	UNIVERSITAS MUHAMMADIYAH MATARAM **STATUS INTITUSI TERAKREDITASI B** *Jl.K.H Ahmad Dahlan No. 1 Telp. (0370) 633723 Fax. (0370) 641906 Kotak Pos No. 108* *Mataram Website : http://www.ummat.ac.id Email : um.mataram@ummat.ac.id* **NUSA TENGGARA BARAT**	
Nomor SOP	*003/PPTIK/SOP/2024*	Edisi/Revisi 02
Nama SOP	*Keamanan Data*	Desember 2024

1. VISI DAN MISI UNIVERSITAS

A. VISI

"Menjadi Universitas Islami, mandiri, unggul dan berdaya saing di kawasan ASEAN pada tahun 2028"

B. MISI

Guna mencapai visi tersebut di atas, ditetapkan misi UMMAT sebagai berikut: 1. Menyelenggarakan Catur Dharma yang mampu memenuhi tuntutan masyarakat atau pengguna output pendidikan tinggi. 2. Menyelenggarakan pendidikan tinggi yang mandiri dan mampu berdaya saing di kawasan ASEAN. 3. Membentuk insan civitas akademika yang berakhlak mulia dan menjunjung tinggi nilai-nilai islam dalam suasana kampus yang islami. 4. Menyelenggarakan pengelolaan universitas yang profesional, akuntabel dan amanah. 5. Membangun kerjasama baik di tingkat regional, nasional dan internasional yang saling menguntungkan.

---

2. TUJUAN

a. *Melindungi kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability) data universitas.*

b. *Mencegah akses tidak sah terhadap sistem dan data universitas.*

c. *Menetapkan prosedur standar dalam penanganan insiden keamanan data.*

d. *Memastikan kepatuhan terhadap regulasi perlindungan data pribadi.*

e. *Meningkatkan kesadaran keamanan informasi di lingkungan civitas akademika.*

---

3. RUANG LINGKUP

a. *Pengelolaan keamanan jaringan dan infrastruktur.*

b. *Pengelolaan keamanan aplikasi dan sistem informasi.*

c. *Penanganan insiden keamanan.*

d. *Pengelolaan kerentanan (vulnerability management).*

e. *Awareness dan pelatihan keamanan informasi.*

f. *Pihak-pihak yang terlibat dalam keamanan data di lingkungan PPTIK UMMAT.*

---

4. RINGKASAN

SOP ini berisi tentang prosedur keamanan data di lingkungan PPTIK Universitas Muhammadiyah Mataram, meliputi pengelolaan keamanan infrastruktur, aplikasi, penanganan insiden, dan program kesadaran keamanan informasi.

---

5. DEFINISI ISTILAH/SINGKATAN/SIMBOL

No	*Istilah/Singkatan*	*Definisi*
a	*Confidentiality*	*Kerahasiaan - memastikan data hanya dapat diakses oleh pihak yang berwenang*
b	*Integrity*	*Integritas - memastikan data tidak diubah tanpa otorisasi*
c	*Availability*	*Ketersediaan - memastikan data dan sistem dapat diakses saat diperlukan*
d	*CIA Triad*	*Prinsip dasar keamanan informasi: Confidentiality, Integrity, Availability*
e	*Firewall*	*Sistem keamanan jaringan yang memantau dan mengontrol lalu lintas jaringan*
f	*IDS/IPS*	*Intrusion Detection/Prevention System - sistem deteksi/pencegahan intrusi*
g	*Vulnerability*	*Kerentanan keamanan pada sistem yang dapat dieksploitasi*
h	*Malware*	*Perangkat lunak berbahaya (virus, trojan, ransomware, dll)*
i	*Phishing*	*Upaya penipuan untuk mendapatkan informasi sensitif*
j	*Encryption*	*Proses mengubah data menjadi kode rahasia untuk melindungi kerahasiaan*
k	*PPTIK*	*Pusat Pengembangan Teknologi Informasi dan Komunikasi*
l	*Incident Response*	*Prosedur penanganan insiden keamanan*

