STANDAR OPERASIONAL PROSEDUR

PENANGANAN GANGGUAN JARINGAN (INCIDENT RESPONSE)

DOKUMEN SOP	
Nomor SOP	*008/PPTIK/SOP/2024*
Tanggal Pembuatan	*15 Desember 2021*
Tanggal Revisi	*01 Desember 2024*
Tanggal Efektif	*01 Januari 2025*
Edisi/Revisi	*01*
Halaman	*1 dari 10*

UNIVERSITAS MUHAMMADIYAH MATARAM

PUSAT PENGEMBANGAN TEKNOLOGI INFORMASI DAN KOMUNIKASI (PPTIK)

Terakreditasi B

Alamat: *Jl. KH. Ahmad Dahlan No. 1, Pagesangan, Mataram, NTB 83127*
Telepon: *(0370) 633723* | **Fax:** *(0370) 633723*
Email: *pptik@ummat.ac.id* | **Website:** *https://pptik.ummat.ac.id*

LEMBAR PENGESAHAN

Jabatan	*Nama*	*Tanda Tangan*	*Tanggal*
Dibuat oleh:*Koordinator Jaringan*	*Nova kurniawan*	……	*……/……/2024*
Diperiksa oleh:*Kepala Divisi Infrastruktur*	*Nova kurniawan*	……	*……/……/2024*
Disahkan oleh:*Kepala PPTIK*	*M.Rizkillah*	……	*……/……/2024*

1. TUJUAN

Prosedur ini bertujuan untuk: 1. Menyediakan framework penanganan insiden jaringan yang terstruktur 2. Meminimalkan dampak dan waktu downtime layanan 3. Memastikan response time sesuai SLA berdasarkan severity 4. Melakukan root cause analysis untuk pencegahan 5. Mendokumentasikan lessons learned untuk improvement

2. RUANG LINGKUP

SOP ini mencakup: - Deteksi dan identifikasi insiden jaringan - Klasifikasi dan prioritisasi insiden - Penanganan dan resolusi insiden - Eskalasi dan komunikasi stakeholder - Root cause analysis dan post-mortem - Dokumentasi dan knowledge base

3. DEFINISI

Istilah	*Definisi*
Incident	*Kejadian yang mengganggu atau berpotensi mengganggu layanan*
Severity	*Tingkat keparahan berdasarkan dampak dan urgensi*
MTTR	*Mean Time to Repair, rata-rata waktu perbaikan*
RCA	*Root Cause Analysis, analisis akar penyebab*
Workaround	*Solusi sementara untuk memulihkan layanan*
Resolution	*Solusi permanen untuk mengatasi masalah*
Post-Mortem	*Review mendalam setelah insiden major*
SLA	*Service Level Agreement, perjanjian tingkat layanan*

4. REFERENSI

1. *UU No. 11 Tahun 2008 jo. UU No. 19 Tahun 2016 tentang ITE*
2. *ISO/IEC 27001:2022 tentang ISMS*
3. *ITIL v4 Incident Management Practice*
4. *NIST Cybersecurity Framework*
5. *Kebijakan Penanganan Insiden PPTIK*

5. PENANGGUNG JAWAB

No	*Jabatan*	*Tanggung Jawab*
1	*Kepala PPTIK*	*Incident Commander untuk P1*
2	*Koordinator Jaringan*	*Incident Manager*
3	*Network Administrator*	*Technical Lead*
4	*NOC Operator*	*First Responder*
5	*Network Technician*	*Field Support*

No	Jabatan	Tanggung Jawab
6	Communication Officer	Stakeholder Communication

6. KLASIFIKASI INSIDEN

6.1 Severity Level

Severity	Nama	Kriteria	Dampak
P1	Critical	Outage total, seluruh kampus terdampak	≥ 1000 users
P2	High	Outage major, satu gedung/fakultas	100-999 users
P3	Medium	Degradasi layanan, beberapa unit	10-99 users
P4	Low	Gangguan minor, individual user	1-9 users

6.2 Response Time & Resolution Target

Severity	Response Time	Target Resolution	Eskalasi
P1	5 menit	1 jam	Immediate ke Kepala PPTIK
P2	15 menit	4 jam	30 menit ke Koordinator
P3	30 menit	8 jam	2 jam ke Network Admin
P4	1 jam	24 jam	8 jam ke Network Admin

7. PROSEDUR

7.1 Deteksi dan Penerimaan Laporan

No	Aktivitas	Pelaksana	Waktu	Output	Dokumen
1	Deteksi via NMS alert atau laporan user	NOC Operator	Real-time	Alert/Ticket	FM_NET_022
2	Log insiden di ticketing system	NOC Operator	2 menit	Ticket ID	FM_NET_022
3	Gather initial information	NOC Operator	5 menit	Initial Data	FM_NET_022
4	Verify dan validate issue	NOC Operator	5 menit	Confirmed Issue	-
5	Klasifikasi severity level	NOC Operator	2 menit	Severity	FM_NET_022
6	Assign ke resolver team	NOC Operator	2 menit	Assignment	FM_NET_022

7.2 Diagnosis dan Investigasi

No	Aktivitas	Pelaksana	Waktu	Output	Dokumen
1	Review alert history dan log	Network Admin	10 menit	Log Data	-
2	Identifikasi scope dampak	Network Admin	10 menit	Impact Scope	FM_NET_023
3	Isolasi masalah (physical/logical)	Network Admin	15 menit	Problem Area	-
4	Check known error database	Network Admin	5 menit	Known Issue?	-
5	Koordinasi dengan tim terkait	Network Admin	As needed	Team Aligned	-
6	Determine root cause hypothesis	Network Admin	15 menit	Hypothesis	FM_NET_023

