UPA TIK
UNIVERSITAS NEGERI MANADO

KEAMANAN INFORMASI, BACKUP & RECOVERY DAN PENANGANAN INSIDEN TEKNOLOGI INFORMASI

Standard Operational Procedure (SOP)

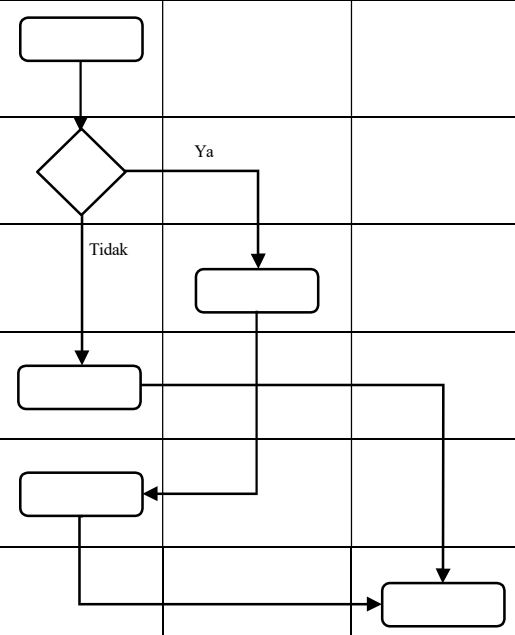
upatik@unima.ac.id

KEMENTERIAN PENDIDIKAN, KEBUDAYAAN, RISET DAN TEKNOLOGI UNIVERSITAS NEGERI MANADO	**NOMOR POS-AP**	009/UN41/UPATIK-SOP/2026
	TGL PEMBUATAN	01 Juli 2026
	REVISI	
	NOMOR POS-AP	
	TGL REVISI	
	TGL EFEKTIF	01 Agustus 2026
	DISAHKAN OLEH	KEPALA  Dr. Quido Conferti Kainde, ST, MM, MT NIP 198406062009121007
	NAMA POS AP	SOP Keamanan Informasi (Cyber Security)

DASAR HUKUM	**TUJUAN**
1. Undang-Undang Nomor 20 Tahun 2003 tentang Sistem Pendidikan Nasional. 2. Peraturan Menteri Pendidikan dan Kebudayaan Nomor 13 Tahun 2020 tentang Sistem Informasi Manajemen Pendidikan Tinggi. 3. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah terakhir dengan UU No. 1 Tahun 2024. 4. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE). 5. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE). 6. Peraturan Peraturan Badan Cyber dan Sandi Negara (BSSN) Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi SPBE dan Standar Penyelenggaraan KAMI.	1. Menjamin kerahasiaan (Confidentiality), integritas (Integrity), dan ketersediaan (Availability) seluruh aset informasi, aplikasi, data, dan infrastruktur jaringan di lingkungan Universitas Negeri Manado. 2. Mencegah, meminimalkan, dan mengendalikan risiko akses tidak sah (unauthorized access), kebocoran data, serangan siber, serta penyalahgunaan fasilitas TIK. 3. Memastikan kepatuhan (compliance) terhadap regulasi keamanan informasi nasional dan standar internasional.
RUANG LINGKUP	**ISTILAH DAN DEFINISI**
1. Manajemen Identitas dan Akses Kontrol (Identity & Access Management / IAM) untuk seluruh sivitas akademika dan pengelola TIK. 2. Keamanan Perangkat Keras, Server, Router, Switch, Firewalls, dan Jaringan Nirkabel (Wi-Fi) UNIMA. 3. Keamanan Sistem Informasi Layanan Akademik, Keuangan, Kepegawaian, dan Portal Utama Universitas	1. UPA TIK: Unit Pendukung Akademik Teknologi Informasi dan Komunikasi Universitas Negeri Manado. 2. MFA (Multi-Factor Authentication): Metode otentikasi keamanan yang memerlukan dua atau lebih bukti identitas. 3. Vulnerability Assessment (VA): Proses identifikasi, evaluasi, dan pengkategorian celah keamanan pada system. 4. Hardening: Proses mengamankan sistem dengan menutup port yang tidak digunakan, mengubah kredensial default, dan mengonfigurasi parameter keamanan.
KETERKAITAN	**PERALATAN/PERLENGKAPAN**
1. SOP Manajemen Resiko TI. 2. SOP Pengelolaan Infrastruktur Jaringan.	1. PC/Laptop 2. Printer 3. Kertas
PERINGATAN	**PENCATATAN DAN PENDATAAN**
1. Peraturan ini dibuat untuk menjelaskan alur Keamanan Teknologi Informasi. 2. Jika SOP ini tidak dilaksanakan, maka akan berdampak terganggunya layanan publik.	Disimpan sebagai data elektronik dan manual.