6. LANDASAN HUKUM

a. *Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) sebagaimana telah diubah dengan UU No. 19 Tahun 2016.*

b. *Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi.*

c. *Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.*

d. *Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi.*

e. *Peraturan Menteri Pendidikan dan Kebudayaan Nomor 49 Tahun 2014 tentang Standar Nasional Pendidikan Tinggi.*

f. *ISO 27001:2022 - Sistem Manajemen Keamanan Informasi.*

g. *Statuta Universitas Muhammadiyah Mataram.*

h. *Kebijakan Keamanan Informasi UMMAT.*

---

7. PROSEDUR, UNIT TERKAIT/PELAKSANA, MUTU BAKU

A. Klasifikasi Data

Klasifikasi	*Deskripsi*	*Contoh*	*Penanganan*
RAHASIA	*Data sangat sensitif yang jika bocor dapat menyebabkan kerugian besar*	*Data keuangan, data pribadi sensitif, password, kunci enkripsi*	*Enkripsi wajib, akses sangat terbatas, audit log ketat*
TERBATAS	*Data internal yang tidak untuk konsumsi publik*	*Data akademik mahasiswa, data kepegawaian, laporan internal*	*Enkripsi direkomendasikan, akses terbatas sesuai kebutuhan*
INTERNAL	*Data yang dapat diakses oleh civitas akademika*	*Pengumuman internal, jadwal, dokumen operasional*	*Kontrol akses standar*
PUBLIK	*Data yang dapat diakses umum*	*Website publik, brosur, informasi umum*	*Tidak perlu enkripsi, pastikan integritas*

B. Prosedur Pengelolaan Keamanan Infrastruktur

No	*Prosedur*	*Unit Terkait*	*Mutu Baku*	*Ket*
		Kepala PPTIK	**Tim Infrastruktur**	**Programmer**
1	*Penyusunan kebijakan keamanan*	✓	✓	✓
2	*Konfigurasi firewall*		✓	
3	*Implementasi IDS/IPS*		✓	
4	*Konfigurasi antivirus/antimalware*		✓	
5	*Segmentasi jaringan*		✓	
6	*Enkripsi data sensitif*		✓	✓
7	*Monitoring keamanan 24/7*		✓	
8	*Audit keamanan berkala*	✓	✓	✓

C. Prosedur Pengelolaan Kerentanan (Vulnerability Management)

No	*Prosedur*	*Unit Terkait*	*Mutu Baku*	*Ket*
		Kepala PPTIK	**Tim Infrastruktur**	**Programmer**
1	*Vulnerability scanning berkala*		✓	
2	*Analisis hasil scan*		✓	✓
3	*Perencanaan patching*	✓	✓	
4	*Pengujian patch di environment test*		✓	✓
5	*Implementasi patch di production*		✓	
6	*Verifikasi pasca-patching*		✓	✓
7	*Dokumentasi*		✓	

D. Prosedur Penanganan Insiden Keamanan

No	*Prosedur*	*Unit Terkait*	*Mutu Baku*	*Ket*
		Kepala PPTIK	**Tim Infrastruktur**	**Programmer**
1	*Deteksi & pelaporan insiden*		✓	
2	*Klasifikasi tingkat keparahan*		✓	
3	*Containment (pembatasan dampak)*		✓	✓
4	*Eskalasi (untuk High/Critical)*	✓	✓	
5	*Investigasi & analisis*		✓	✓
6	*Eradikasi (penghapusan*		✓	✓

