UNIVERSITAS ALMUSLIM **UPT. PUSAT KOMPUTER (PUSKOM)** DOKUMEN STANDAR LAYANAN	NOMOR DOKUMEN	SLA/PUSKOM/01/2026
	TANGGAL PEMBUATAN	04 September 2026
	TANGGAL REVISI	-
	TANGGAL EFEKTIF	01 Desember 2026
	DISAHKAN OLEH	KEPALA UPT. PUSKOM **Husni, S.Kom., M.Kom.** NIDN. -
	NAMA DOKUMEN	**Service Level Agreement (SLA) Layanan TIK**

1. PENDAHULUAN

Service Level Agreement (SLA) ini merupakan komitmen standar layanan UPT. Pusat Komputer (Puskom) Universitas Almuslim kepada pengguna layanan teknologi informasi dan komunikasi (TIK). SLA menetapkan jenis layanan, jam layanan, kanal pelaporan, tingkat prioritas, target waktu respons dan penyelesaian, serta mekanisme eskalasi dan evaluasi.

2. TUJUAN

1. Memberikan kepastian waktu dan kualitas layanan TIK kepada pengguna.
2. Menjadi tolok ukur kinerja UPT. Puskom dan dasar evaluasi layanan.
3. Menyelaraskan harapan antara UPT. Puskom dan unit kerja pengguna layanan.

3. PARA PIHAK

a. **Penyedia layanan**: UPT. Pusat Komputer (Puskom) Universitas Almuslim.
b. **Pengguna layanan**: pimpinan, unit kerja, dosen, tenaga kependidikan, dan mahasiswa Universitas Almuslim.

4. KATALOG LAYANAN

No	Layanan	Bidang Penanggung Jawab	Acuan
1	Pembuatan dan reset akun SIAKAD, email institusi, dan hotspot	Sistem Informasi dan Pengembangan Web	SOP/PUSKOM/01/2026
2	Penanganan gangguan jaringan dan internet	Infrastruktur dan Jaringan	SOP/PUSKOM/02/2026
3	Pemeliharaan dan perbaikan perangkat komputer	Infrastruktur dan Jaringan	SOP/PUSKOM/03/2026
4	Backup dan pemulihan data	Sistem Informasi dan Pengembangan Web	SOP/PUSKOM/04/2026
5	Pengembangan sistem informasi dan aplikasi	Sistem Informasi dan Pengembangan Web	SOP/PUSKOM/05/2026
6	Subdomain dan website unit	Sistem Informasi dan Pengembangan Web	SOP/PUSKOM/06/2026
7	Pelaporan dan perbaikan data PDDikti (Neo Feeder/Forlap)	Data Perguruan Tinggi dan Forlap Dikti	Jadwal pelaporan PDDikti
8	Pemutakhiran dan pendampingan data dosen (SISTER)	Data Dosen & SISTER	Ketentuan SISTER

5. JAM LAYANAN DAN KANAL PELAPORAN

1. Jam layanan: **Senin–Jumat, pukul 08.00–16.00 WIB**, kecuali hari libur nasional dan cuti bersama.

2. Gangguan berprioritas Kritis di luar jam layanan ditangani melalui kontak darurat UPT. Puskom.
3. Kanal pelaporan: loket Helpdesk UPT. Puskom, WhatsApp/telepon helpdesk, email Puskom, atau formulir/tiket daring yang ditetapkan UPT. Puskom.
4. Setiap laporan dicatat dan diberi nomor tiket sebagai dasar pemantauan waktu layanan.

6. TINGKAT PRIORITAS DAN TARGET WAKTU

Waktu respons dihitung sejak laporan diterima dan tercatat sampai petugas mulai menangani. Waktu penyelesaian dihitung sampai layanan pulih atau permintaan selesai, dalam jam layanan.

Prioritas	Kriteria	Contoh	Respons	Target Penyelesaian
P1 Kritis	Layanan utama tidak berfungsi dan berdampak pada banyak pengguna atau seluruh kampus.	SIAKAD tidak dapat diakses; internet seluruh kampus mati; website diretas.	30 menit	4 jam
P2 Tinggi	Gangguan pada satu gedung/unit atau fungsi penting dengan batas waktu dekat.	Jaringan satu gedung mati; gangguan saat masa KRS atau pelaporan PDDikti.	1 jam	1 hari kerja
P3 Sedang	Gangguan yang berdampak pada pengguna perorangan.	Komputer staf rusak; Wi-Fi satu ruangan lemah.	4 jam	3 hari kerja
P4 Rendah	Permintaan layanan, konsultasi, atau perubahan terencana.	Permintaan subdomain baru; konsultasi aplikasi.	1 hari kerja	5 hari kerja atau sesuai jadwal

7. TARGET LAYANAN PER JENIS LAYANAN

Layanan	Target	Catatan
Reset kata sandi akun	1 hari kerja	Setelah identitas terverifikasi
Pembuatan akun baru	1 hari kerja	Setelah data induk tersedia
Penanganan gangguan jaringan	Sesuai prioritas (butir 6)	Eskalasi ISP mengikuti perjanjian dengan ISP
Perbaikan perangkat tanpa suku cadang	3 hari kerja	
Perbaikan perangkat dengan suku cadang	Mengikuti proses pengadaan	Pemohon diberi informasi perkiraan waktu
Pemulihan (restore) data	1 hari kerja	Setelah disetujui Kepala UPT. Puskom
Pembuatan subdomain/website unit	3 hari kerja	Setelah permohonan disetujui
Pengembangan sistem informasi	Sesuai jadwal proyek	Jadwal disepakati dalam rancangan sistem
Perbaikan data PDDikti	3 hari kerja	Setelah data dari program studi/unit lengkap
Pemutakhiran data dosen pada SISTER	3 hari kerja	Setelah dokumen pendukung lengkap

8. TARGET KETERSEDIAAN LAYANAN

Layanan	Target Ketersediaan	Periode Ukur
SIAKAD	99%	Per bulan
Website utama universitas	99%	Per bulan
Akses internet kampus	98%	Per bulan
Hotspot/Wi-Fi area utama	95%	Per bulan

Ketersediaan dihitung di luar waktu pemeliharaan terjadwal dan gangguan yang termasuk pengecualian pada butir 12.

9. PEMELIHARAAN TERJADWAL

1. Pemeliharaan yang menghentikan layanan diumumkan sekurang-kurangnya 3 (tiga) hari kerja sebelumnya.
2. Pemeliharaan dilakukan di luar jam sibuk dan tidak dijadwalkan pada masa KRS, input nilai, ujian, atau batas waktu pelaporan PDDikti, kecuali keadaan mendesak.
3. Pemeliharaan darurat untuk menutup celah keamanan dapat dilakukan sewaktu-waktu dengan pemberitahuan secepatnya.

10. ESKALASI

Level	Penanggung Jawab	Kondisi Eskalasi
1	Helpdesk/staf UPT. Puskom	Penanganan awal seluruh laporan.
2	Kepala Bidang terkait	Target respons atau penyelesaian berpotensi terlampaui, atau masalah memerlukan keahlian khusus.
3	Kepala UPT. Puskom	Gangguan P1, target penyelesaian terlampaui, atau perlu keputusan sumber daya.
4	Pimpinan Universitas/vendor	Bencana TIK, insiden keamanan besar, atau memerlukan anggaran/pihak eksternal.

11. KEWAJIBAN PENGGUNA

1. Melaporkan gangguan melalui kanal resmi dengan informasi yang jelas (lokasi, gejala, waktu kejadian, dan kontak).
2. Melengkapi data dan dokumen yang diperlukan untuk permintaan layanan.
3. Menjaga kerahasiaan akun dan mematuhi Kebijakan Keamanan Informasi.
4. Melakukan backup data pribadi/kerja sebelum menyerahkan perangkat untuk diperbaiki.
5. Mengonfirmasi penyelesaian layanan dan mengisi survei kepuasan bila diminta.

