersediaan (uptime) dan potensi kerentanan keamanan.
2. Lembaga Penjaminan Mutu (LPM) melakukan audit mutu internal terhadap tata kelola data dan informasi minimal 1 kali per semester.
3. Hasil monitoring dan audit dilaporkan kepada pimpinan sebagai bahan evaluasi dan perbaikan berkelanjutan kebijakan keamanan data.

VI. PIHAK TERKAIT DAN TANGGUNG JAWAB

Pihak	Tanggung Jawab
Unit TIK	Mengelola infrastruktur, keamanan sistem, backup data, dan penanganan insiden teknis.
Operator Akademik Prodi	Melakukan verifikasi awal data akademik yang diinput dosen.
Ketua Program Studi	Melakukan validasi akhir data akademik sebelum dikunci setiap semester.
Lembaga Penjaminan Mutu (LPM)	Melakukan audit mutu internal terhadap tata kelola data dan keamanan informasi.
Pimpinan UPPS	Mengambil keputusan strategis berdasarkan hasil monitoring, evaluasi, dan laporan insiden.

VII. REFERENSI

- Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi;
- Peraturan Menteri Pendidikan, Kebudayaan, Riset, dan Teknologi tentang Pangkalan Data Pendidikan Tinggi;

- Statuta Perguruan Tinggi dengan nomor surat SK. 230321/UII.O85/REK/03/2023
- Pedoman Sistem Penjaminan Mutu Internal (SPMI) Universitas Islam Internasional Darullughah Wadda'wah Pasuruan.