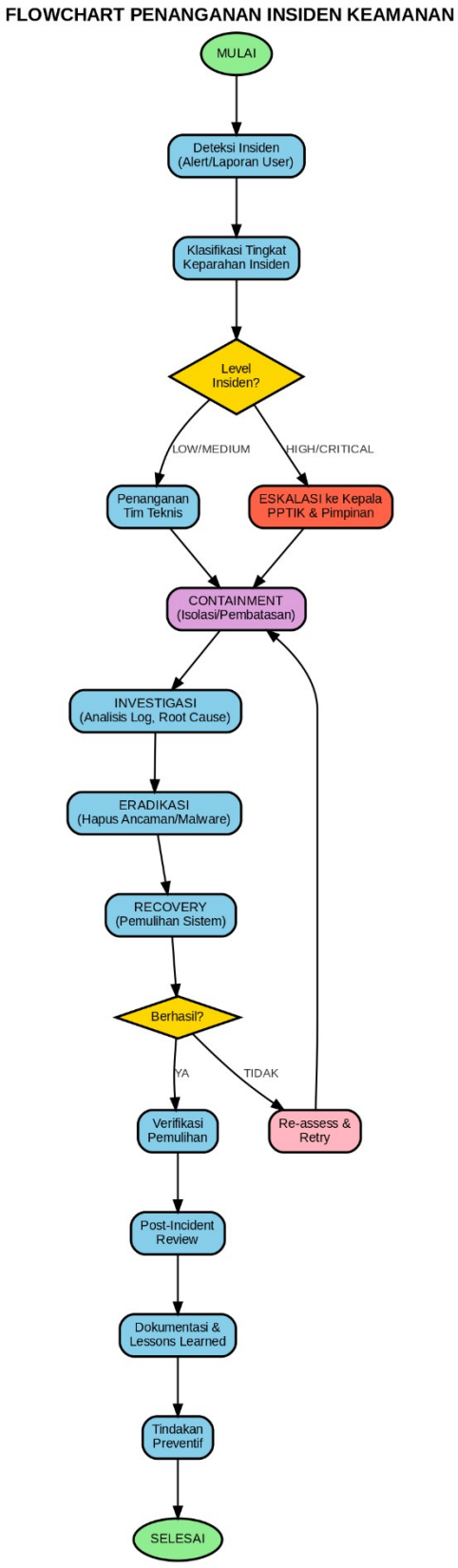
No	Prosedur	Unit Terkait	Mutu Baku	Ket
	ancaman)			
7	Recovery (pemulihan sistem)		✓	✓
8	Post-incident review	✓	✓	✓
9	Tindakan preventif	✓	✓	✓

E. Matriks Klasifikasi Insiden

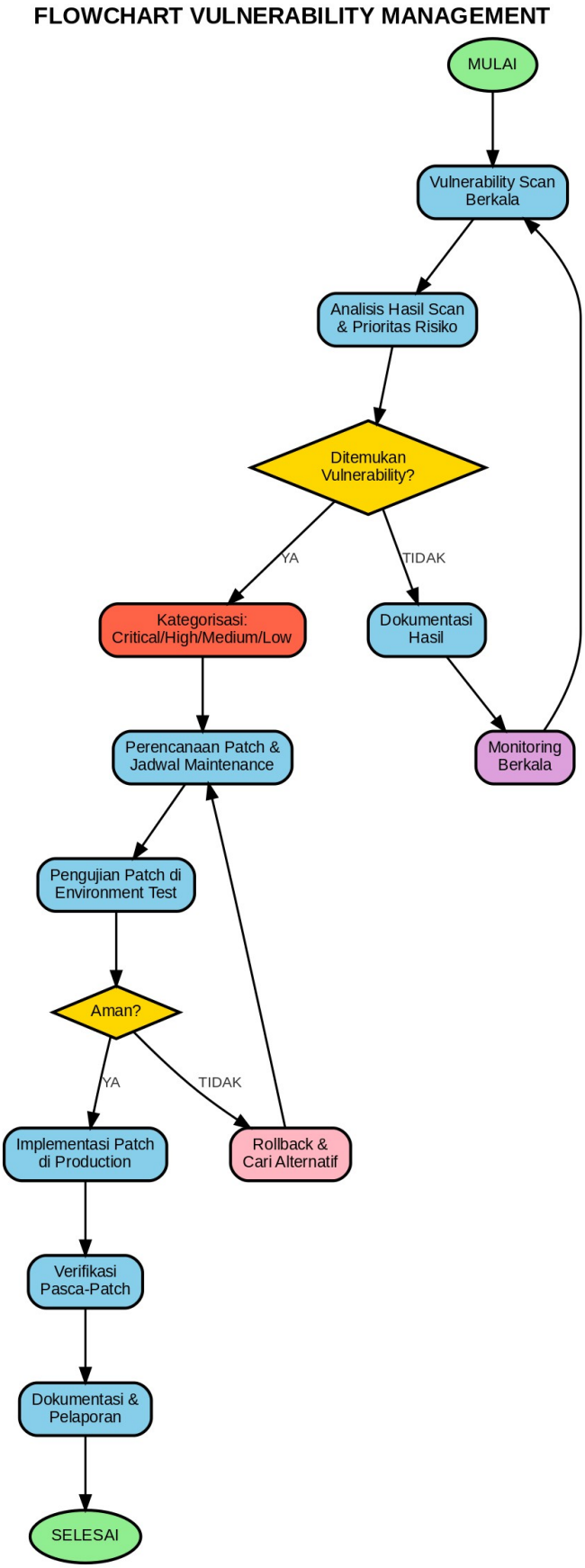
Level	Deskripsi	Contoh	Response Time	Eskalasi
CRITICAL	Dampak sangat besar, sistem utama down, data breach besar	Ransomware, data breach massal, server utama compromised	15 menit	Rektor, Kepala PPTIK, Tim Krisis
HIGH	Dampak besar, layanan terganggu signifikan	Serangan DDoS, malware menyebar, unauthorized access	1 jam	Kepala PPTIK, Tim Infrastruktur
MEDIUM	Dampak sedang, layanan parsial terganggu	Phishing berhasil, virus terdeteksi (terisolasi)	4 jam	Tim Infrastruktur
LOW	Dampak kecil, tidak mengganggu operasional	Spam, false positive, policy violation minor	24 jam	Tim Infrastruktur

