

**KEBIJAKAN KEAMANAN INFORMASI &
PELINDUNGAN DATA PRIBADI (PDP)
RSUD KABUPATEN TEMANGGUNG
TAHUN 2026**



RSUD KABUPATEN TEMANGGUNG

I. LATAR BELAKANG

Dalam era digitalisasi layanan kesehatan, RSUD Kabupaten Temanggung mengandalkan Sistem Informasi Manajemen Rumah Sakit (SIMRS), anjungan pasien mandiri (APM), rekam medis elektronik (RME), serta pengelolaan kanal pengaduan dan media digital secara terintegrasi.

Transformasi ini menuntut jaminan keamanan informasi yang ketat guna melindungi kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability) data pasien, data medis, serta data administratif rumah sakit. Oleh karena itu, diperlukan kebijakan tata kelola keamanan siber dan perlindungan data pribadi yang merujuk pada SNI ISO/IEC 27001 serta Peraturan Badan Siber dan Sandi Negara (BSSN) Nomor 8 Tahun 2020 tentang Pengamanan Sistem Elektronik.

II. KERANGKA ACUAN & RUANG LINGKUP KEBIJAKAN

Kebijakan keamanan informasi ini mencakup tiga pilar utama keamanan siber di lingkungan RSUD Kabupaten Temanggung:

- 1. Keamanan Data Pasien & Medis (Rekam Medis Elektronik / RME): Menjaga privasi pasien dari akses ilegal, kebocoran data, atau modifikasi data tanpa izin.
- 2. Keamanan Infrastruktur Jaringan & SIMRS: Melindungi perangkat keras, server lokal/cloud, jaringan internet/intranet rumah sakit dari ancaman siber (ransomware, malware, ddos).
- 3. Kepatuhan Regulasi & Pelindungan Data Pribadi (PDP): Menyelaraskan tata kelola data dengan standar operasional keamanan informasi nasional.

III. MATRIKS KEBIJAKAN KEAMANAN INFORMASI & PDP

No.	Aspek Tata Kelola	Acuan Standar (ISO 27001 / Peraturan BSSN No. 8/2020)	Implementasi Kebijakan di RSUD Kabupaten Temanggung
1.	Kebijakan Kontrol Akses (Access Control)	• SNI ISO/IEC 27001 (Klausul A.9) • Peraturan BSSN No. 8/2020	• Penerapan hak akses SIMRS berbasis peran (Role-Based Access Control / RBAC) di setiap instalasi (misal: tenaga medis hanya bisa mengakses rekam medis pasien di unitnya). • Kewajiban penggantian password akun sistem secara berkala minimal 3 bulan sekali serta penerapan strong password.
2.	Keamanan Perangkat & Jaringan (Endpoint & Network Security)	• SNI ISO/IEC 27001 (Klausul A.12 & A.13) • Peraturan BSSN No. 8/2020	• Instalasi perangkat lunak antivirus/antimalware resmi yang terpusat dan diperbarui otomatis pada seluruh komputer unit pelayanan. • Pemisahan jaringan (Network Segmentation) antara jaringan publik (Wi-Fi pasien) dengan jaringan operasional internal/medis yang krusial.
3.	Manajemen Cadangan Data (Backup & Recovery)	• SNI ISO/IEC 27001 (Klausul A.12.3) • Peraturan BSSN No. 8/2020	• Pelaksanaan pencadangan data (backup) basis data SIMRS dan rekam medis secara rutin (harian/mingguan) dengan skema local & off-site backup untuk mengantisipasi kegagalan sistem atau serangan siber.
4.	Pelindungan Data Pribadi (PDP) Pasien	• Undang-Undang Pelindungan Data Pribadi • SNI ISO/IEC 27001 (Klausul A.18)	• Larangan keras menyebarluaskan rekam medis, identitas, atau foto pasien ke media sosial pribadi tanpa persetujuan tertulis (informed consent). • Enkripsi data sensitif pasien pada penyimpanan digital rumah sakit.

5.	Penanganan Insiden Keamanan Siber (Incident Management)	• SNI ISO/IEC 27001 (Klausul A.16) • Peraturan BSSN No. 8/2020	• Pembentukan mekanisme tanggap darurat siber oleh Tim Instalasi SIMRS berkoordinasi dengan BSSN/CSIRT daerah jika terjadi gangguan sistem atau peretasan. • Pelaporan insiden secara berjenjang kepada Direksi rumah sakit.
----	---	--	--

IV. PENGINTEGRASIAN KE DALAM REGULASI INTERNAL

Sebagai wujud komitmen nyata manajemen, kebijakan keamanan siber dan PDP ini dilegalkan melalui kerangka hukum internal rumah sakit:

1. Penerbitan SK Direktur tentang Kebijakan Keamanan Informasi
 - Bentuk Kebijakan: Keputusan Direktur RSUD Kabupaten Temanggung tentang Pedoman Tata Kelola Keamanan Informasi, SIMRS, dan Pelindungan Data Pribadi Tahun 2026.
 - Muatan Utama: Menetapkan bahwa setiap pegawai (baik tenaga medis maupun non-medis) bertanggung jawab penuh terhadap kerahasiaan user ID masing-masing dan wajib menjaga kerahasiaan data pasien sesuai ketentuan perundang-undangan.
2. Penyusunan SOP Pendukung Keamanan Siber
 - Judul SOP: SOP Penanganan Insiden Keamanan Sistem Informasi dan Pelindungan Data Pasien di RSUD Kabupaten Temanggung.
 - Poin Prosedur: Langkah-langkah taktis yang harus dilakukan oleh unit kerja apabila menemukan anomali sistem, indikasi kebocoran data, atau kerusakan perangkat akibat ancaman siber.
3. Peningkatan Kesadaran Pegawai (Security Awareness)

Melakukan sosialisasi berkala atau edukasi singkat (briefing) kepada seluruh pegawai terkait pentingnya kewaspadaan terhadap ancaman siber jenis phishing, tautan mencurigakan, atau penjagaan kerahasiaan sandi sistem rumah sakit.