12. PENGECUALIAN

Target SLA tidak berlaku atau ditangguhkan dalam kondisi berikut:

a. Keadaan kahar (force majeure) seperti bencana alam, kerusuhan, atau pemadaman listrik berkepanjangan oleh PLN.
b. Gangguan pada layanan pihak ketiga di luar kendali universitas, misalnya ISP, server PDDikti, SISTER, atau penyedia email.
c. Keterlambatan akibat data atau dokumen dari pengguna belum lengkap.
d. Perangkat pribadi yang bukan inventaris universitas (ditangani sebatas kemampuan).
e. Pemeliharaan terjadwal yang telah diumumkan.

13. PEMANTAUAN, PELAPORAN, DAN EVALUASI

1. UPT. Puskom merekap tiket layanan setiap bulan, meliputi jumlah laporan, waktu respons, waktu penyelesaian, dan persentase pemenuhan target SLA.
2. Target pemenuhan SLA sekurang-kurangnya **90%** tiket diselesaikan sesuai target waktu.
3. Survei kepuasan pengguna dilaksanakan setiap semester dengan target sekurang-kurangnya **80%** responden menyatakan puas.
4. Hasil pemantauan dilaporkan kepada pimpinan dan dibahas dalam Rapat Tinjauan Manajemen (RTM) sebagai dasar perbaikan berkelanjutan.
5. SLA ini ditinjau sekurang-kurangnya satu kali setiap tahun.

14. PENUTUP

SLA ini berlaku sejak tanggal efektif yang ditetapkan dan menjadi acuan bersama bagi UPT. Puskom dan seluruh pengguna layanan TIK di lingkungan Universitas Almuslim.

Ditetapkan di : Bireuen
Pada tanggal : 04 September 2026
Kepala UPT. Pusat Komputer,

Husni, S.Kom., M.Kom.
NIDN. -

UNIVERSITAS ALMUSLIM **UPT. PUSAT KOMPUTER (PUSKOM)** DOKUMEN KEBIJAKAN	NOMOR DOKUMEN	KEB/PUSKOM/02/2026
	TANGGAL PEMBUATAN	04 September 2026
	TANGGAL REVISI	-
	TANGGAL EFEKTIF	01 Desember 2026
	DISAHKAN OLEH	KEPALA UPT. PUSKOM **Husni, S.Kom., M.Kom.** NIDN. -
	NAMA DOKUMEN	**Kebijakan Backup dan Disaster Recovery Plan (DRP)**

1. TUJUAN

1. Menjamin data dan sistem informasi Universitas Almuslim dapat dipulihkan apabila terjadi kehilangan, kerusakan, atau serangan.
2. Menetapkan jadwal, metode, retensi, dan tanggung jawab pelaksanaan backup.
3. Menetapkan rencana pemulihan bencana (Disaster Recovery Plan/DRP) agar layanan TIK prioritas dapat kembali beroperasi dalam batas waktu yang ditentukan.

2. RUANG LINGKUP

Kebijakan ini berlaku untuk seluruh data, aplikasi, server, dan perangkat jaringan yang dikelola UPT. Puskom, termasuk SIAKAD, website universitas dan website unit, basis data pelaporan PDDikti (Neo Feeder), data dosen/SISTER yang dikelola universitas, repositori kode sumber, serta konfigurasi perangkat jaringan. Layanan yang dikelola penyedia eksternal (misalnya email institusi berbasis cloud) diatur sesuai ketentuan penyedia, dengan pengawasan UPT. Puskom.

3. DASAR HUKUM DAN ACUAN

1. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024.
2. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.
3. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.
4. Statuta Universitas Almuslim.
5. Kebijakan Keamanan Informasi (ISMS) UPT. Puskom (KEB/PUSKOM/01/2026).
6. SNI ISO/IEC 27001:2022 dan ISO 22301:2019 Sistem Manajemen Keberlangsungan Usaha (sebagai acuan).

4. DEFINISI

Istilah	Pengertian
Backup penuh (full)	Salinan seluruh data pada suatu sistem pada waktu tertentu.
Backup inkremental	Salinan data yang berubah sejak backup terakhir.
Retensi	Lamanya salinan backup disimpan sebelum dihapus atau ditimpa.
RPO (Recovery Point Objective)	Batas maksimal data yang boleh hilang, diukur dalam waktu sejak backup terakhir.
RTO (Recovery Time Objective)	Batas maksimal waktu sampai layanan kembali beroperasi setelah terjadi gangguan.

Istilah	Pengertian
Bencana TIK	Kejadian yang menyebabkan satu atau lebih layanan TIK prioritas tidak dapat beroperasi melebihi batas waktu normal penanganan gangguan.
DRP	Rencana dan langkah terdokumentasi untuk memulihkan layanan TIK setelah terjadi bencana TIK.

5. KEBIJAKAN BACKUP

5.1 Prinsip Umum

1. Backup mengikuti aturan **3-2-1**: sekurang-kurangnya 3 salinan data, pada 2 jenis media berbeda, dan 1 salinan disimpan di luar lokasi (offsite/cloud).
2. Backup dilakukan secara otomatis sesuai jadwal; backup manual dilakukan sebelum perubahan besar (pembaruan aplikasi, migrasi, sinkronisasi PDDikti).
3. Media dan file backup dienkripsi serta disimpan di tempat dengan akses terbatas.
4. Setiap backup diverifikasi keberhasilannya dan dicatat pada log backup.

5.2 Jadwal dan Retensi Backup

Aset	Jenis dan Frekuensi	Retensi	Lokasi Penyimpanan
Basis data SIAKAD	Inkremental harian; penuh mingguan; penuh sebelum dan sesudah masa KRS/nilai	Harian 30 hari; mingguan 3 bulan; semesteran 5 tahun	Server backup lokal + penyimpanan offsite/cloud
Basis data Neo Feeder PDDikti	Penuh sebelum dan sesudah sinkronisasi; penuh mingguan	Per periode pelaporan, minimal 5 tahun	Server backup lokal + offsite/cloud
Data dosen/SISTER yang dikelola universitas	Penuh mingguan	1 tahun	Server backup lokal + offsite/cloud
Website universitas dan website unit (file + basis data)	Penuh mingguan; penuh sebelum pembaruan CMS/plugin	3 bulan	Server backup lokal + offsite/cloud
Repositori kode sumber aplikasi	Setiap perubahan (repositori) + salinan penuh bulanan	1 tahun	Repositori resmi + offsite
Konfigurasi perangkat jaringan (router, switch, firewall)	Setiap perubahan + bulanan	1 tahun	Server backup lokal
Image server/mesin virtual	Bulanan dan sebelum perubahan besar	3 versi terakhir	Media penyimpanan eksternal

5.3 Verifikasi dan Uji Pemulihan

1. Log backup harian diperiksa setiap hari kerja; backup yang gagal diulang pada hari yang sama.
2. Uji pemulihan (restore test) dilakukan setiap bulan pada lingkungan uji untuk sekurang-kurangnya satu sistem prioritas secara bergiliran.
3. Hasil uji pemulihan dicatat dalam laporan uji pemulihan dan dilaporkan kepada Kepala UPT. Puskom.

5.4 Tanggung Jawab Backup

Pelaksana	Tanggung Jawab
Kepala UPT. Puskom	Menetapkan jadwal backup, menyetujui pemulihan data pada sistem produksi, dan meninjau laporan backup.
Bidang Sistem Informasi dan Pengembangan Web	Melaksanakan backup SIAKAD, website, basis data aplikasi, dan repositori kode sumber.

