



PEMERINTAH PROVINSI SULAWESI SELATAN
DINAS KOMUNIKASI, INFORMATIKA, STATISTIK DAN PERSANDIAN

Jl. Urip Sumoharjo No. 269, Panaikang, Kecamatan Panakkukang, Kota Makassar, Sulawesi Selatan 90231

Nomor SOP	SOP-IT-SULSEL-002
Tanggal Pembuatan	
Tanggal Revisi	– (Revisi 00)
Tanggal Efektif	
Disahkan Oleh	Kepala Dinas Komunikasi, Informatika, Statistik dan Persandian Provinsi Sulawesi Selatan, ... NIP.
Nama SOP	Penanganan Gangguan Jaringan

Dasar Hukum

1. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 1 Tahun 2024;
2. Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi;
3. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik;
4. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik;
5. Peraturan Presiden Nomor 82 Tahun 2022 tentang Pelindungan Infrastruktur Informasi Vital;
6. Peraturan Presiden Nomor 132 Tahun 2022 tentang Arsitektur Sistem Pemerintahan Berbasis Elektronik Nasional;
7. Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2020 tentang Sistem Pengamanan dalam Penyelenggaraan Sistem Elektronik;
8. Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi SPBE dan Standar Teknis dan Prosedur Keamanan SPBE;
9. Peraturan Badan Siber dan Sandi Negara Nomor 1 Tahun 2024 tentang Pengelolaan Insiden Siber;
10. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 35 Tahun 2012 tentang Pedoman Penyusunan Standar Operasional Prosedur Administrasi Pemerintahan;
11. Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Nomor 59 Tahun 2020 tentang Pemantauan dan Evaluasi Sistem Pemerintahan Berbasis Elektronik;
12. Peraturan Gubernur Sulawesi Selatan tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik [nomor dan tahun diisi sesuai peraturan yang berlaku].

Kualifikasi Pelaksana

1. Memahami topologi dan konfigurasi jaringan, meliputi routing, switching, firewall, VPN, DNS, dan DHCP;
2. Mampu melakukan diagnosa gangguan jaringan secara berlapis dan menggunakan sistem pemantauan jaringan;
3. Memahami prosedur penanganan insiden keamanan siber dan pengamanan bukti;
4. Mampu mengoperasikan sistem helpdesk serta berkomunikasi dengan pengguna, ISP, dan vendor.

Keterkaitan

1. SOP-IT-SULSEL-001 tentang Penyediaan dan Pengelolaan Layanan Jaringan;
2. SOP-IT-SULSEL-003 tentang Penyediaan dan Pengelolaan Layanan Server Virtual bagi Perangkat Daerah;
3. SOP-IT-SULSEL-004 tentang Pengembangan dan Integrasi Aplikasi.

Peralatan/Perlengkapan

1. Sistem helpdesk dan pencatatan tiket;
2. Sistem pemantauan jaringan dan server log terpusat;
3. Perangkat diagnosa: laptop, kabel konsol, penguji kabel, dan pengukur daya optik atau OTDR;
4. Perangkat cadangan: switch, modul SFP, dan access point;
5. Saluran komunikasi resmi: telepon, surat elektronik, dan WhatsApp helpdesk;
6. Formulir Laporan Gangguan (Lampiran 1) dan Matriks Eskalasi dan Daftar Kontak (Lampiran 2).

Peringatan

Apabila SOP ini tidak dilaksanakan, gangguan jaringan dapat berlangsung melampaui target pemulihan dan mengganggu layanan publik serta operasional Perangkat Daerah, bukti insiden keamanan siber dapat hilang, dan kewajiban pelaporan insiden kepada Badan Siber dan Sandi Negara tidak terpenuhi. Perangkat yang diduga terkena serangan tidak boleh dimulai ulang sebelum log dan bukti diamankan.

Pencatatan dan Pendataan

Setiap gangguan dicatat sebagai tiket pada sistem helpdesk. Formulir Laporan Gangguan, review pasca-insiden, dan laporan bulanan disimpan secara elektronik sekurang-kurangnya 2 (dua) tahun sebagai bahan pemantauan dan evaluasi SPBE.

Alur Penanganan Gangguan Jaringan

Urutan langkah sejak gangguan jaringan terjadi sampai tiket ditutup dan dikaji. Setiap gangguan dicatat sebagai tiket, diprioritaskan, ditangani sesuai target waktu, dan dieskalasi bila target terlampaui. Diagram alir lengkap ada di halaman 3.

Notifikasi awal P1/P2 ≤ 30 menit

Tiket ke ISP ≤ 15 menit

Lapor CSIRT ≤ 1 jam

RCA P1 ≤ 5 hari kerja

1. Prioritas dan target waktu

Angka 4.2; sama dengan angka 13.2 SOP-IT-SULSEL-003. Di luar jam helpdesk (08.00–16.00 WITA), P1 dan P2 ditangani petugas piket.

Prioritas	Contoh gangguan	Respons	Pemulihan	Pembaruan
P1 – Kritis	Internet putus total; switch inti, firewall, atau router batas gagal; konektivitas Data Center putus	15 menit	4 jam	Tiap 30 menit
P2 – Tinggi	Satu OPD terputus; VPN tidak berfungsi; access point beberapa area mati	30 menit	8 jam	Tiap 2 jam
P3 – Sedang	Latensi tinggi, packet loss, kecepatan menurun	4 jam	2 hari kerja	Tiap hari kerja
P4 – Rendah	Satu pengguna dengan solusi sementara; perangkat non-produksi	1 hari kerja	5 hari kerja	Saat selesai

2. Eskalasi berbasis waktu

Tingkat	Penanggung jawab	Pemicu
Tingkat 1	Administrator Jaringan / piket	Sejak tiket ditugaskan
Tingkat 2	Koordinator Tim Infrastruktur	Belum tertangani dalam 50% target pemulihan
Tingkat 3	Kepala Bidang Infrastruktur TIK	Target pemulihan terlampaui, atau gangguan besar
Tingkat 4	Kepala Dinas	Berdampak luas atau melebihi 2× target pemulihan

3. Insiden keamanan siber

- Lapor Tim Keamanan / SULSELPROV-CSIRT paling lambat 1 jam.
- Batasi dampak: isolasi segmen, blokir sumber serangan.
- Amankan log dan konfigurasi **sebelum** restart perangkat.
- CSIRT melapor ke BSSN; kebocoran data pribadi diberitahukan 3×24 jam.

4. Batas tanggung jawab

- Diskominfo-SP: jaringan sampai perangkat terminasi di lokasi OPD.
- OPD: LAN internal, access point milik OPD, dan perangkat pengguna.
- ISP: tautan internet sesuai kontrak; tiket dibuka Diskominfo-SP.
- Server dan aplikasi: dialihkan ke SOP-003 dan SOP-004.