POS-AP KEAMANAN INFORMASI (CYBER SECURITY)

No	Kegiatan	Pelaksana			Mutu Baku			Keterangan
		Tim Cyber Security	Admin Server / Jaringan	Ketua UPATIK	Persyaratan/ Input	Waktu	Output	
1	Melakukan scanning kerentanan rutin (Vulnerability Assessment) pada server & jaringan.				Jadwal Audit / Daftar IP Server	1 hari	Draft Laporan Hasil Audit VA	
2	Apakah ditemukan celah kerentanan tingkat Tinggi (High/Critical)?		Ya		Hasil VA Scanner	2 Jam	Kategori Risiko (Kritis / Rendah)	
3	Melakukan patching firmware/OS, penutupan port, dan hardening konfigurasi.	Tidak			Rekomendasi Perbaikan & Patch File	1-3 Hari	Sistem Ter-patch & Log Patching	
4	Mendokumentasikan status aman ke dalam Log Keamanan Rutin.				Laporan VA Bersih	1 Jam	Dokumen Log Rutin	
5	Melakukan Re-scanning (Pemeriksaan Ulang) untuk verifikasi penutupan celah.				Sistem Pasca Patching	4 Jam	Laporan Verifikasi Keamanan	
6	Menerima, mereview, dan menandatangani Laporan Evaluasi Keamanan Informasi Bulanan				Laporan Verifikasi Keamanan	1 Hari	Laporan Disetujui & Dearsipkan	



KEMENTERIAN PENDIDIKAN, KEBUDAYAAN, RISET DAN TEKNOLOGI UNIVERSITAS NEGERI MANADO	**NOMOR POS-AP**	010/UN41/UPATIK-SOP/2026
	TGL PEMBUATAN	01 Juli 2026
	REVISI	
	NOMOR POS-AP	
	TGL REVISI	
	TGL EFEKTIF	01 Agustus 2026
	DISAHKAN OLEH	KEPALA Dr. Quido Conferti Kainde, ST, MM, MT NIP 198406062009121007
	NAMA POS AP	SOP Cadangan dan Pemulihan Data (Backup dan Recovery)