Pelaksana	Tanggung Jawab
Bidang Infrastruktur dan Jaringan	Menyediakan media/server backup, melaksanakan backup konfigurasi jaringan dan image server.
Bidang Data Perguruan Tinggi dan Forlap Dikti	Memastikan backup Neo Feeder dilakukan sebelum dan sesudah setiap sinkronisasi pelaporan.
Bidang Data Dosen & SISTER	Memastikan data dosen yang dikelola universitas tercakup dalam jadwal backup.

6. DISASTER RECOVERY PLAN (DRP)

6.1 Prioritas Layanan dan Target Pemulihan

Layanan	Prioritas	RTO	RPO
SIAKAD	Kritis	4 jam	24 jam
Jaringan dan akses internet kampus	Kritis	4 jam	-
Neo Feeder PDDikti (masa pelaporan)	Kritis	4 jam	Sinkronisasi terakhir
Website utama universitas	Tinggi	8 jam	7 hari
Email institusi	Tinggi	Sesuai SLA penyedia	Sesuai SLA penyedia
Neo Feeder PDDikti (di luar masa pelaporan)	Tinggi	1 hari kerja	Sinkronisasi terakhir
Website unit (subdomain)	Sedang	3 hari kerja	7 hari

6.2 Skenario Bencana dan Respons Utama

Skenario	Respons Utama
Kerusakan perangkat keras server	Memindahkan layanan ke server cadangan/mesin virtual lain, memulihkan dari backup terakhir, kemudian memperbaiki atau mengganti perangkat.
Ransomware atau peretasan	Segera memutus server terdampak dari jaringan, mengamankan bukti dan log, mengganti seluruh kata sandi terkait, memulihkan dari backup bersih yang telah diverifikasi, menutup celah keamanan sebelum layanan dibuka kembali.
Deface/penyusupan konten ilegal pada website	Menonaktifkan sementara website, membersihkan atau memulihkan dari backup bersih, memperbarui CMS/plugin, mengganti kredensial, dan memantau ulang.
Gangguan listrik berkepanjangan	Menjalankan UPS dan genset (jika tersedia), mematikan server secara terkendali bila daya cadangan hampir habis, menghidupkan kembali sesuai urutan prioritas.
Gangguan ISP	Mengalihkan ke jalur internet cadangan (jika tersedia) dan melakukan eskalasi ke ISP sesuai perjanjian layanan.
Bencana alam (gempa, banjir, kebakaran)	Mengutamakan keselamatan personel, menilai kerusakan, memulihkan layanan prioritas dari backup offsite/cloud pada infrastruktur alternatif.
Kesalahan manusia (data terhapus/terubah)	Memulihkan data dari backup sesuai SOP Backup dan Pemulihan Data setelah disetujui Kepala UPT. Puskom.

6.3 Tim Tanggap Darurat TIK

Peran	Pejabat	Tugas
Koordinator	Kepala UPT. Puskom (Husni, S.Kom., M.Kom.)	Menetapkan status bencana TIK, memimpin pemulihan, melapor kepada Rektor.
Infrastruktur	Kepala Bidang Infrastruktur dan Jaringan (Hermansyah, S.E., S.Kom., M.Kom.)	Memulihkan jaringan, server, listrik, dan perangkat.
Aplikasi dan data sistem	Kepala Bidang Sistem Informasi dan Pengembangan Web (Al-Khaidar, S.Tr.Kom., M.Kom.)	Memulihkan aplikasi, basis data, dan website dari backup.
Data PDDikti	Kepala Bidang Data Perguruan Tinggi dan Forlap Dikti (Ridwan, S.Pd., M.Pd.)	Memulihkan Neo Feeder dan memastikan keutuhan data pelaporan.

Peran	Pejabat	Tugas
Data dosen	Kepala Bidang Data Dosen & SISTER (Fadhil, S.Kom.)	Memastikan keutuhan data dosen dan koordinasi layanan SISTER.
Komunikasi	Unit Humas Universitas	Menyampaikan informasi gangguan dan pemulihan kepada sivitas akademika.

6.4 Tahapan Pemulihan

1. **Deteksi dan pelaporan**: gangguan diketahui dari pemantauan atau laporan pengguna, lalu dilaporkan kepada Kepala UPT. Puskom.
2. **Penilaian dan penetapan status**: Kepala UPT. Puskom menilai dampak dan menetapkan status bencana TIK apabila target RTO berpotensi terlampaui.
3. **Aktivasi tim**: Tim Tanggap Darurat TIK dihubungi dan berkumpul (langsung atau daring).
4. **Pembatasan dampak**: mengisolasi sistem terdampak, terutama pada serangan siber, serta mengamankan bukti.
5. **Pemulihan**: memulihkan layanan sesuai urutan prioritas pada butir 6.1 menggunakan backup terverifikasi.
6. **Verifikasi**: menguji fungsi layanan dan keutuhan data bersama pemilik aset.
7. **Kembali normal**: layanan dibuka kembali dan diumumkan kepada pengguna.
8. **Laporan pasca-insiden**: disusun paling lambat 7 (tujuh) hari kerja, memuat kronologi, penyebab, dampak, dan tindakan pencegahan.

6.5 Daftar Kontak Darurat

No	Nama/Jabatan	Nomor HP	Keterangan
1	Kepala UPT. Puskom		Koordinator
2	Kepala Bidang Infrastruktur dan Jaringan		
3	Kepala Bidang Sistem Informasi dan Pengembangan Web		
4	Kepala Bidang Data Perguruan Tinggi dan Forlap Dikti		
5	Kepala Bidang Data Dosen & SISTER		
6	Penyedia layanan internet (ISP)		Nomor layanan pelanggan
7	PLN setempat		

Daftar kontak ini diperbarui setiap terjadi perubahan personel dan disimpan dalam bentuk cetak di ruang Puskom serta salinan digital di luar server utama.

7. PENGUJIAN DAN PEMELIHARAAN DRP

1. Simulasi (drill) pemulihan bencana dilaksanakan sekurang-kurangnya satu kali setiap tahun untuk layanan berprioritas Kritis.
2. Hasil simulasi dievaluasi untuk memperbaiki prosedur, kontak, dan target pemulihan.
3. Dokumen ini ditinjau sekurang-kurangnya satu kali setiap tahun atau setelah terjadi bencana TIK.

8. REKAMAN

1. Log backup dan verifikasi backup.
2. Laporan uji pemulihan bulanan.
3. Laporan simulasi DRP tahunan.
4. Laporan insiden dan laporan pasca-insiden.
5. Berita acara pemulihan data.

9. PENUTUP

Kebijakan ini berlaku sejak tanggal efektif yang ditetapkan dan menjadi acuan pelaksanaan SOP Backup dan Pemulihan Data Sistem Informasi (SOP/PUSKOM/04/2026).

Ditetapkan di : Bireuen
Pada tanggal : 04 September 2026

Kepala UPT. Pusat Komputer,

Husni, S.Kom., M.Kom.
NIDN. -

UNIVERSITAS ALMUSLIM **UPT. PUSAT KOMPUTER (PUSKOM)** DOKUMEN SUMBER DAYA	NOMOR DOKUMEN	DOK/PUSKOM/01/2026
	TANGGAL PEMBUATAN	04 September 2026
	TANGGAL REVISI	-
	TANGGAL EFEKTIF	01 Desember 2026
	DISAHKAN OLEH	KEPALA UPT. PUSKOM **Husni, S.Kom., M.Kom.** NIDN. -
	NAMA DOKUMEN	**Dokumen Sumber Daya Teknologi Informasi dan Komunikasi (TIK)**

1. PENDAHULUAN

Dokumen ini menguraikan sumber daya yang dikelola UPT. Pusat Komputer (Puskom) Universitas Almuslim untuk menjamin layanan TIK berjalan efektif, sebagai pemenuhan klausul 7.1 SNI ISO 9001:2015 dan SNI ISO 21001:2018. Sumber daya yang diuraikan meliputi sumber daya manusia (7.1.2), infrastruktur (7.1.3), lingkungan untuk operasi proses (7.1.4), sumber daya pemantauan dan pengukuran (7.1.5), serta pengetahuan organisasi (7.1.6).

