

SOP Pengelolaan Wi-Fi Kampus (SSID, Keamanan, dan Bandwidth)

1. Tujuan

Menetapkan standar operasional dalam pengelolaan jaringan Wi-Fi kampus agar seluruh civitas akademika dapat mengakses jaringan nirkabel dengan aman, stabil, dan terkontrol sesuai kebijakan penggunaan sumber daya teknologi informasi.

2. Ruang Lingkup

SOP ini mencakup seluruh aktivitas pengelolaan jaringan Wi-Fi di area kampus, meliputi:

- Desain dan konfigurasi SSID (student, staff, guest, dan admin);
- Manajemen keamanan dan autentikasi pengguna;
- Pengaturan bandwidth, QoS, dan pemantauan trafik;
- Pemeliharaan perangkat Access Point (AP);
- Dokumentasi dan pelaporan performa jaringan.

3. Penanggung Jawab

Jabatan	Tugas
Administrator Jaringan (Network Admin)	Instalasi, konfigurasi, dan pemantauan Wi-Fi
Kepala STK	Persetujuan konfigurasi dan kebijakan akses
Tim IT Support	Penanganan keluhan pengguna dan perawatan perangkat

4. Referensi

- Standar keamanan jaringan IEEE 802.11.
- Kebijakan keamanan TI kampus.

5. Peralatan dan Perangkat

- Access Point (Cisco, Mikrotik, TP-Link dll).
- Wireless Controller (jika sistem terpusat).
- Laptop admin (dengan aplikasi manajemen AP).
- Network monitoring tools (Grafana, atau The Dude).
- Alat uji sinyal (Wi-Fi Analyzer, NetSpot).

6. Prosedur

6.1 Desain dan Konfigurasi SSID

1. Penentuan SSID

- Gunakan nama SSID yang konsisten dan mudah diidentifikasi, misalnya:
 - Universitas Sumatera Selatan (akses public mahasiswa dan tamu)
 - USS-Office (akses staf dan dosen)
 - USS-Admin (khusus teknisi jaringan)
- Hindari penggunaan SSID generik seperti “default” atau “linksys”.

2. Segmentasi VLAN

- Setiap SSID wajib terhubung ke VLAN terpisah.
- VLAN Admin hanya bisa diakses oleh perangkat IT.
- 3. Autentikasi Pengguna
 - Gunakan sistem autentikasi

6.2 Pengaturan Keamanan Wi-Fi

1. Gunakan WPA dengan dukungan keamanan terbaru
2. Nonaktifkan SSID broadcast untuk jaringan admin/internal.
3. Batasi jumlah koneksi per user (misal: 3 perangkat maksimum).
4. Gunakan MAC filtering untuk perangkat kritis (server, AP manajemen).
5. Update firmware access point secara berkala.
6. Nonaktifkan remote management dari jaringan publik.
7. Catat seluruh konfigurasi keamanan dan backup secara rutin.

6.3 Pengelolaan Bandwidth dan QoS

1. Gunakan fitur Smart Queue / Bandwidth Control / Simple Queue di router utama.
2. Prioritaskan trafik akademik (e-learning, repository, jurnal) dibanding sosial media/video streaming.
3. Monitor penggunaan bandwidth dan lakukan penyesuaian sesuai laporan bulanan.

6.4 Pemeliharaan Jaringan Wi-Fi

1. Harian
 - Pantau status access point dan pengguna aktif.
 - Tindak cepat jika ada AP offline atau lonjakan trafik.
 - Cek notifikasi dari sistem monitoring.
2. Mingguan
 - Lakukan uji kecepatan di beberapa titik area kampus.
 - Periksa sinyal lemah (RSSI < -70 dBm).
 - Bersihkan perangkat dari debu.
3. Bulanan
 - Update firmware AP & controller.
 - Review log keamanan (login gagal, brute force, dll).
 - Backup konfigurasi semua AP.
4. Tahunan
 - Evaluasi distribusi AP (heatmap coverage).
 - Uji kapasitas kanal dan interferensi.
 - Rekomendasikan upgrade perangkat jika diperlukan.

6.5 Penanganan Gangguan

1. Terima laporan dari helpdesk/tiket.
2. Identifikasi lokasi dan SSID yang terdampak.
3. Periksa status AP dan koneksi backhaul.
4. Lakukan reboot, reset konfigurasi, atau penggantian perangkat jika perlu.
5. Dokumentasikan penyebab dan tindakan perbaikan di log jaringan

7. Dokumentasi

- Data SSID dan VLAN Mapping.
- Log aktivitas pengguna
- Laporan bulanan performa Wi-Fi.
- Backup konfigurasi perangkat.
- Heatmap coverage area kampus.

8. Catatan

- Perubahan konfigurasi SSID hanya boleh dilakukan oleh Network Admin dengan persetujuan Kepala STK.
- Semua aktivitas pemeliharaan wajib tercatat dalam log monitoring.