DASAR HUKUM	**TUJUAN**
1. Undang-Undang Nomor 20 Tahun 2003 tentang Sistem Pendidikan Nasional. 2. Peraturan Menteri Pendidikan dan Kebudayaan Nomor 13 Tahun 2020 tentang Sistem Informasi Manajemen Pendidikan Tinggi. 3. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah terakhir dengan UU No. 1 Tahun 2024. 4. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE). 5. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE). 6. Peraturan Pemerintah No. 71 Tahun 2019 tentang PSTE (Kewajiban Pengelolaan Cadangan Data dan Disaster Recovery). 7. ISO/IEC 27001:2022 Kontrol A.8.13 (Information Backup). 8. ISO/IEC 27031 (Guidelines for information and communication technology readiness for business continuity).	1. Memastikan seluruh data kritis Universitas Negeri Manado (Database Akademik, Data Keuangan, Data Kepegawaian, Repositori, dan Konfigurasi Server) tersimpan secara aman dan teratur. 2. Menjamin ketersediaan data dan keberlangsungan operasional TIK jika terjadi kegagalan perangkat keras, bencana alam, atau serangan malware/ransomware. 3. Menetapan standar waktu pemulihan data (Recovery Time Objective / RTO) dan batas kehilangan data (Recovery Point Objective / RPO) yang terukur.
RUANG LINGKUP	**ISTILAH DAN DEFINISI**
1. Database seluruh aplikasi kampus. 2. Source code aplikasi, repositori dokumen digital, dan asset file pengajar & mahasiswa. 3. File Konfigurasi Perangkat Jaringan (Router, Switch, Firewall, Domain Name Server). 4. Virtual Machine dan Image Operating System pada Data Center UPA TIK UNIMA.	1. UPA TIK: Unit Pendukung Akademik Teknologi Informasi dan Komunikasi Universitas Negeri Manado. 2. MFA (Multi-Factor Authentication): Metode otentikasi keamanan yang memerlukan dua atau lebih bukti identitas. 3. Vulnerability Assessment (VA): Proses identifikasi, evaluasi, dan pengkategorian celah keamanan pada system. 4. Hardening: Proses mengamankan sistem dengan menutup port yang tidak digunakan, mengubah kredensial default, dan mengonfigurasi parameter keamanan.
KETERKAITAN	**PERALATAN/PERLENGKAPAN**
1. SOP Manajemen Resiko TI. 2. SOP Pengelolaan Infrastruktur Jaringan. 3. SOP Keamanan Informasi (Cyber Security)	1. PC/Laptop 2. Printer 3. Kertas
PERINGATAN	**PENCATATAN DAN PENDATAAN**
1. Peraturan ini dibuat untuk menjelaskan alur Cadangan dan Pemulihan Data (Backup dan Recovery). 2. Jika SOP ini tidak dilaksanakan, maka akan berdampak terganggunya layanan publik.	Disimpan sebagai data elektronik dan manual.

POS-AP Cadangan dan Pemulihan Data (Backup dan Recovery)

No	Kegiatan	Pelaksana			Mutu Baku			Keterangan
		Tim Cyber Security	Admin Server / Jaringan	Ketua UPATIK	Persyaratan/ Input	Waktu	Output	
1	Menjalankan skrip backup otomatis (Full Backup Mingguan, Incremental Backup Harian).				Jadwal Cronjob / Backup Script	Sesuai Jadwal	File Backup Terenkripsi (.sql.gz / .iso)	
2	Melakukan verifikasi integritas file cadangan (Checksum SHA256) & Replikasi ke Offsite Cloud.				File Backup Hasil Eksekusi	1 Jam	Log Checksum & Status Sync Cloud	
3	Apakah terjadi kerusakan data / insiden yang membutuhkan pemulihan (Recovery)?		Tidak / Ya		Laporan Kegagalan System / Request	15 Menit	Keputusan Pemulihan Data	
4	jika Ada Recovery Request Melakukan isolasi lingkungan staging dan eksekusi skrip Restorasi Data.				File Backup Terverifikasi & Server Staging	2 - 4 Jam (RTO)	Data Terpulihkan di Staging	
5	Melakukan uji coba pengembalian data (Disaster Recovery Simulation) bulanan.				Sampel File Backup	1 Hari	Laporan Uji Coba Pemulihan Data	
6	Pemeriksaan akhir kesesuaian data terpulihkan & Penandatanganan Berita Acara Pemulihan Data.				Data Teruji & Laporan Restorasi	1 Jam	File Backup Terenkripsi (.sql.gz / .iso)	

KEMENTERIAN PENDIDIKAN, KEBUDAYAAN, RISET DAN TEKNOLOGI UNIVERSITAS NEGERI MANADO	**NOMOR POS-AP**	010/UN41/UPATIK-SOP/2026
	TGL PEMBUATAN	01 Juli 2026
	REVISI	
	NOMOR POS-AP	
	TGL REVISI	
	TGL EFEKTIF	01 Agustus 2026
	DISAHKAN OLEH	KEPALA  Dr. Quido Conferti Kainde, ST, MM, MT NIP 198406062009121007
	NAMA POS AP	SOP Penanganan Insiden IT