Dokumen ini dimutakhirkan sekurang-kurangnya satu kali setiap semester oleh bidang terkait dan disahkan Kepala UPT. Puskom.

2. SUMBER DAYA MANUSIA (KLAUSUL 7.1.2)

2.1 Struktur dan Personel UPT. Puskom

No	Jabatan	Nama	Tugas Pokok	Kompetensi yang Dipersyaratkan	Pelatihan/Sertifikasi yang Dimiliki
1	Kepala UPT. Puskom	Husni, S.Kom., M.Kom.	Memimpin, merencanakan, dan mengendalikan seluruh layanan TIK; menetapkan kebijakan dan SOP unit.	Manajemen TI, tata kelola dan keamanan informasi, perencanaan anggaran TIK.	-
2	Kepala Bidang Data Perguruan Tinggi dan Forlap Dikti	Ridwan, S.Pd., M.Pd.	Mengelola pelaporan PDDikti (Neo Feeder), validasi dan sinkronisasi data perguruan tinggi.	Pengelolaan Neo Feeder/PDDikti, validasi data akademik, basis data.	-
3	Kepala Bidang Data Dosen & SISTER	Fadhil, S.Kom.	Mengelola dan memutakhirkan data dosen pada SISTER; pendampingan dosen dan operator.	Pengelolaan SISTER, data kepegawaian dosen, layanan pengguna.	-
4	Kepala Bidang Infrastruktur dan Jaringan	Hermansyah, S.E., S.Kom., M.Kom.	Mengelola jaringan, internet, server fisik, ruang server, dan perangkat komputer.	Jaringan komputer (routing, switching, wireless), administrasi server, keamanan jaringan.	-

No	Jabatan	Nama	Tugas Pokok	Kompetensi yang Dipersyaratkan	Pelatihan/Sertifikasi yang Dimiliki
5	Kepala Bidang Sistem Informasi dan Pengembangan Web	Al-Khaidar, S.Tr.Kom., M.Kom.	Mengelola dan mengembangkan SIAKAD, website, aplikasi, basis data, akun, dan backup sistem.	Pemrograman web, basis data, analisis sistem, keamanan aplikasi, administrasi CMS.	-

2.2 Pengembangan Kompetensi

1. Kebutuhan pelatihan personel diidentifikasi setiap tahun berdasarkan kompetensi yang dipersyaratkan dan hasil evaluasi kinerja.
2. Prioritas pelatihan: keamanan informasi, administrasi jaringan dan server, pengelolaan PDDikti/SISTER, serta pengembangan aplikasi.
3. Bukti pelatihan (sertifikat, surat tugas, daftar hadir) disimpan sebagai rekaman kompetensi dan diserahkan salinannya ke BPKU (Kepegawaian).
4. Pelatihan silang antarbidang dilakukan untuk mengurangi ketergantungan pada personel kunci (Register Risiko R12).

3. INFRASTRUKTUR (KLAUSUL 7.1.3)

3.1 Komponen Infrastruktur TIK

Infrastruktur TIK yang dikelola UPT. Puskom terdiri atas komponen berikut. Rincian jumlah, merek/tipe, spesifikasi, tahun pengadaan, dan kondisi setiap perangkat tercatat pada **Daftar Inventaris Aset Universitas (BPKU)** dan **Daftar Inventaris Perangkat TIK UPT. Puskom** yang dimutakhirkan setiap semester.

No	Kelompok	Komponen	Fungsi
1	Server dan penyimpanan data	Server aplikasi SIAKAD dan basis data, server website, server Neo Feeder PDDikti, media/server backup	Menjalankan sistem informasi universitas dan menyimpan data institusi beserta salinannya
2	Perangkat jaringan	Router/gateway, firewall, core switch, distribution/access switch, access point, kabel backbone	Menghubungkan seluruh gedung dan pengguna ke layanan internal dan internet
3	Koneksi internet	Layanan internet dari penyedia jasa internet (ISP)	Menyediakan akses internet bagi sivitas akademika dan layanan daring
4	Kelistrikan pendukung	UPS untuk server dan perangkat jaringan inti	Menjaga layanan tetap berjalan saat gangguan listrik singkat
5	Perangkat kerja dan alat teknisi	Komputer/laptop kerja, printer/scanner, LAN tester, crimping tool, perangkat cadangan	Mendukung pekerjaan personel dan perbaikan gangguan

Penanggung Jawab Infrastruktur	Bidang
Server, jaringan, internet, kelistrikan pendukung, dan perangkat kerja	Bidang Infrastruktur dan Jaringan
Aplikasi, basis data, dan backup sistem informasi	Bidang Sistem Informasi dan Pengembangan Web
Server dan aplikasi Neo Feeder PDDikti	Bidang Data Perguruan Tinggi dan Forlap Dikti

3.2 Sistem Informasi dan Aplikasi

No	Sistem/Aplikasi	Alamat/Akses	Pengelola	Pengguna
1	Sistem Informasi Akademik (SIAKAD)	sia.umuslim.ac.id	Bidang SI dan Pengembangan Web	Mahasiswa, dosen, BAKK, fakultas, prodi
2	Website universitas	umuslim.ac.id	Bidang SI dan Pengembangan Web	Publik dan sivitas akademika

No	Sistem/Aplikasi	Alamat/Akses	Pengelola	Pengguna
3	Website unit (subdomain)	*.umuslim.ac.id	Bidang SI dan Pengembangan Web (teknis); unit (konten)	Publik dan sivitas akademika
4	Neo Feeder PDDikti	Jaringan internal	Bidang Data PT dan Forlap Dikti	Operator PDDikti, prodi
5	SISTER	Layanan Kementerian	Bidang Data Dosen & SISTER (pendampingan)	Dosen, operator
6	Email institusi	@umuslim.ac.id	Bidang SI dan Pengembangan Web	Dosen, tenaga kependidikan, mahasiswa
7	Hotspot/Wi-Fi kampus	Seluruh area kampus	Bidang Infrastruktur dan Jaringan	Sivitas akademika

4. LINGKUNGAN UNTUK OPERASI PROSES (KLAUSUL 7.1.4)

UPT. Puskom menetapkan persyaratan lingkungan kerja berikut. Pemenuhannya diperiksa setiap semester oleh Bidang Infrastruktur dan Jaringan, dan kekurangan yang ditemukan diusulkan perbaikannya melalui rencana kerja dan anggaran.

