RSAU dr. ESNAWAN ANTARIKSA	PENGELOLAAN KEAMANAN DATA DAN INFORMASI		
	No. Dokumen SPO/ 55 /MRMIK.Akr/XI/2025	No. Revisi	Halaman 1 dari 2
STANDAR PROSEDUR OPERASIONAL	Tanggal Terbit 12 November 2025	Ditetapkan oleh, Kepala RSAU dr. Esnawan Antariksa, dr. Imam Fathurrohman W., Sp.B., M.Si., MARS. Kolonel Kes NRP 524330	

PENGERTIAN	Serangkaian proses sistematis untuk melindungi kerahasiaan, menjaga integritas, dan memastikan ketersediaan data serta informasi di lingkungan RSAU dr. Esnawan Antariksa sesuai dengan peraturan perundangan yang berlaku.
TUJUAN	1. Memastikan kerahasiaan data pasien dan informasi rumah sakit 2. Menjamin ketersediaan sistem informasi untuk pelayanan kesehatan 3. Memenuhi kewajiban hukum sesuai peraturan perundangan 4. Mencegah kebocoran, kehilangan, atau penyalahgunaan data 5. Memberikan panduan penanganan insiden keamanan data 6. Meningkatkan kesadaran keamanan informasi seluruh pegawai 7. Memastikan akuntabilitas dalam pengelolaan data
KEBIJAKAN	Surat Keputusan Kepala RSAU dr. Esnawan Antariksa tentang Kebijakan pengelolaan keamanan data dan informasi
PROSEDUR	1. Permohonan akses sistem • Calon user mengisi form permohonan akses kepada tim IT • Tim IT memverifikasi calon user dan hak akses yang dibutuhkan bagi user • Pembuatan akun oleh Tim IT • Pelatihan penggunaan system oleh Tim IT kepada user 2. Klasifikasi Hak Akses Hak akses didasarkan pada level akses sesuai dengan role di Rumah Sakit. Terdapat beberapa level akses yaitu : • Level Super Admin : Hanya Ka IT • Level Administrator : Konfigurasi sistem, user manajemen • Level Manajemen : Karumkit, Sesrumkit • Level Dokter : Dokter • Level Perawat : Perawat

	• Level Farmasi : Petugas Farmasi • Level Laboratorium/Radiologi : Petugas Laboratorium/Radiologi • Level Kasir : Petugas Kasir 3. Pengelolaan password • Kebijakan password bersifat unik terdiri dari huruf dan angka • Untuk reset password akibat lupa atau terblokir dapat menghubungi Tim IT untuk proses reset password 4. Pengamanan Data • Enkripsi data • Melakukan backup dan recovery secara berkala 5. Monitoring dan Audit • Melakukan monitoring dan audit baik untuk user dan system secara berkala 6. Penanganan Insiden Keamanan 7. Keamanan Fisik • Helpdesk menerima laporan • Melakukan initial assessment • Klasifikasi level insiden • Eskalasi sesuai level: - Critical/High: Langsung ke Tim Tanggap Insiden - Medium: Ke Koordinator TI - Low: Handled by Helpdesk 8. Keamanan Jaringan • Memastikan jaringan berjalan dengan aman dengan menggunakan software dan hardware yang sesuai dengan aplikasi yang digunakan 9. Keamanan Aplikasi • Secure Development • Melakukan patching dan update • Proteksi Web Application Firewall (WAF)
UNIT TERKAIT	Unit IT