8. BAGAN ALUR (FLOWCHART) KEAMANAN DATA

A. Flowchart Penanganan Insiden Keamanan



B. Flowchart Vulnerability Management



9. PERLENGKAPAN

1. *Firewall (Hardware/Software)*
2. *Antivirus/Antimalware Enterprise*
3. *IDS/IPS (Intrusion Detection/Prevention System)*
4. *SIEM (Security Information and Event Management)*
5. *Vulnerability Scanner (Nessus, OpenVAS, dll)*
6. *Tools Enkripsi*
7. *SSL/TLS Certificates*
8. *VPN untuk remote access*
9. *Log Management System*
10. *Komputer admin dan ATK*

10. FORMULIR KEGIATAN

No	*Nama Formulir*	*Kode Formulir*
1	*Form Laporan Insiden Keamanan*	*PPTIK/FM/013*
2	*Form Klasifikasi Insiden*	*PPTIK/FM/014*
3	*Form Laporan Investigasi Insiden*	*PPTIK/FM/015*
4	*Form Berita Acara Pemulihan Insiden*	*PPTIK/FM/016*
5	*Form Laporan Vulnerability Scan*	*PPTIK/FM/017*
6	*Form Checklist Audit Keamanan*	*PPTIK/FM/018*
7	*Form Post-Incident Review*	*PPTIK/FM/019*

11. PENUTUP

Standard Operating Procedure (SOP) ini ditujukan bagi seluruh staf PPTIK dan unit terkait di lingkungan kampus Universitas Muhammadiyah Mataram dalam rangka menjaga keamanan data dan sistem informasi universitas.

Selanjutnya dalam implementasinya dapat menyesuaikan dengan kondisi dan ketentuan yang berlaku di lingkungan PPTIK dan dapat menyusun petunjuk pelaksanaan dan petunjuk teknis atau ketentuan lain yang bersifat teknis operasional dalam penyelenggaraan kegiatan.

Dibuat/Diajukan Oleh	*Diperiksa Oleh*	*Disetujui Oleh*
Programmer PPTIK	**Kepala PPTIK**	**Wakil Rektor I**
Tanggal: ……	*Tanggal: ……*	*Tanggal: ……*