	KEAMANAN TEKNOLOGI INFORMASI (TI)		
	No. Dokumen	No. Revisi	Halaman
STANDAR PROSEDUR OPERASIONAL	TANGGAL TERBIT	DI TETAPKAN KEPALA RUMAH SAKIT BHAYANGKARA BENGKULU Dr. dr. Julian Famil, Sp.B.,FICS.,FINACS, MARS AJUN KOMISARIS BESAR POLISI NRP. 71070496	
Pengertian	Keamanan Teknologi Informasi (TI) adalah serangkaian proses, kebijakan, tindakan teknis, dan prosedur pengelolaan yang diterapkan untuk melindungi aset informasi dan sistem TI Rumah Sakit Bhayangkara Bengkulu dari akses yang tidak sah, penggunaan, pengungkapan, gangguan, modifikasi, atau perusakan yang tidak disengaja maupun disengaja. Ini mencakup perlindungan terhadap kerahasiaan, integritas, dan ketersediaan informasi.		
Tujuan	1. Melindungi seluruh aset informasi dan sistem TI Rumah Sakit dari ancaman internal dan eksternal. 2. Menjamin kerahasiaan data pasien dan informasi sensitif lainnya. 3. Memastikan integritas data agar tetap akurat, lengkap, dan tidak termodifikasi tanpa otorisasi. 4. Memastikan ketersediaan sistem dan data TI sehingga dapat diakses oleh pengguna yang berwenang kapan pun dibutuhkan. 5. Memenuhi persyaratan peraturan perundang-undangan dan standar keamanan informasi yang berlaku. 6. Meningkatkan kesadaran keamanan TI di kalangan seluruh staf Rumah Sakit.		
Kebijakan	1. Undang-Undang No. 36 Tahun 2009 tentang Kesehatan 2. Peraturan Menteri Kesehatan No. 269/MENKES/PER/III/2008 tentang Rekam Medis 3. Peraturan Menteri Kesehatan No. 24 Tahun 2022 tentang Sistem Informasi Kesehatan 4. Peraturan Kepala Rumah Sakit Bhayangkara Bengkulu Nomor: ... /		

<table>
<tr><td rowspan="2"></td><td colspan="3">KEAMANAN TEKNOLOGI INFORMASI (TI)</td></tr>
<tr><td>No. Dokumen</td><td>No. Revisi</td><td>Halaman</td></tr>
<tr><td></td><td colspan="3">... /2025/RUMKIT tentang Tata Kelola Teknologi Informasi di Rumah Sakit Bhayangkara Bengkulu.</td></tr>
<tr><td>Prosedur</td><td colspan="3">
A. Manajemen Akses Pengguna
1. Pemberian Hak Akses:
• Setiap permintaan akses ke sistem atau data TI harus diajukan secara tertulis/elektronik dan disetujui oleh Kepala Unit terkait dan Tim/Instalasi SIMRS.
• Hak akses diberikan berdasarkan peran dan tanggung jawab pengguna (prinsip need-to-know dan least privilege).
• Pemberian hak akses baru dicatat dalam log akses pengguna.
2. Manajemen Kata Sandi:
• Pengguna wajib menggunakan kata sandi yang kuat (kombinasi huruf besar, kecil, angka, simbol) dengan panjang minimal [contoh: 8 karakter].
• Kata sandi wajib diganti secara berkala [contoh: setiap 90 hari].
• Kebijakan penggunaan kata sandi yang aman harus disosialisasikan
3. Peninjauan dan Pencabutan Akses:
• Tim/Instalasi SIMRS melakukan peninjauan hak akses pengguna secara berkala [contoh: setiap 6 bulan] untuk memastikan relevansinya.
• Hak akses harus segera dicabut atau dinonaktifkan ketika seorang staf pindah unit kerja, cuti panjang, mengundurkan diri, atau diberhentikan.

B. Perlindungan Terhadap Malware dan Virus
1. Pemasangan Antivirus:
</td></tr>
</table>

- Setiap komputer dan server di Rumah Sakit wajib terinstal perangkat lunak antivirus/anti-malware yang up-to-date.
- Pastikan update definisi virus berjalan secara otomatis dan terjadwal.

