SOP Monitoring dan Troubleshooting Jaringan

1. Tujuan

Menetapkan tata cara pemantauan dan penanganan gangguan jaringan agar ketersediaan (availability), keamanan (security), dan kinerja (performance) jaringan kampus tetap optimal dan sesuai standar layanan TI, serta menyediakan transparansi status layanan kepada publik melalui laman status resmi kampus.

2. Ruang Lingkup

SOP ini mencakup kegiatan:

- Pemantauan kondisi perangkat dan layanan jaringan;
- Deteksi dini gangguan serta notifikasi otomatis;
- Penanganan insiden dan troubleshooting;
- Pelaporan status jaringan internal dan publik (melalui laman status);
- Dokumentasi hasil serta tindak lanjut perbaikan.

3. Penanggung Jawab

Jabatan	Tanggung Jawab
Network Administrator	Melakukan pemantauan dan penanganan gangguan jaringan
Kepala STK	Persetujuan perubahan dan eskalasi
Helpdesk / IT Support	Penerima laporan awal dan eskalasi insiden

4. Referensi

- Kebijakan Keamanan Jaringan Kampus
- Situs status jaringan kampus: https://usscampus.instatus.com/

5. Peralatan dan Aplikasi

- Network Monitoring: Cacti, The Dude.
- Logging: Syslog, Graylog, atau ELK Stack.
- Portal Status Publik: Instatus — usscampus.instatus.com.
- Tools Diagnostik: ping, traceroute, mtr, iperf3, nmap.
- Tiket & Dokumentasi: Helpdesk, Knowledgebase internal.

6. Prosedur

6.1 Monitoring Jaringan

1. Konfigurasi Sistem Monitoring
    - Setiap perangkat jaringan dikonfigurasi dengan SNMP, Syslog, dan ICMP aktif.
    - Threshold (ambang batas alert):
        - CPU > 85% (warning), >95% (critical)
        - Memory > 90%
        - Link down > 3 menit → alert otomatis
    - Notifikasi dikirim ke grup admin (email & Telegram).
2. Pemantauan Harian

- Cek dashboard monitoring pagi dan sore.
- Pastikan semua router, switch, AP, dan server aktif.
- Lakukan review mingguan untuk tren trafik dan uptime.

3. Publikasi Status
    - Status jaringan dan layanan penting (internet, OJS, e-learning, email kampus, dsb) ditampilkan di laman: https://usscampus.instatus.com
    - Setiap gangguan berdampak publik wajib diperbarui statusnya dalam waktu maksimal 30 menit sejak insiden terdeteksi.

6.2 Deteksi dan Notifikasi Gangguan

1. Sistem monitoring atau pengguna melaporkan gangguan.
2. Admin memverifikasi dengan:
    - Ping IP perangkat,
    - Cek syslog,
    - Validasi status pada controller (Mikrotik, UniFi, dll).
3. Jika gangguan berskala luas → update laman status publik.
4. Jika gangguan lokal → tindak lanjut tanpa publikasi.

6.3 Prosedur Troubleshooting

Tahap	Kegiatan	Tools/Referensi
1. Identifikasi	Tentukan lokasi dan jenis gangguan	ping, traceroute, monitoring
2. Isolasi	Pisahkan perangkat atau segmen yang bermasalah	CLI/web interface
3. Analisis	Cek log, bandwidth, konfigurasi	Syslog, Grafana
4. Perbaikan	Reboot/ganti perangkat, reset koneksi, restore konfigurasi	sesuai kasus
5. Verifikasi	Pastikan layanan normal	mtr, iperf3, portal status
6. Dokumentasi	Catat waktu, penyebab, tindakan, hasil	log insiden

6.4 Eskalasi Gangguan

Level	Jenis Gangguan	Penanganan	Publikasi Status
Level 1 (Minor)	1–2 pengguna	IT Support	Tidak perlu
Level 2 (Moderate)	1 perangkat jaringan	Network Admin	Opsional
Level 3 (Major)	1 segmen/gedung down	Admin + Kepala Divisi	Ya, di Instatus
Level 4 (Critical)	Internet kampus / layanan utama down	Admin + Vendor	Wajib publikasi di Instatus

6.5 Pemulihan dan Dokumentasi

1. Setelah pulih, lakukan Root Cause Analysis (RCA).
2. Update status di laman Instatus ke *Resolved*.
3. Catat langkah perbaikan dan pencegahan di log internal.
4. Sertakan laporan bulanan untuk Kepala STK.

7. Dokumentasi

- Log monitoring & syslog.
- Laporan insiden.
- Rekap status publik (Instatus).
- Topologi jaringan.
- Backup konfigurasi perangkat.

8. Catatan

- Uptime target jaringan kampus: ≥ 99% per bulan.
- Update laman Instatus maksimal 30 menit setelah insiden terdeteksi.
- Semua laporan publik harus disetujui oleh Kepala STK sebelum diumumkan.