

DOKUMEN

SISTEM INFORMASI ADMINISTRASI PERGURUAN TINGGI

Dokumen perlindungan dan pencadangan data



**Universitas Islam Internasional
Darullughah Wadda'wah**

Unit Pengelola Program Studi (UPPS)

Pasuruan, November 2025

KEBIJAKAN DAN PROSEDUR PERLINDUNGAN DAN PENCADANGAN DATA AKADEMIK

PROGRAM STUDI SEJARAH PERADABAN ISLAM

Keterangan	Isian
Nomor dokumen	547B/102/78/DALWA/UII/XI/25
Versi / revisi	1 (Satu)
Tanggal berlaku	Juli 2027
Disusun oleh	Lembaga Penjaminan Mutu Universitas Islam Internasional Darullughah Wadda'wah

Kebijakan dan Prosedur Perlindungan dan Pencadangan Data Akademik

Program Studi Sejarah Peradaban Islam

Halaman Pengesahan

Keterangan	Isian
Judul dokumen	Kebijakan dan Prosedur Perlindungan dan Pencadangan Data Akademik
Unit pengelola	PTIPD UII DALWA
Ditetapkan melalui	SK Rektor Nomor: 575A/65/98/DALWA/UII/V/2025
Berlaku sejak	7 Oktober 2027
Penanggung jawab	Muhammad Fahmi Ali Fikri, S.I.Kom.
Pengawas mutu	Novianto Puji Raharjo, M.I.Kom.

BAB I. PENDAHULUAN

1.1 Latar Belakang

Data akademik, yaitu data mahasiswa, nilai, kurikulum, dosen, dan arsip kelulusan, adalah aset yang tidak tergantikan bagi UPPS. Kehilangan, kerusakan, atau kebocoran data dapat menghentikan layanan akademik, merugikan mahasiswa, dan melanggar ketentuan perlindungan data pribadi. Dokumen ini menetapkan kebijakan dan prosedur untuk melindungi data tersebut dan memulihkannya apabila terjadi gangguan.

1.2 Tujuan

1. Menjaga kerahasiaan, keutuhan, dan ketersediaan data akademik.
2. Menjamin data dapat dipulihkan dalam batas waktu dan kehilangan data yang dapat diterima.
3. Menetapkan tanggung jawab yang jelas dalam perlindungan, pencadangan, dan pemulihan data.
4. Memenuhi ketentuan peraturan perundang-undangan tentang perlindungan data pribadi dan keamanan informasi.

1.3 Ruang Lingkup

Kebijakan berlaku untuk seluruh sistem dan data yang dikelola atau digunakan UPPS, meliputi sistem informasi akademik, platform pembelajaran daring, repositori, situs web, basis data kepegawaian dan dosen, serta berkas arsip digital, baik di server lokal maupun layanan *cloud*, dan berlaku bagi seluruh pengelola dan pengguna dengan hak akses.

BAB II. LANDASAN HUKUM DAN ACUAN

1. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.
2. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahannya.
3. Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik.
4. Undang-Undang Nomor 12 Tahun 2012 tentang Pendidikan Tinggi.
5. Peraturan tentang penyelenggaraan sistem dan transaksi elektronik serta keamanan informasi yang berlaku.
6. Ketentuan Kementerian Agama tentang pengelolaan data dan sistem informasi: [isi: nomor dan tahun].
7. Acuan praktik: standar manajemen keamanan informasi (misalnya keluarga ISO/IEC 27001) sebagai pedoman, bukan sebagai klaim sertifikasi.
8. Statuta dan SK internal

Seluruh rujukan perlu dicek ulang terhadap versi terbaru sebelum dilampirkan.

BAB III. ISTILAH DAN KLASIFIKASI DATA

3.1 Istilah

- **RPO (*Recovery Point Objective*)**: batas maksimum kehilangan data yang dapat diterima, diukur dalam waktu.
- **RTO (*Recovery Time Objective*)**: batas waktu maksimum untuk memulihkan layanan setelah gangguan.
- **Cadangan penuh (*full*)**: salinan seluruh data. **Cadangan inkremental**: salinan data yang berubah sejak cadangan terakhir.
- **Data pribadi**: data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi.

