



Innovation in Healthcare IT

MERAWAT RAGA MENJAGA DATA

Implementasi Sistem Manajemen Keamanan
Informasi di RSNU Tuban

2025

www.rsnutuban.com

Kata Pengantar

Banyak cara rumah sakit menunjukkan dedikasi untuk negeri. Bagi kami di Rumah Sakit Nahdlatul Ulama Tuban, dedikasi bukan hanya tentang ruang operasi yang lengkap atau tenaga medis yang sigap, tetapi juga tentang bagaimana kami merangkul masyarakat, menjaga lingkungan, dan menanam harapan untuk masa depan yang lebih baik.

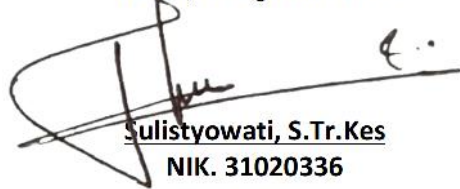
Karya ilmiah ini adalah kisah perjalanan kami, sebuah cerita tentang keyakinan bahwa pelayanan kesehatan dapat berjalan beriringan dengan tanggung jawab pelayanan, kepedulian, pemberdayaan, kepedulian lingkungan dan adaptasi mengikuti kemajuan teknologi. Setiap program yang tertulis di sini lahir dari kebutuhan nyata di lapangan, tumbuh dari gotong royong seluruh karyawan, dan bertumbuh bersama kepercayaan masyarakat.

Kami percaya, perubahan besar dimulai dari langkah kecil yang konsisten.

Di rumah sakit, setiap *byte* data bukan sekadar angka dan huruf, tetapi amanah tentang hidup, harapan, dan kepercayaan yang harus dijaga sepenuh hati. Semua ini kami rangkai bukan sekadar untuk melunasi kewajiban, namun untuk mewariskan nilai bahwa kesehatan dan kepedulian untuk menjaganya adalah hak semua orang dan tanggung jawab kita bersama.

Terima kasih kami sampaikan kepada pimpinan, rekan sejawat, mitra, dan masyarakat yang telah menjadi bagian dari cerita ini. Semoga apa yang kami tuangkan di sini menjadi inspirasi bagi rumah sakit lain untuk terus berinovasi, melayani dengan hati, dan menjaga keberlanjutan kehidupan.

Tuban, 13 Agustus 2025



Sulistyowati, S.Tr.Kes
NIK. 31020336

Daftar Isi

Kata Pengantar	ii
Daftar Isi	iii
Daftar Tabel	iv
Daftar Gambar	iv
Ringkasan.....	1
1. Latar Belakang	2
2. Tujuan	2
a. Kualitas Keamanan Data	2
b. Kepatuhan Regulasi.....	2
c. Membangun Kepercayaan Publik	2
d. Minimalisasi Risiko Keamanan.....	2
e. Meningkatkan Respon Insiden.....	2
f. Menumbuhkan Budaya Keamanan Informasi	3
3. Langkah Kerja	3
a. Analisa Kesenjangan.....	3
b. Kick-off.....	3
c. Implementasi Sistem	3
d. Monitoring Keamanan Digital	4
e. Sistem Manajemen Insiden	4
f. Monitoring dan Evaluasi.....	4
g. Internal Audit dan Tinjauan Manajemen	4
4. Hasil	4
a. Kepatuhan terhadap Standar Internasional	4
b. Peningkatan Koordinasi dan Tanggung Jawab Tim	5
c. Deteksi Dini Ancaman Siber	5
d. Respons Cepat terhadap Insiden.....	5
e. Pengelolaan Risiko yang Lebih Matang	5
f. Peningkatan Kesadaran Karyawan	6
g. Evaluasi dan Perbaikan Berkelanjutan	6
LAMPIRAN	7

Daftar Tabel

Tabel 1 Implementasi pengamanan informasi di RSNU Tuban	4
Tabel 2 Perbandingan Sebelum & Sesudah Implementasi Sistem Deteksi Dini Ancaman Siber	6