DASAR HUKUM	**TUJUAN**
1. Undang-Undang Nomor 20 Tahun 2003 tentang Sistem Pendidikan Nasional. 2. Peraturan Menteri Pendidikan dan Kebudayaan Nomor 13 Tahun 2020 tentang Sistem Informasi Manajemen Pendidikan Tinggi. 3. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana diubah terakhir dengan UU No. 1 Tahun 2024. 4. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PSTE). 5. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE). 6. Peraturan Peraturan Badan Cyber dan Sandi Negara (BSSN) Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi SPBE dan Standar Penyelenggaraan KAMI.	1. Menjadi pedoman baku dalam mengidentifikasi, merespons, menanggulangi, dan memulihkan sistem TIK Universitas Negeri Manado dari gangguan siber, serangan Ransomware, Deface Website, DDoS, atau kebocoran data. 2. Mencegah eskalasi dampak serangan siber agar tidak meluas ke jaringan internal kampus. 3. Memastikan koordinasi yang cepat dan efektif antara Tim UPATIK UNIMA, BSSN, dan pimpinan Universitas.
RUANG LINGKUP	**ISTILAH DAN DEFINISI**
1. Kategori Rendah: Gangguan layanan lokal, masalah login individu, salah konfigurasi minor. 2. Kategori Sedang: Serangan Defacement pada website fakultas/prodi, serangan Brute Force terdeteksi. 3. Kategori Tinggi / Kritis: Serangan Ransomware pada data center, kebocoran basis data utama (Data Breach), Malware spreading, atau DDoS melumpuhkan server jaringan utama.	1. UPA TIK: Unit Pendukung Akademik Teknologi Informasi dan Komunikasi Universitas Negeri Manado. 2. MFA (Multi-Factor Authentication): Metode otentikasi keamanan yang memerlukan dua atau lebih bukti identitas. 3. Vulnerability Assessment (VA): Proses identifikasi, evaluasi, dan pengkategorian celah keamanan pada system. 4. Hardening: Proses mengamankan sistem dengan menutup port yang tidak digunakan, mengubah kredensial default, dan mengonfigurasi parameter keamanan.
KETERKAITAN	**PERALATAN/PERLENGKAPAN**
1. SOP Manajemen Resiko TI. 2. SOP Pengelolaan Infrastruktur Jaringan. 3. SOP Keamanan Informasi (Cyber Security) 4. Cadangan dan Pemulihan Data (Backup dan Recovery).	1. PC/Laptop 2. Printer 3. Kertas
PERINGATAN	**PENCATATAN DAN PENDATAAN**
1. Peraturan ini dibuat untuk menjelaskan alur Penanganan Insiden TI. 2. Jika SOP ini tidak dilaksanakan, maka akan berdampak terganggunya layanan publik.	Disimpan sebagai data elektronik dan manual.

POS-AP SOP Penanganan Insiden IT

No	Kegiatan	Pelaksana				Mutu Baku			Keterangan
		Pengguna	Tim Cyber Security	Admin Server / Jaringan	Ketua UPATIK	Kelengkapan	Waktu	Output	
1	Mengirimkan laporan adanya anomali / deteksi serangan siber oleh					Tiket Laporan / Alert SIEM	15 Menit	Notifikasi Insiden Masuk	
2	Melakukan Verifikasi & Triage (Klasifikasi tingkat keparahan insiden: Rendah, Sedang, Kritis).					Alert & Bukti Awal Insiden	30 Menit	Formulir Klasifikasi Insiden	
3	Melakukan Tindakan Isolasi / Containment (Memutuskan koneksi jaringan server terinfeksi agar tidak menyebar).					Daftar Host Terinfeksi	15 - 30 Menit	Sistem Terisolasi (Containment)	
4	Melakukan Analisis Bukti Forensik Digital (Memory Dump, Log Server, Malware Analysis).					Log Server & Evidence Data	1 - 2 Hari	Laporan Root Cause Analysis	
5	Eradikasi (Pembersihan malware) & Pemulihan (Restorasi data bersih dari backup terverifikasi).					Laporan Forensik & Backup Clean	2 - 6 Jam	Sistem Pulih & Berjalan Normal	
6	Menyusun Laporan Pasca Insiden (Post-Incident Report) & Pelaporan ke BSSN/Rektorat.					Seluruh Rangkaian Dokumen Insiden	2 Hari	Laporan Akhir Insiden TI	