3.2 Klasifikasi Data

Kelas	Contoh Data	Perlakuan Minimum
Rahasia	Data pribadi mahasiswa dan dosen, nilai individual, kata sandi (tersimpan terenkripsi/hash), kunci enkripsi	Akses terbatas, enkripsi saat disimpan dan dikirim, log akses
Internal	Notulen rapat, laporan mutu internal, SOP, draf dokumen	Akses berbasis peran, dicadangkan
Publik	Profil prodi, kurikulum, daftar dosen, kalender akademik	Dijaga keutuhannya, dicadangkan, dipublikasikan sesuai Daftar Informasi Publik
Arsip permanen	Transkrip, data kelulusan, ijazah dan SK yudisium	Retensi permanen, cadangan terpisah, dijaga keutuhan

BAB IV. ORGANISASI DAN TANGGUNG JAWAB

Peran	Tanggung Jawab
Pimpinan UPPS	Menetapkan kebijakan, menyediakan sumber daya, menyetujui rencana pemulihan
Kepala UPT TIK/Pusat Data	Mengoperasikan sistem, pencadangan, pemulihan, dan keamanan infrastruktur
Administrator sistem	Menjalankan dan memantau pencadangan harian, mengelola hak akses, mencatat log
Pemilik data (Ketua Prodi, bagian akademik, bagian kepegawaian)	Menentukan klasifikasi dan kebutuhan retensi data, memverifikasi hasil pemulihan
Petugas pelindungan data pribadi	Memantau kepatuhan pelindungan data pribadi dan menangani permintaan subjek data
Ketua LPM/UPM	Mengaudit kepatuhan dan menindaklanjuti temuan
Seluruh pengguna	Mematuhi kebijakan, menjaga kerahasiaan akun, melaporkan insiden

BAB V. KEBIJAKAN PERLINDUNGAN DATA

5.1 Pengendalian Akses

1. Setiap pengguna memiliki akun individual. Akun bersama tidak diperbolehkan.
2. Hak akses diberikan berdasarkan peran dan prinsip kebutuhan minimum (*least privilege*).
3. Permintaan, perubahan, dan pencabutan hak akses dicatat dan disetujui pemilik data.

4. Hak akses ditinjau setiap semester. Akun pengguna yang sudah tidak bertugas dinonaktifkan paling lambat 3 hari kerja.
5. Kata sandi paling sedikit 12 karakter, tidak dipakai ulang di layanan lain, dan diganti bila diduga bocor. Autentikasi dua faktor diwajibkan bagi akun administrator.

5.2 Perlindungan Teknis

1. **Enkripsi.** Data kelas Rahasia dienkripsi saat disimpan dan saat dikirim (HTTPS/TLS). Kunci enkripsi disimpan terpisah dari data.
2. **Jaringan.** *Firewall* aktif, port yang tidak diperlukan ditutup, dan akses administrasi jarak jauh dibatasi serta tercatat.
3. **Pembaruan.** Pembaruan keamanan sistem operasi, aplikasi, dan basis data dipasang paling lambat 30 hari setelah tersedia. Pembaruan kritis dipasang lebih cepat.
4. **Perlindungan terhadap perangkat lunak berbahaya.** Perangkat server dan komputer pengelola dilengkapi perlindungan antivirus atau EDR yang diperbarui.
5. **Log dan pemantauan.** Aktivitas masuk (*login*), perubahan nilai, dan perubahan hak akses dicatat dan disimpan minimal 12 bulan. Log ditinjau berkala.
6. **Pemisahan lingkungan.** Lingkungan uji dan produksi dipisahkan. Data pribadi nyata tidak dipakai pada lingkungan uji tanpa penyamaran.

5.3 Perlindungan Fisik

Ruang server atau pusat data memiliki kontrol akses terbatas, catatan kunjungan, perlindungan dari api, kelembapan, dan gangguan listrik (UPS/genset) sebagaimana tersedia: [isi: kondisi ruang server sebenarnya].

5.4 Perlindungan Data Pribadi

1. Data pribadi dikumpulkan seperlunya sesuai tujuan layanan akademik dan diproses secara sah.
2. Data pribadi tidak dipublikasikan tanpa dasar hukum atau persetujuan pemilik data.
3. Permintaan subjek data (akses, perbaikan, penghapusan sepanjang diizinkan) ditangani oleh petugas perlindungan data pribadi.
4. Kegagalan perlindungan data pribadi dilaporkan sesuai ketentuan UU Pelindungan Data Pribadi, termasuk pemberitahuan tertulis dalam waktu 3 x 24 jam.
5. Pihak ketiga pengolah data (misalnya penyedia *cloud*) terikat perjanjian yang memuat kewajiban perlindungan data.