Daftar Gambar

Gambar 1: Surat Pengesahan	7
Gambar 2: Menyusun <i>Gap analysis</i>	8
Gambar 3: <i>Kick-Off</i>	8
Gambar 4: <i>Awerness</i> karyawan	8
Gambar 5: Pelatihan SMKI.....	8
Gambar 6: Sertifikasi ISO 27001:2022.....	8
Gambar 7: Perlindungan hardware dan infrastruktur.....	9
Gambar 8: <i>Collocation</i>	9
Gambar 9: <i>Firewall</i>	9
Gambar 10: Monitoring Keamanan <i>Datacenter</i>	9
Gambar 11: Sertifikat ISO 27001:2022 dan Sertifikat Trustmark Bintang 3.....	9

RINGKASAN

Data rumah sakit adalah aset kritis dan sensitif karena mencakup data pribadi, riwayat kesehatan pasien dan manajemen operasional yang bersifat rahasia. Perlindungan data menjadi kewajiban fundamental untuk menjaga keberlangsungan layanan, membangun kepercayaan publik, mengantisipasi ancaman siber, serta memenuhi regulasi. RSNU Tuban termasuk sedikit dari rumah sakit yang memiliki kesadaran tinggi akan keamanan data. Upaya nyata dilakukan melalui penilaian risiko, monitoring keamanan digital, sistem manajemen insiden dan program *Security Awareness*. Kami meraih sertifikasi ISO 27001:2022 dan *Trustmark* Bintang 3 BPJS Kesehatan, membuktikan tata kelola keamanan data yang baik melalui *respon time* dan kepuasan pengguna.

Kata kunci: Keamanan Data, Ancaman Siber

Merawat Raga Menjaga Data

Implementasi Sistem Manajemen Keamanan Informasi di RSNU Tuban

1. Latar Belakang

Di era digital, data rumah sakit merupakan aset yang sangat kritis dan sensitif. Data tersebut mencakup informasi pribadi pasien, riwayat kesehatan, hingga detail manajemen operasional yang bersifat rahasia. Kerahasiaan, integritas dan ketersediaan data menjadi faktor penting dalam menjaga keberlangsungan layanan kesehatan. Kegagalan dalam melindungi data dapat menurunkan kepercayaan publik, mengganggu pelayanan, serta berpotensi menimbulkan kerugian hukum dan reputasi.

Perlindungan data tidak hanya menjadi tanggung jawab teknis, tetapi juga kewajiban fundamental sesuai regulasi, yang telah diatur di dalam Undang-Undang Perlindungan Data Pribadi dan peraturan Kementerian Kesehatan. Ancaman siber yang semakin kompleks saat ini menuntut rumah sakit memiliki sistem keamanan informasi yang kokoh dan terkelola dengan baik.

RSNU Tuban adalah salah satu rumah sakit yang memiliki kesadaran tinggi terhadap pentingnya keamanan data. Berbagai langkah strategis telah dilakukan melalui pelaksanaan penilaian risiko, pemantauan keamanan digital secara berkelanjutan, penerapan sistem manajemen insiden yang responsif serta program *Security Awareness* bagi seluruh karyawan untuk mengurangi risiko *human error*.

Komitmen RSNU Tuban terhadap keamanan informasi dibuktikan dengan sertifikasi ISO 27001:2022 dan *Trustmark* Bintang 3 dari BPJS Kesehatan, yang menjadi pengakuan formal atas kualitas tata kelola keamanan informasi. Hasil implementasi ini terlihat dari peningkatan kecepatan respon insiden serta tingginya kepuasan pengguna layanan.

Berdasarkan pertimbangan kebutuhan dan tanggung jawab tersebut, inovasi keamanan informasi berbasis manajemen risiko di RSNU Tuban dapat menjadi model penerapan tata kelola data yang standar, efektif dan berkelanjutan di sektor kesehatan.

