LAPORAN PENANGANAN KEJADIAN DAN INSIDEN SIBER RSUD KABUPATEN TEMANGGUNG

PERIODE JANUARI S.D. JULI 2026

RSUD KABUPATEN TEMANGGUNG

I. PENDAHULUAN

Perkembangan teknologi informasi di RSUD Kabupaten Temanggung yang mencakup Sistem Informasi Manajemen Rumah Sakit (SIMRS), Rekam Medis Elektronik (RME), Anjungan Pasien Mandiri (APM), serta integrasi layanan digital dan media publik membawa konsekuensi logis terhadap peningkatan risiko kerentanan keamanan siber.

Pelindungan terhadap kerahasiaan, integritas, dan ketersediaan data serta infrastruktur elektronik menjadi prioritas utama manajemen. Berdasarkan hal tersebut, Instalasi SIMRS bersama unit terkait secara berkala melakukan pemantauan, deteksi dini, serta penanganan terhadap potensi anomali maupun insiden siber guna memastikan kesinambungan layanan kesehatan bagi masyarakat.

II. TUJUAN PELAPORAN

1. Memberikan gambaran komprehensif mengenai keamanan sistem elektronik dan jaringan di RSUD Kabupaten Temanggung selama semester pertama tahun 2026.
2. Mendokumentasikan rekapitulasi kejadian, anomali, maupun insiden siber yang terdeteksi beserta langkah penanganan dan mitigasinya.
3. Menjadi bahan evaluasi dan perbaikan berkelanjutan terhadap standar pengamanan sistem informasi sesuai dengan SNI ISO/IEC 27001 dan Peraturan BSSN No. 8 Tahun 2020.

III. REKAPITULASI PENANGANAN KEJADIAN & INSIDEN SIBER

Selama periode Januari s.d. Juli 2026, tercatat kondisi keamanan siber sebagai berikut:

Januari 2026

- Klasifikasi: Percobaan pemindaian port dan akses tidak sah dari IP eksternal pada server publik.
- Dampak: Rendah / Tidak ada gangguan layanan.
- Tindakan: Pemblokiran otomatis oleh firewall dan pengetatan aturan akses jaringan luar.
- Status: Selesai / Aman.

Februari 2026

- Klasifikasi: Lonjakan trafik sesaat (micro-DDoS) pada website resmi.
- Dampak: Rendah / Gangguan sesaat (< 15 menit).
- Tindakan: Aktivasi filter proteksi trafik server hosting dan pemantauan jaringan.
- Status: Selesai / Normal.

Maret 2026

- Klasifikasi: Deteksi malware lokal pada PC unit pelayanan akibat media penyimpanan luar.
- Dampak: Sedang / Terisolasi pada 1 unit PC.
- Tindakan: Isolasi perangkat, pembersihan sistem (deep cleaning), dan pemulihan data backup bersih.
- Status: Selesai / Teratasi.

April 2026

- Klasifikasi: Percobaan phishing/tautan palsu kepada beberapa staf.
- Dampak: Rendah / Nihil kerugian data.
- Tindakan: Edukasi cepat kepada staf dan pengaktifan Multi-Factor Authentication (MFA).
- Status: Selesai / Aman.

Mei 2026

- Klasifikasi: Pemeliharaan berkala dan patching celah keamanan server utama SIMRS.
- Dampak: Preventif (Pencegahan).
- Tindakan: Penerapan patch update resmi untuk menutup celah kerentanan.
- Status: Selesai / Aman.

Juni 2026

- Klasifikasi: Anomali percobaan akses dasbor media sosial dari lokasi tidak dikenal.
- Dampak: Rendah / Nihil kebocoran.
- Tindakan: Force logout semua sesi aktif, ganti password, dan aktivasi verifikasi dua langkah.
- Status: Selesai / Aman.

Juli 2026

- Klasifikasi: Pemeriksaan integritas basis data dan evaluasi fail-over backup RME.
- Dampak: Preventif (Pencegahan).
- Tindakan: Validasi backup data harian untuk memastikan pemulihan darurat.
- Status: Selesai / Aman.

Kesimpulan Rekapitulasi: Tidak ditemukan insiden kebocoran data pasien yang massif atau peretasan fatal. Sebagian besar insiden berskala rendah hingga menengah dan berhasil ditangani dengan cepat.

IV. ANALISIS & EVALUASI KEAMANAN SIBER

1. Efektivitas Sistem Pertahanan: Firewall dan perangkat jaringan terbukti aktif mendeteksi dan memblokir intrusi luar.
2. Kontrol Akses: Penerapan Role-Based Access Control (RBAC) menekan risiko eksploitasi akun internal.
3. Kesadaran Pegawai: Faktor human error masih menjadi tantangan yang perlu ditekan melalui edukasi rutin.Sebagai wujud komitmen nyata manajemen, kebijakan keamanan siber dan PDP ini dilegalkan melalui kerangka hukum internal rumah sakit.

V. RENCANA TINDAK LANJUT & REKOMENDASI

1. Peningkatan kapasitas teknis pengelolaan IT terkait respons cepat tanggap darurat insiden siber.
2. Pelaksanaan Vulnerability Assessment secara rutin pada infrastruktur server SIMRS dan aplikasi publik.
3. Penguatan sosialisasi keamanan informasi dan pencegahan social engineering bagi seluruh pegawai.