5.5 Pengelolaan Perangkat dan Media

Perangkat yang memuat data kelas Rahasia dilindungi kata sandi dan enkripsi. Media penyimpanan yang tidak lagi dipakai dihapus secara aman atau dimusnahkan, dan pemusnahannya dicatat.

BAB VI. KEBIJAKAN PENCADANGAN DATA

6.1 Sasaran Pemulihan

Sasaran	Nilai	Keterangan
RPO	Maksimal 24 jam	Data yang hilang tidak lebih dari satu hari kerja
RTO sistem akademik	Maksimal 8 jam kerja	Layanan KRS, nilai, dan transkrip pulih
RTO sistem pendukung (situs web, repositori)	Maksimal 24 jam	Layanan informasi publik pulih

6.2 Strategi Pencadangan 3-2-1

Setiap data penting memiliki minimal **3 salinan** (1 data produksi dan 2 cadangan), pada **2 jenis media** yang berbeda, dengan **1 salinan** disimpan di lokasi lain yang terpisah dari lokasi utama (misalnya *cloud* atau gedung berbeda).

6.3 Jadwal dan Retensi

Jenis Cadangan	Frekuensi	Waktu Pelaksanaan	Retensi
Inkremental	Harian	[isi: jam, di luar jam layanan]	30 hari
Penuh (<i>full</i>)	Mingguan	[isi: hari dan jam]	3 bulan
Penuh bulanan	Bulanan	Akhir bulan	12 bulan
Arsip akhir semester	Setiap semester	Setelah nilai dikunci	5 tahun
Arsip permanen (kelulusan, transkrip)	Setiap yudisium	Setelah yudisium	Permanen

Retensi dapat disesuaikan dengan kebijakan kearsipan institusi dan peraturan yang berlaku.

6.4 Cakupan Cadangan

Sistem/Data	Isi yang Dicadangkan
Sistem informasi akademik	Basis data, berkas unggahan, konfigurasi
Platform pembelajaran daring	Basis data, materi, tugas
Repositori dan jurnal	Berkas karya ilmiah, metadata
Situs web UPPS/prodi	Berkas situs, basis data, konfigurasi

Sistem/Data	Isi yang Dicadangkan
Data kepegawaian dan dosen	Basis data
Dokumen kerja prodi	Folder bersama (misalnya penyimpanan <i>cloud</i> institusi)

6.5 Keamanan Cadangan

1. Cadangan dienkripsi, dan kunci enkripsi disimpan terpisah serta dicadangkan secara aman.
2. Akses ke media cadangan dibatasi bagi administrator yang berwenang.
3. Salinan di luar lokasi utama dilindungi dari penghapusan tidak sengaja (misalnya salinan tidak dapat diubah atau akses hapus dibatasi).
4. Media cadangan yang sudah habis masa retensinya dimusnahkan secara aman.

BAB VII. PROSEDUR PENCADANGAN

Tahap	Kegiatan	Penanggung Jawab
1	Pekerjaan cadangan berjalan otomatis sesuai jadwal Bab VI	Administrator sistem
2	Administrator memeriksa status keberhasilan setiap hari kerja (log atau notifikasi)	Administrator sistem
3	Cadangan gagal atau tidak lengkap dicatat dan diulang pada hari yang sama	Administrator sistem
4	Verifikasi integritas cadangan (<i>checksum</i> atau uji baca) dilakukan setiap minggu	Administrator sistem
5	Hasil pencadangan dicatat pada Log Pencadangan (Lampiran A)	Administrator sistem
6	Rekapitulasi bulanan dilaporkan kepada Kepala UPT TIK	Administrator sistem
7	Kegagalan berulang (3 kali berturut-turut) dieskalasi kepada pimpinan	Kepala UPT TIK

BAB VIII. PROSEDUR PEMULIHAN DAN UJI PEMULIHAN

8.1 Prosedur Pemulihan

1. Pelaporan gangguan atau kehilangan data kepada administrator sistem.
2. Penilaian dampak dan penentuan cakupan pemulihan oleh Kepala UPT TIK bersama pemilik data.
3. Persetujuan pemulihan oleh Kepala UPT TIK (dan pimpinan UPPS bila berdampak pada layanan akademik).
4. Pemilihan titik pemulihan (cadangan terbaru yang valid).