2. Pemindaian Berkala:
   - Melakukan pemindaian sistem secara berkala (misalnya, mingguan) untuk mendeteksi keberadaan virus atau malware.
3. Edukasi Pengguna:
   - Memberikan edukasi kepada pengguna untuk tidak membuka lampiran email yang mencurigakan atau mengklik tautan yang tidak dikenal.
   - Melarang penggunaan flash drive atau media penyimpanan eksternal yang tidak dipindai antivirus.

C. Keamanan Jaringan

1. Penggunaan Firewall:
   - Mengimplementasikan firewall pada titik-titik krusial jaringan untuk mengontrol lalu lintas data masuk dan keluar.
   - Konfigurasi firewall harus ditinjau dan diperbarui secara berkala.
2. Segmentasi Jaringan:
   - Melakukan segmentasi jaringan (misalnya dengan VLAN) untuk memisahkan jaringan internal, publik (Wi-Fi pasien), dan server agar membatasi penyebaran ancaman.
3. Sistem Deteksi/Pencegahan Intrusi (IDS/IPS):
   - Menggunakan IDS/IPS (jika tersedia) untuk mendeteksi dan mencegah aktivitas jaringan yang mencurigakan.

D. Enkripsi Data

1. Data dalam Transmisi:
   - Menggunakan protokol komunikasi yang aman (misalnya HTTPS, VPN) untuk melindungi data yang ditransmisikan melalui jaringan, terutama saat diakses dari luar jaringan internal.
2. Data dalam Penyimpanan:
   - Mengimplementasikan enkripsi pada data sensitif yang tersimpan di server atau perangkat penyimpanan, jika diperlukan dan sesuai standar.

E. Penanganan Insiden Keamanan TI

1. Identifikasi Insiden:
   - Pengguna atau sistem pemantau melaporkan anomali atau dugaan insiden keamanan (misalnya, akun diretas, data hilang, serangan ransomware).
2. Respons Insiden:
   - Tim/Instalasi SIMRS segera merespons insiden dengan langkah-langkah:
     - Isolasi: Mengisolasi sistem atau perangkat yang terinfeksi untuk mencegah penyebaran.
     - Investigasi: Melakukan investigasi untuk mengidentifikasi penyebab, dampak, dan ruang lingkup insiden.
     - Perbaikan: Melakukan tindakan perbaikan untuk menghilangkan ancaman dan memulihkan sistem.
     - Pemulihan: Mengembalikan operasional sistem ke kondisi normal.
3. Pelaporan Insiden:
   - Setiap insiden keamanan harus didokumentasikan dan

<table>
<tr><td rowspan="2"></td><td colspan="3">KEAMANAN TEKNOLOGI INFORMASI (TI)</td></tr>
<tr><td>No. Dokumen</td><td>No. Revisi</td><td>Halaman</td></tr>
<tr><td></td><td colspan="3">dilaporkan kepada manajemen Rumah Sakit dan/atau pihak berwenang sesuai kebijakan.

F. Audit Keamanan TI
1. Audit Berkala:
• Melakukan audit keamanan sistem TI dan jaringan secara berkala [contoh: tahunan] oleh pihak internal atau eksternal untuk mengidentifikasi celah keamanan.
2. Peninjauan Log Sistem:
• Tim/Instalasi SIMRS secara rutin meninjau log aktivitas sistem (misalnya, log login, log akses file) untuk mendeteksi aktivitas yang tidak biasa atau mencurigakan.

G. Edukasi dan Kesadaran Keamanan
1. Program Edukasi:
• Mengadakan program edukasi dan pelatihan keamanan TI secara berkala bagi seluruh staf Rumah Sakit.
2. Penyebaran Informasi:
• Menyebarkan informasi terkini mengenai ancaman keamanan siber dan praktik terbaik melalui media internal.</td></tr>
<tr><td>Unit Terkait</td><td colspan="3">1. Tim/Instalasi SIMRS (Penanggung Jawab Utama)
2. Seluruh Unit Kerja Pengguna Perangkat Lunak</td></tr>
</table>