No	Persyaratan Lingkungan	Tujuan
1	Ruang server terkunci dengan akses terbatas dan catatan akses	Mencegah akses fisik oleh pihak yang tidak berwenang
2	Pendingin ruangan (AC) ruang server beroperasi terus-menerus	Menjaga suhu perangkat agar tidak cepat rusak
3	UPS, grounding, dan penangkal petir/arrester	Melindungi perangkat dari gangguan listrik dan sambaran petir
4	Alat pemadam api ringan (APAR) di ruang server	Penanganan awal bila terjadi kebakaran
5	Rak server dan pengaturan kabel yang rapi serta berlabel	Memudahkan pemeliharaan dan penanganan gangguan
6	Ruang layanan helpdesk yang mudah dijangkau pengguna	Mendukung layanan tatap muka kepada pengguna
7	Ruang kerja personel yang memadai (pencahayaan, ventilasi, ergonomi)	Mendukung kenyamanan dan produktivitas kerja

5. SUMBER DAYA PEMANTAUAN DAN PENGUKURAN (KLAUSUL 7.1.5)

No	Sarana	Yang Dipantau/Diukur	Frekuensi	Penanggung Jawab
1	Aplikasi/sistem pemantauan jaringan dan server	Status perangkat, pemakaian bandwidth, ketersediaan layanan (uptime)	Terus-menerus	Bidang Infrastruktur dan Jaringan
2	Log sistem dan log akses server	Aktivitas akses, kesalahan sistem, indikasi serangan	Harian	Bidang SI dan Pengembangan Web
3	Log backup	Keberhasilan backup dan uji pemulihan	Harian/bulanan	Bidang SI dan Pengembangan Web
4	Buku log/aplikasi tiket helpdesk	Jumlah laporan, waktu respons, waktu penyelesaian (SLA)	Setiap laporan; rekap bulanan	Kepala UPT. Puskom
5	Survei kepuasan pengguna layanan TIK	Tingkat kepuasan pengguna	Setiap semester	Kepala UPT. Puskom
6	Laporan validasi PDDikti	Kelengkapan dan kesesuaian data pelaporan	Setiap periode pelaporan	Bidang Data PT dan Forlap Dikti

Indikator dan target pengukuran mengacu pada Service Level Agreement (SLA) Layanan TIK (SLA/PUSKOM/01/2026).

6. PENGETAHUAN ORGANISASI (KLAUSUL 7.1.6)

No	Pengetahuan	Bentuk Penyimpanan	Penanggung Jawab

No	Pengetahuan	Bentuk Penyimpanan	Penanggung Jawab
1	Kebijakan, SOP, dan SLA Puskom	Dokumen terkendali (cetak dan digital)	Kepala UPT. Puskom
2	Topologi jaringan dan konfigurasi perangkat	Diagram topologi dan backup konfigurasi	Bidang Infrastruktur dan Jaringan
3	Dokumentasi teknis sistem informasi (rancangan, basis data, manual)	Repositori dokumentasi dan kode sumber	Bidang SI dan Pengembangan Web
4	Panduan pelaporan PDDikti dan kalender pelaporan	Dokumen panduan internal	Bidang Data PT dan Forlap Dikti
5	Panduan SISTER untuk dosen dan operator	Dokumen panduan dan materi pelatihan	Bidang Data Dosen & SISTER
6	Kredensial sistem penting	Penyimpanan terenkripsi dengan akses terbatas	Kepala UPT. Puskom
7	Pembelajaran dari insiden dan gangguan	Laporan pasca-insiden dan rekap tiket	Kepala UPT. Puskom

7. PEMUTAKHIRAN

1. Dokumen ini dimutakhirkan sekurang-kurangnya satu kali setiap semester atau saat terjadi perubahan sumber daya yang signifikan.
2. Kebutuhan penambahan atau peremajaan sumber daya diusulkan melalui rencana kerja dan anggaran tahunan UPT. Puskom.
3. Dokumen terkait: Register Analisis Risiko UPT. Puskom, Kebijakan Backup dan DRP, SLA Layanan TIK, serta SOP/PUSKOM/01–06/2026.

Ditetapkan di : Bireuen
Pada tanggal : 04 September 2026

Kepala UPT. Pusat Komputer,

Husni, S.Kom., M.Kom.
NIDN. -

UNIVERSITAS ALMUSLIM **UPT. PUSAT KOMPUTER (PUSKOM)** DOKUMEN REGISTER RISIKO	NOMOR DOKUMEN	REG/PUSKOM/01/2026
	TANGGAL PEMBUATAN	04 September 2026
	TANGGAL REVISI	-
	TANGGAL EFEKTIF	01 Desember 2026
	DISAHKAN OLEH	KEPALA UPT. PUSKOM **Husni, S.Kom., M.Kom.** NIDN. -
	NAMA DOKUMEN	**Register Analisis Risiko UPT. Puskom**

1. PENDAHULUAN

Register ini mendokumentasikan hasil identifikasi, analisis, dan rencana penanganan risiko serta peluang pada layanan TIK yang dikelola UPT. Pusat Komputer (Puskom) Universitas Almuslim, sebagai pemenuhan klausul 6.1 SNI ISO 9001:2015 dan acuan Kebijakan Keamanan Informasi (KEB/PUSKOM/01/2026). Register ditinjau sekurang-kurangnya satu kali setiap semester, setelah terjadi insiden besar, atau apabila ada perubahan sistem yang signifikan.

2. KRITERIA PENILAIAN RISIKO

Nilai risiko = Kemungkinan (K) × Dampak (D). Masing-masing dinilai dengan skala 1–5 sebagai berikut:

Skor	Kemungkinan (K)	Keterangan	Skor	Dampak (D)	Keterangan
1	Sangat jarang	Hampir tidak pernah terjadi (lebih dari 5 tahun sekali)	1	Tidak signifikan	Tidak mengganggu layanan; tertangani rutin
2	Jarang	Dapat terjadi sekali dalam 2–5 tahun	2	Kecil	Gangguan pada sedikit pengguna, pulih kurang dari 1 hari
3	Kadang-kadang	Dapat terjadi sekali dalam setahun	3	Sedang	Gangguan pada satu unit/gedung atau layanan penting tertunda
4	Sering	Dapat terjadi beberapa kali dalam setahun	4	Besar	Layanan utama terganggu luas, kehilangan data sebagian, keluhan meluas
5	Hampir pasti	Terjadi setiap bulan atau lebih sering	5	Sangat besar	Kehilangan data penting, kebocoran data pribadi, sanksi/akreditasi terdampak, reputasi rusak

Rendah (1–4)	Sedang (5–9)	Tinggi (10–14)	Sangat Tinggi (15–25)
Diterima; dipantau secara rutin.	Dikendalikan dengan prosedur yang ada; dipantau tiap semester.	Wajib ada rencana mitigasi dengan PIC dan target waktu.	Prioritas utama; mitigasi segera dan dilaporkan kepada pimpinan.