5. Pemulihan pada lingkungan yang aman, bila perlu pada server pengganti.
6. Verifikasi kebenaran dan kelengkapan data oleh pemilik data.
7. Pengaktifan kembali layanan dan pengumuman kepada pengguna.
8. Pencatatan pada Berita Acara Pemulihan dan evaluasi penyebab (Lampiran B).

8.2 Uji Pemulihan

1. Uji pemulihan dilakukan **minimal satu kali setahun** untuk sistem informasi akademik dan **satu kali setahun** untuk sistem lain secara bergantian.
2. Uji dilakukan pada lingkungan terpisah, dengan membandingkan data hasil pemulihan terhadap sumber.
3. Hasil uji dicatat pada Berita Acara Uji Pemulihan (Lampiran B) dan mencakup waktu pemulihan aktual terhadap RTO serta selisih data terhadap RPO.
4. Temuan ditindaklanjuti melalui perbaikan prosedur atau infrastruktur.

BAB IX. KONTINUITAS LAYANAN DAN PEMULIHAN BENCANA

1. **Skenario gangguan** yang dicakup: kerusakan perangkat keras, kegagalan perangkat lunak, kesalahan operasi, serangan siber (termasuk *ransomware*), kebakaran atau banjir ruang server, dan gangguan listrik atau jaringan berkepanjangan.
2. **Layanan prioritas** pemulihan: sistem informasi akademik, kemudian platform pembelajaran daring, kemudian situs web dan repositori.
3. **Cara kerja sementara** saat sistem gangguan: layanan manual terbatas (misalnya pencatatan nilai dan presensi sementara pada formulir atau berkas lokal) yang kemudian diinput ulang setelah sistem pulih.
4. **Daftar kontak darurat** (pimpinan, UPT TIK, penyedia layanan) dipelihara dan diperbarui setiap semester: [isi: kontak].
5. **Penanganan ransomware**: sistem terdampak segera diisolasi dari jaringan, cadangan di luar lokasi dipastikan tidak terdampak, dan pemulihan dilakukan dari cadangan bersih.

BAB X. PENANGANAN INSIDEN KEAMANAN DATA

Tahap	Kegiatan	Batas Waktu
Deteksi dan pelaporan	Pengguna atau administrator melaporkan dugaan insiden kepada UPT TIK	Maksimal 24 jam sejak diketahui
Triase	Menentukan jenis dan tingkat keparahan insiden	Segera
Penahanan	Mengisolasi sistem atau akun terdampak	Segera
Investigasi	Menelusuri penyebab dan data yang terdampak melalui log	[isi: sesuai tingkat keparahan]
Pemulihan	Mengembalikan layanan dan data (Bab VIII)	Sesuai RTO
Pemberitahuan	Pemberitahuan kepada pimpinan dan, bila menyangkut data pribadi, kepada subjek data dan	Maksimal 3 x 24 jam

Tahap	Kegiatan	Batas Waktu
	pihak berwenang sesuai UU PDP	
Evaluasi	Laporan insiden dan perbaikan (Lampiran C)	Maksimal 14 hari setelah penanganan

BAB XI. PEMANTAUAN, AUDIT, DAN EVALUASI

1. **Indikator:** persentase pencadangan berhasil (target minimal 98% per bulan), hasil uji pemulihan (memenuhi RTO dan RPO), jumlah insiden dan waktu penanganannya, serta persentase akun yang ditinjau tepat waktu.
2. **Audit internal:** dilakukan oleh LPM/UPM bersama UPT TIK satu kali setahun terhadap log pencadangan, hak akses, dan berita acara uji.
3. **Tinjauan manajemen:** hasil pemantauan dibahas dalam rapat tinjauan manajemen setiap semester dan dituangkan dalam rencana tindak lanjut.
4. **Pelatihan:** pengelola dan pengguna mengikuti sosialisasi keamanan informasi dan perlindungan data pribadi minimal satu kali setahun.
5. **Peninjauan dokumen:** kebijakan ini ditinjau minimal setahun sekali atau saat terjadi perubahan sistem yang signifikan.