7.3 Resolusi dan Recovery

No	Aktivitas	Pelaksana	Waktu	Output	Dokumen
1	Implement workaround (jika ada)	Network Admin	Varies	Service Restored	FM_NET_024
2	Apply permanent fix	Network Admin	Varies	Issue Resolved	FM_NET_024
3	Verify service restoration	Network Admin	10 menit	Verification	FM_NET_024
4	Monitor pasca perbaikan	NOC Operator	1 jam	Stable Status	-
5	Konfirmasi ke user/affected party	Comm Officer	10 menit	User Confirmed	-
6	Update ticket status	NOC Operator	5 menit	Ticket Updated	FM_NET_022

7.4 Eskalasi

No	Aktivitas	Pelaksana	Trigger	Output	Dokumen
1	Eskalasi L1 → L2	NOC Operator	Tidak resolve 15 menit	Escalated	FM_NET_025
2	Eskalasi L2 → L3	Network Admin	Tidak resolve atau P1/P2	Escalated	FM_NET_025
3	Eskalasi ke vendor	Koordinator	Hardware failure	Vendor Ticket	FM_NET_025
4	Eskalasi ke	Koordinator	P1 atau	Mgmt	FM_NET_025

No	Aktivitas	Pelaksana	Trigger	Output	Dokumen
	manajemen		dampak besar	Informed	
5	Aktivasi crisis team (jika P1)	Kepala PPTIK	P1 > 30 menit	Crisis Mode	-

7.5 Komunikasi

Severity	Stakeholder	Channel	Frequency
P1	All stakeholders, Rektorat	Email, WA Group, Portal	Every 30 menit
P2	Affected unit, Kepala PPTIK	Email, WA	Every 1 jam
P3	Affected users	Email, Ticket update	At resolution
P4	Reporter only	Ticket update	At resolution

7.6 Post-Incident Review

No	Aktivitas	Pelaksana	Waktu	Output	Dokumen
1	Complete incident documentation	Network Admin	24 jam	Full Report	FM_NET_026
2	Root Cause Analysis (P1/P2)	Koordinator	3 hari	RCA Report	FM_NET_027
3	Post-mortem meeting (P1)	All stakeholders	5 hari	Meeting Notes	FM_NET_028
4	Identify preventive actions	Koordinator	5 hari	Action Items	FM_NET_028
5	Update knowledge base	Network Admin	7 hari	KB Updated	-
6	Implement improvements	Assigned	Per timeline	Improvements	FM_NET_029

8. INCIDENT RESPONSE TEAM (IRT)

8.1 P1 Crisis Team Composition

Role	Person	Responsibility
Incident Commander	Kepala PPTIK	Keputusan strategis
Incident Manager	Koordinator Jaringan	Koordinasi response
Technical Lead	Network Admin Senior	Penanganan teknis
Communication Lead	Comm Officer	Komunikasi stakeholder
Scribe	Staff Admin	Dokumentasi

8.2 Contact List

Role	*Primary*	*Backup*	*Phone*
Kepala PPTIK	*[Nama]*	*[Nama]*	*[No HP]*
Koordinator	*[Nama]*	*[Nama]*	*[No HP]*
NOC	*On-duty*	*Shift backup*	*[No HP]*

9. KNOWN ERROR DATABASE (KEDB)

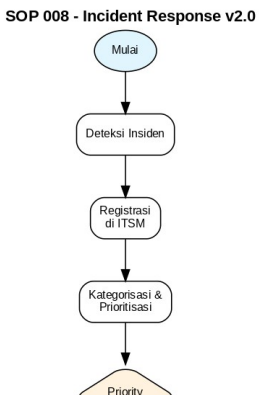
Dokumentasi masalah yang sudah pernah terjadi dan solusinya untuk mempercepat resolusi di kemudian hari.

Error Code	*Symptom*	*Root Cause*	*Resolution*	*MTTR*
NET-001	*No connectivity*	*Kabel putus*	*Ganti kabel*	*30m*
NET-002	*Slow connection*	*Bandwidth full*	*QoS/Limit user*	*15m*
NET-003	*Intermittent*	*Port flapping*	*Config/Ganti port*	*45m*
[dst]	*...*	*...*	*...*	*...*

10. KEY PERFORMANCE INDICATORS

KPI	*Target*	*Pengukuran*
First Call Resolution	*≥ 70%*	*Monthly*
MTTR P1	*≤ 1 jam*	*Per incident*
MTTR P2	*≤ 4 jam*	*Per incident*
Incident Recurrence	*≤ 5%*	*Monthly*
SLA Compliance	*≥ 95%*	*Monthly*
Customer Satisfaction	*≥ 4.0/5.0*	*Survey*

11. FLOWCHART



12. DOKUMEN TERKAIT

Kode	*Nama Form*	*Fungsi*
FM_NET_022	*Form Laporan Insiden Jaringan*	*Registrasi insiden*
FM_NET_023	*Form Investigation Worksheet*	*Lembar investigasi*
FM_NET_024	*Form Resolution Log*	*Log resolusi*
FM_NET_025	*Form Escalation Record*	*Catatan eskalasi*
FM_NET_026	*Form Incident Report*	*Laporan lengkap*
FM_NET_027	*Form Root Cause Analysis*	*Template RCA*
FM_NET_028	*Form Post-Mortem Meeting*	*Notulen post-mortem*
FM_NET_029	*Form Improvement Action*	*Tracking improvement*

13. CATATAN REVISI

Revisi	*Tanggal*	*Uraian Perubahan*	*Oleh*
00	*15/12/2021*	*Dokumen awal*	*Tim PPTIK*
01	*01/12/2024*	*Penambahan: severity classification, SLA targets, RCA process, post-mortem, KEDB, crisis team, communication matrix, KPI*	*Tim PPTIK*