3. REGISTER RISIKO

No	Kode	Kategori	Risiko	Penyebab	Dampak	K	D	Nilai	Tingkat	Pengendalian yang Ada	Rencana Mitigasi	PIC	Target Waktu	Status
1	R01	Infrastruktur	Server SIAKAD mati atau rusak	Perangkat keras tua, tidak ada server cadangan	SIAKAD tidak dapat diakses, KRS/nilai terhambat	2	5	10	Tinggi	Backup basis data, UPS	Menyiapkan server/mesin virtual cadangan dan prosedur failover; peremajaan perangkat	Kabid Infrastruktur dan Jaringan	Juni 2027	Terbuka
2	R02	Keamanan	Serangan ransomware/malware pada server	Celah keamanan belum ditambal, kata sandi lemah	Data terenkripsi/hilang, layanan berhenti lama	3	5	15	Sangat Tinggi	Antivirus, firewall	Patch berkala maks. 14 hari, backup offline/offsite, 2FA admin, pembatasan akses jarak jauh	Kabid SI dan Pengembangan Web	Desember 2026	Terbuka
3	R03	Keamanan	Website diretas/deface atau disusupi konten judi online	CMS/plugin usang, akun admin lemah, website unit tidak terawat	Reputasi universitas rusak, domain masuk daftar blokir	4	4	16	Sangat Tinggi	Pembaruan CMS tidak terjadwal	Pembaruan CMS/plugin bulanan, 2FA admin, pemindaian malware, inventaris dan penonaktifan website tidak aktif	Kabid SI dan Pengembangan Web	Desember 2026	Terbuka
4	R04	Data	Kebocoran data pribadi mahasiswa/dosen	Hak akses berlebihan, ekspor data tanpa kendali, celah aplikasi	Pelanggaran UU PDP, sanksi, kehilangan kepercayaan	2	5	10	Tinggi	Hak akses berbasis peran di SIAKAD	Peninjauan hak akses tiap semester, penyamaran data di tampilan publik, log akses, sosialisasi PDP	Kepala UPT. Puskom	Maret 2027	Terbuka
5	R05	Akun	Pencurian akun melalui phishing atau kata sandi lemah	Kesadaran pengguna rendah, kata sandi dipakai ulang	Penyalahgunaan akun, perubahan data tanpa izin	4	3	12	Tinggi	Reset kata sandi via helpdesk	Kebijakan kata sandi minimal 10 karakter, 2FA untuk akun penting, sosialisasi anti-phishing	Kabid SI dan Pengembangan Web	Maret 2027	Terbuka
6	R06	Infrastruktur	Koneksi internet terputus (gangguan ISP)	Satu jalur ISP, gangguan kabel/fiber	Layanan daring dan pelaporan terhenti	3	4	12	Tinggi	Eskalasi ke ISP	Menyediakan jalur ISP cadangan/failover, perjanjian SLA dengan ISP	Kabid Infrastruktur dan Jaringan	Juni 2027	Terbuka
7	R07	Infrastruktur	Gangguan listrik dan kerusakan akibat petir	Listrik tidak stabil, grounding/penangkal petir kurang	Perangkat rusak, server mati mendadak, data korup	3	4	12	Tinggi	UPS pada server	Pemeriksaan grounding dan arrester, uji kapasitas UPS, kajian genset untuk ruang server	Kabid Infrastruktur dan Jaringan	Maret 2027	Terbuka
8	R08	Bencana	Gempa, banjir, atau kebakaran merusak ruang server	Lokasi rawan gempa, seluruh data di satu lokasi	Kehilangan perangkat dan data, layanan berhenti lama	2	5	10	Tinggi	APAR di ruang server	Backup offsite/cloud sesuai aturan 3-2-1, simulasi DRP tahunan	Kepala UPT. Puskom	Desember 2026	Terbuka
9	R09	Data	Backup gagal atau tidak dapat dipulihkan	Backup tidak diverifikasi, media rusak	Data tidak dapat dipulihkan saat dibutuhkan	2	5	10	Tinggi	Backup terjadwal	Verifikasi log harian dan uji restore bulanan terdokumentasi	Kabid SI dan Pengembangan Web	Desember 2026	Terbuka
10	R10	Pelaporan	Pelaporan PDDikti terlambat atau tidak valid	Data prodi terlambat/tidak lengkap, kendala Neo Feeder	Status mahasiswa/prodi bermasalah, nilai akreditasi terdampak	3	5	15	Sangat Tinggi	Pendampingan prodi menjelang pelaporan	Kalender pelaporan internal, validasi data sebelum sinkronisasi, backup Neo Feeder sebelum/sesudah sinkronisasi	Kabid Data PT dan Forlap Dikti	Setiap semester	Terbuka
11	R11	Data dosen	Data dosen pada SISTER tidak mutakhir	Dokumen dosen terlambat, kurangnya pendampingan	Proses jabatan fungsional, BKD, dan sertifikasi dosen terhambat	3	4	12	Tinggi	Layanan konsultasi SISTER	Jadwal pemutakhiran berkala, pengingat ke dosen, pelatihan operator fakultas	Kabid Data Dosen & SISTER	Setiap semester	Terbuka

No	Kode	Kategori	Risiko	Penyebab	Dampak	K	D	Nilai	Tingkat	Pengendalian yang Ada	Rencana Mitigasi	PIC	Target Waktu	Status
12	R12	SDM	Ketergantungan pada personel kunci	Pengetahuan sistem tidak terdokumentasi, kurangnya personel cadangan	Layanan terhenti saat personel tidak ada	3	4	12	Tinggi	-	Dokumentasi teknis, penyimpanan kredensial terkendali, pelatihan silang antarbidang	Kepala UPT. Puskom	Juni 2027	Terbuka
13	R13	Aplikasi	Kegagalan pembaruan SIAKAD pada masa sibuk	Pengujian kurang, pembaruan langsung di produksi	Gangguan KRS/input nilai	3	4	12	Tinggi	Pengujian oleh pengembang	Server staging, UAT, larangan pembaruan pada masa KRS/nilai, rencana rollback	Kabid SI dan Pengembangan Web	Desember 2026	Terbuka
14	R14	Kapasitas	Bandwidth tidak mencukupi pada jam sibuk	Pertumbuhan pengguna, tidak ada manajemen bandwidth	Akses lambat, keluhan pengguna	4	3	12	Tinggi	Pembatasan sebagian	Manajemen bandwidth per segmen, pemantauan pemakaian, kajian penambahan kapasitas	Kabid Infrastruktur dan Jaringan	Maret 2027	Terbuka
15	R15	Kepatuhan	Penggunaan perangkat lunak tidak berlisensi	Anggaran lisensi terbatas, instalasi oleh pengguna	Risiko hukum dan malware	3	3	9	Sedang	-	Inventaris perangkat lunak, penggunaan alternatif open source, pembatasan hak instalasi	Kabid Infrastruktur dan Jaringan	Juni 2027	Terbuka

4. PETA RISIKO (SEBELUM MITIGASI)

Kemungkinan \ Dampak	D = 1	D = 2	D = 3	D = 4	D = 5
K = 5					
K = 4			R05, R14	R03	
K = 3			R15	R06, R07, R11, R12, R13	R02, R10
K = 2					R01, R04, R08, R09
K = 1					

Ringkasan: 15 risiko teridentifikasi, terdiri atas 3 risiko Sangat Tinggi, 11 risiko Tinggi, 1 risiko Sedang, dan 0 risiko Rendah. Risiko Sangat Tinggi menjadi prioritas penanganan dan dilaporkan kepada pimpinan universitas.

5. REGISTER PELUANG

No	Kode	Peluang	Manfaat	Rencana Tindak Lanjut	PIC	Target
1	P01	Integrasi akun tunggal (Single Sign-On) untuk SIAKAD, email, dan layanan lain	Pengguna cukup satu akun; pengelolaan akun lebih aman dan efisien	Kajian teknis dan uji coba SSO bertahap	Kabid SI dan Pengembangan Web	Desember 2027
2	P02	Pemanfaatan layanan cloud untuk backup offsite	Memenuhi aturan 3-2-1 dengan biaya relatif rendah	Pemilihan penyedia dan uji pemulihan dari cloud	Kabid Infrastruktur dan Jaringan	Maret 2027
3	P03	Dashboard data institusi terintegrasi PDDikti dan SISTER	Mendukung akreditasi, pengambilan keputusan, dan pemantauan mutu data	Perancangan dashboard bersama bidang data	Kabid Data PT dan Forlap Dikti	Juni 2027
4	P04	Sistem tiket helpdesk daring	Pemantauan SLA otomatis dan rekap layanan akurat	Implementasi aplikasi tiket sumber terbuka	Kabid SI dan Pengembangan Web	Maret 2027

6. RIWAYAT PENINJAUAN

No	Tanggal Tinjauan	Perubahan/Hasil Tinjauan	Ditinjau Oleh
1	04 September 2026	Penyusunan register awal	Kepala UPT. Puskom
2			
3			

Ditetapkan di : Bireuen
Pada tanggal : 04 September 2026

Kepala UPT. Pusat Komputer,



Husni, S.Kom., M.Kom.
NIDN. -

UNIVERSITAS ALMUSLIM **UPT. PUSAT KOMPUTER (PUSKOM)** DOKUMEN KEBIJAKAN	NOMOR DOKUMEN	KEB/PUSKOM/01/2026
	TANGGAL PEMBUATAN	04 September 2026
	TANGGAL REVISI	-
	TANGGAL EFEKTIF	01 Desember 2026
	DISAHKAN OLEH	KEPALA UPT. PUSKOM **Husni, S.Kom., M.Kom.** NIDN.
	NAMA DOKUMEN	**Kebijakan Keamanan Informasi (ISMS)**

1. LATAR BELAKANG

Universitas Almuslim mengelola informasi dalam jumlah besar melalui sistem informasi akademik (SIAKAD), website, email institusi, pelaporan Pangkalan Data Pendidikan Tinggi (PDDikti), data dosen pada SISTER, serta jaringan dan server kampus. Informasi tersebut merupakan aset penting yang menentukan kelancaran tridharma perguruan tinggi, akreditasi, dan kepercayaan sivitas akademika.

Ancaman terhadap informasi, seperti peretasan, pengubahan tampilan (deface) dan penyusupan konten ilegal pada website, ransomware, pencurian akun, kebocoran data pribadi, kerusakan perangkat, serta bencana alam, menuntut adanya kebijakan keamanan informasi yang jelas, terdokumentasi, dan dipatuhi seluruh pihak. Kebijakan ini menjadi landasan Sistem Manajemen Keamanan Informasi (Information Security Management System/ISMS) di lingkungan Universitas Almuslim.

2. TUJUAN

1. Melindungi kerahasiaan, keutuhan (integritas), dan ketersediaan informasi milik Universitas Almuslim.
2. Melindungi data pribadi mahasiswa, dosen, tenaga kependidikan, dan pihak lain sesuai ketentuan peraturan perundang-undangan.
3. Menetapkan peran, tanggung jawab, dan aturan minimum keamanan informasi bagi seluruh pengguna layanan TIK.
4. Mengurangi risiko dan dampak insiden keamanan informasi serta menjamin keberlangsungan layanan TIK.
5. Menjadi acuan penyusunan SOP, standar teknis, dan pengendalian keamanan informasi di UPT. Puskom dan unit kerja.

3. RUANG LINGKUP

Kebijakan ini berlaku bagi seluruh aset informasi dan seluruh pengguna di lingkungan Universitas Almuslim, meliputi:

a. **Aset informasi**: data akademik, data keuangan yang tersimpan pada sistem TIK, data kepegawaian, data pelaporan PDDikti, data dosen (SISTER), dokumen elektronik, dan kode sumber aplikasi.
b. **Sistem dan layanan**: SIAKAD, website universitas dan website unit (subdomain umuslim.ac.id), email institusi, aplikasi Neo Feeder PDDikti, hotspot/Wi-Fi, server, basis data, dan aplikasi lain yang dikelola atau digunakan universitas.
c. **Infrastruktur**: jaringan kampus, perangkat jaringan, ruang server, perangkat komputer milik universitas, dan layanan cloud yang digunakan universitas.

d. **Pengguna**: pimpinan, dosen, tenaga kependidikan, mahasiswa, serta pihak ketiga (vendor, mitra, tenaga kontrak) yang diberi akses.

4. DASAR HUKUM DAN ACUAN

1. Undang-Undang Nomor 12 Tahun 2012 tentang Pendidikan Tinggi.
2. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024.
3. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.
4. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.
5. Statuta Universitas Almuslim.
6. SNI ISO/IEC 27001:2022 Sistem Manajemen Keamanan Informasi (sebagai acuan).
7. SNI ISO 9001:2015 Sistem Manajemen Mutu, klausul 6.1, 7.1, 7.5, dan 8.1 (sebagai acuan).

5. DEFINISI

Istilah	Pengertian
Informasi	Data yang telah diolah dan memiliki nilai bagi universitas, dalam bentuk elektronik maupun cetak.
Aset informasi	Informasi beserta sistem, perangkat, dan media yang digunakan untuk mengolah, menyimpan, atau mengirimkannya.
Keamanan informasi	Terjaganya kerahasiaan (confidentiality), keutuhan (integrity), dan ketersediaan (availability) informasi.
Insiden keamanan informasi	Kejadian yang mengancam atau telah merusak keamanan informasi, misalnya peretasan, malware, kebocoran data, atau penyalahgunaan akun.
Data pribadi	Data tentang orang perseorangan yang teridentifikasi atau dapat diidentifikasi, sebagaimana dimaksud dalam UU Pelindungan Data Pribadi.
Pemilik aset informasi	Unit kerja yang bertanggung jawab atas isi dan penggunaan suatu data atau sistem (misalnya Biro Akademik untuk data akademik).
Pengelola TIK	UPT. Puskom selaku unit yang mengelola infrastruktur dan sistem informasi universitas.
Pengguna	Setiap orang yang diberi hak akses terhadap sistem atau layanan TIK universitas.

6. PRINSIP KEAMANAN INFORMASI

1. **Kerahasiaan**: informasi hanya dapat diakses oleh pihak yang berwenang.
2. **Keutuhan**: informasi akurat, lengkap, dan tidak diubah tanpa kewenangan.
3. **Ketersediaan**: informasi dan layanan dapat diakses saat dibutuhkan oleh pihak yang berwenang.
4. **Hak akses minimum**: setiap pengguna hanya diberi akses sebatas yang diperlukan untuk tugasnya.
5. **Akuntabilitas**: setiap aktivitas pada sistem penting dapat ditelusuri ke akun pengguna tertentu.
6. **Berbasis risiko**: pengendalian keamanan ditetapkan berdasarkan hasil analisis risiko (Register Analisis Risiko UPT. Puskom).

7. PERNYATAAN KEBIJAKAN

7.1 Organisasi dan Tanggung Jawab

Peran	Tanggung Jawab
Rektor	Menetapkan arah kebijakan keamanan informasi, menyediakan sumber daya, dan menerima laporan insiden besar.

Peran	Tanggung Jawab
Kepala UPT. Puskom	Penanggung jawab penerapan kebijakan; mengoordinasikan pengendalian keamanan, penanganan insiden, dan peninjauan kebijakan.
Kepala Bidang Infrastruktur dan Jaringan	Keamanan jaringan, server, ruang server, perangkat, dan pemantauan gangguan.
Kepala Bidang Sistem Informasi dan Pengembangan Web	Keamanan aplikasi, basis data, website, akun dan hak akses sistem, serta backup data sistem informasi.
Kepala Bidang Data Perguruan Tinggi dan Forlap Dikti	Keamanan, keakuratan, dan kerahasiaan data pelaporan PDDikti serta akun Neo Feeder.
Kepala Bidang Data Dosen & SISTER	Keamanan, keakuratan, dan kerahasiaan data dosen serta akun SISTER.
Pimpinan unit kerja (pemilik aset)	Menentukan klasifikasi data unitnya, menyetujui hak akses, dan memastikan staf mematuhi kebijakan.
Seluruh pengguna	Menjaga kerahasiaan akun, mematuhi kebijakan ini, dan segera melaporkan dugaan insiden.

7.2 Klasifikasi Informasi

Setiap informasi diklasifikasikan oleh pemilik aset dan diperlakukan sesuai tingkatnya:

Kelas	Contoh	Perlakuan Minimum
Publik	Profil universitas, berita, pengumuman, informasi program studi.	Boleh dipublikasikan setelah disetujui unit berwenang.
Internal	Surat edaran internal, jadwal rapat, notulen umum.	Hanya untuk sivitas akademika; tidak disebarkan ke luar tanpa izin.
Terbatas	Nilai mahasiswa, data kepegawaian, data PDDikti, data SISTER, data keuangan.	Akses berdasarkan peran dan persetujuan pemilik aset; disimpan pada sistem resmi.
Rahasia	Kata sandi, kunci enkripsi, NIK dan data pribadi spesifik, konfigurasi keamanan server.	Akses sangat terbatas; wajib dienkripsi saat disimpan atau dikirim; tidak boleh dibagikan melalui media terbuka.

7.3 Pengendalian Akses dan Akun

1. Setiap pengguna memperoleh akun pribadi yang unik. Penggunaan akun bersama tidak diperkenankan, kecuali akun layanan yang tercatat dan memiliki penanggung jawab.
2. Pemberian, perubahan, dan pencabutan hak akses dilakukan sesuai SOP Pembuatan dan Reset Akun Layanan TIK serta persetujuan pemilik aset.
3. Kata sandi minimal 10 karakter, tidak mudah ditebak, tidak sama dengan kata sandi layanan lain, dan wajib diganti apabila diduga diketahui pihak lain.
4. Akun administrator sistem, server, Neo Feeder, dan panel website wajib dilindungi autentikasi dua faktor (2FA) apabila tersedia.
5. Hak akses pegawai yang mutasi, berhenti, atau pensiun dicabut/disesuaikan paling lambat 7 (tujuh) hari kerja setelah pemberitahuan dari unit kepegawaian.
6. Peninjauan hak akses pada sistem penting dilakukan sekurang-kurangnya satu kali setiap semester.

7.4 Penggunaan Layanan TIK yang Dapat Diterima

Pengguna dilarang:

a. Memberikan akun atau kata sandi kepada orang lain.
b. Mengakses, mengubah, atau menghapus data tanpa kewenangan.
c. Memasang perangkat lunak tidak berlisensi atau berbahaya pada perangkat milik universitas.
d. Menggunakan jaringan kampus untuk perjudian daring, pornografi, peretasan, penyebaran hoaks, atau kegiatan melanggar hukum lainnya.

e. Memasang perangkat jaringan (router, access point) pada jaringan kampus tanpa izin UPT. Puskom.
f. Mengunggah data berklasifikasi Terbatas atau Rahasia ke layanan pihak ketiga yang tidak disetujui universitas.

7.5 Keamanan Jaringan, Server, dan Perangkat

1. Ruang server dikunci, aksesnya dicatat, serta dilengkapi pendingin ruangan, UPS, dan alat pemadam api ringan.
2. Jaringan dilindungi firewall dan dipisahkan (segmentasi) antara jaringan server, jaringan staf, dan jaringan hotspot mahasiswa.
3. Pembaruan keamanan (patch) kritis pada server, CMS, dan aplikasi dipasang paling lambat 14 (empat belas) hari sejak dirilis, didahului backup.
4. Perangkat komputer universitas dilengkapi antivirus/antimalware yang aktif dan diperbarui.
5. Log akses dan log sistem pada server penting disimpan sekurang-kurangnya 6 (enam) bulan.
6. Perubahan konfigurasi perangkat inti dan server produksi dicatat dan disetujui Kepala UPT. Puskom.

7.6 Pelindungan Data Pribadi

1. Data pribadi hanya dikumpulkan dan diproses sesuai tujuan yang sah dan seperlunya (prinsip minimisasi data).
2. Data pribadi pada sistem universitas tidak boleh diekspor, disalin ke perangkat pribadi, atau diserahkan ke pihak lain tanpa persetujuan pemilik aset.
3. Tampilan data pribadi pada website publik wajib dibatasi (misalnya penyamaran sebagian NIK/nomor telepon).
4. Pemusnahan media penyimpanan yang berisi data pribadi dilakukan dengan cara yang menjamin data tidak dapat dipulihkan.

7.7 Backup dan Keberlangsungan Layanan

Backup data dan pemulihan layanan dilaksanakan sesuai Kebijakan Backup dan Disaster Recovery Plan (DRP) UPT. Puskom serta SOP Backup dan Pemulihan Data Sistem Informasi.

7.8 Pengembangan dan Pengadaan Sistem

1. Pengembangan aplikasi mengikuti SOP Pengembangan Sistem Informasi dan Aplikasi, termasuk pengujian keamanan dasar sebelum digunakan.
2. Pengembangan dan pengujian dilakukan pada server pengembangan/staging, bukan langsung pada sistem produksi.
3. Kode sumber disimpan pada repositori resmi universitas dan tidak boleh memuat kata sandi atau kunci rahasia secara langsung.
4. Pengadaan aplikasi atau layanan dari pihak ketiga wajib mempertimbangkan aspek keamanan dan pelindungan data.

7.9 Pihak Ketiga

Vendor, mitra, atau tenaga kontrak yang memperoleh akses terhadap sistem atau data universitas wajib menandatangani perjanjian kerahasiaan, diberi akses sebatas pekerjaannya, dan aksesnya dicabut setelah pekerjaan selesai.

7.10 Penanganan Insiden Keamanan Informasi

1. Setiap pengguna wajib melaporkan dugaan insiden kepada Helpdesk UPT. Puskom paling lambat 1x24 jam sejak diketahui.

2. UPT. Puskom mencatat, mengklasifikasi, membatasi dampak (misalnya memutus sistem yang terinfeksi), memulihkan layanan, dan menelusuri penyebab insiden.
3. Insiden berdampak besar dilaporkan oleh Kepala UPT. Puskom kepada Rektor.
4. Apabila terjadi kegagalan pelindungan data pribadi, universitas menyampaikan pemberitahuan tertulis kepada subjek data pribadi dan lembaga yang berwenang paling lambat 3x24 jam sesuai UU Pelindungan Data Pribadi.
5. Setiap insiden dibuatkan laporan pasca-insiden yang memuat kronologi, dampak, penyebab, dan tindakan perbaikan.

7.11 Kesadaran dan Pelatihan

UPT. Puskom menyelenggarakan sosialisasi keamanan informasi sekurang-kurangnya satu kali setiap tahun, antara lain tentang kata sandi yang aman, pengenalan phishing, dan pelindungan data pribadi. Personel UPT. Puskom mengikuti peningkatan kompetensi keamanan informasi secara berkala.

8. SANKSI

Pelanggaran terhadap kebijakan ini dapat dikenai tindakan berupa penangguhan atau pencabutan hak akses, serta sanksi sesuai peraturan kepegawaian dan peraturan akademik Universitas Almuslim, tanpa mengurangi tanggung jawab hukum berdasarkan peraturan perundang-undangan.

9. PEMANTAUAN, EVALUASI, DAN PENINJAUAN

1. Penerapan kebijakan ini dipantau oleh UPT. Puskom dan dievaluasi melalui Audit Mutu Internal (AMI).
2. Kebijakan ditinjau sekurang-kurangnya satu kali setiap tahun, atau lebih cepat apabila terjadi perubahan peraturan, perubahan sistem yang signifikan, atau insiden besar.
3. Hasil peninjauan dilaporkan dalam Rapat Tinjauan Manajemen (RTM).

10. DOKUMEN TERKAIT

1. Kebijakan Backup dan Disaster Recovery Plan (DRP) UPT. Puskom.
2. Service Level Agreement (SLA) Layanan TIK.
3. Register Analisis Risiko UPT. Puskom.
4. SOP/PUSKOM/01/2026 sampai dengan SOP/PUSKOM/06/2026.

11. PENUTUP

Kebijakan ini berlaku sejak tanggal efektif yang ditetapkan dan wajib dipatuhi oleh seluruh pengguna layanan TIK di lingkungan Universitas Almuslim.

Ditetapkan di : Bireuen
Pada tanggal : 04 September 2026
Kepala UPT. Pusat Komputer,

Husni, S.Kom., M.Kom.
NIDN. -