2. Tujuan

a. Kualitas Keamanan Data

Melindungi kerahasiaan data pasien serta informasi operasional dari gangguan internal maupun eksternal.

b. Kepatuhan Regulasi

Implementasi UU nomor 17 tahun 2023 tentang Kesehatan, UU nomor 27 tahun 2022 tentang Perlindungan Data Pribadi, Peraturan Menteri Kesehatan nomor 24 tahun 2022 tentang Rekam Medis Elektronik, Sertifikasi ISO 27001:2022 tentang Sistem Manajemen Keamanan Informasi dan Standarisasi *Trustmark* BPJS Kesehatan.

c. Membangun Kepercayaan Publik

Meningkatkan kepercayaan pasien, keluarga dan mitra bahwa data di rumah sakit telah dikelola secara aman dan profesional.

d. Minimalisasi Risiko Keamanan

Mengidentifikasi, menilai dan mengendalikan potensi ancaman melalui manajemen risiko yang terstruktur.

e. **Meningkatkan Respon Insiden**

Mempercepat deteksi dan penanganan insiden untuk mengurangi dampak pada layanan dan reputasi rumah sakit.

f. **Menumbuhkan Budaya Keamanan Informasi**

Mendorong kesadaran seluruh pegawai melalui pelatihan, sosialisasi dan penerapan kebijakan yang konsisten.

3. **Langkah Kerja**

a. **Analisa Kesenjangan**

Tahap awal penerapan Sistem Manajemen Keamanan Informasi (SMKI) adalah melakukan gap analysis untuk membandingkan kondisi eksisting manajemen keamanan informasi di RSNU Tuban dengan persyaratan ISO 27001:2022. Proses ini melibatkan identifikasi kekuatan, kelemahan, peluang perbaikan dan area yang belum sesuai dengan standar. Data dikumpulkan melalui wawancara, tinjauan dokumen dan observasi langsung. Hasil *gap analysis* menjadi peta jalan (*roadmap*) yang jelas untuk menentukan prioritas implementasi dan memastikan setiap langkah yang diambil tepat sasaran.

b. **Kick-off**

Setelah *gap analysis* selesai, dilakukan kegiatan *kick-off* meeting sebagai penanda dimulainya implementasi SMKI secara resmi. Pada tahap ini, manajemen menetapkan Tim SMKI yang terdiri dari perwakilan unit terkait, seperti IT, rekam medis, manajemen risiko dan SDM. Tim ini bertugas merancang, menjalankan dan mengawasi implementasi SMKI. Penetapan peran dan tanggung jawab dilakukan secara jelas untuk menghindari tumpang tindih tugas dan memastikan koordinasi yang efektif.

c. **Implementasi Sistem**

Implementasi pengamanan informasi di RSNU Tuban dilaksanakan melalui:

FOKUS	TUJUAN	IMPLEMENTASI
Keamanan Fisik	Perlindungan <i>hardware</i> dan infrastruktur	Ruang server akses biometrik, CCTV 24/7, sensor kebakaran, sistem pendingin khusus
<i>Colocation</i>	Penempatan server di pusat data pihak ketiga dengan fasilitas keamanan dan infrastruktur standar	Sertifikasi Tier 3, akses terbatas, pemantauan 24/7
Keamanan Jaringan	Pengamanan lalu lintas data dari akses atau serangan tidak sah	Firewall, IDS/IPS, segmentasi jaringan
Keamanan Data	Melindungi data tetap rahasia, utuh dan siap saat dibutuhkan	Enkripsi RME, <i>backup</i> harian, replikasi data
Manajemen Risiko	Identifikasi, penilaian dan mitigasi potensi ancaman keamanan	<i>Risk assessment</i> setiap 6 bulan
Manajemen Insiden	Prosedur penanganan dan pemulihan insiden keamanan	Regulasi penanganan kebocoran data, Tim BCP, simulasi serangan siber
<i>Awareness</i>	Meningkatkan pengetahuan karyawan terkait keamanan informasi	Pelatihan keamanan data, simulasi <i>phishing</i> , poster edukasi

Kepatuhan Regulasi	Memastikan sistem sesuai regulasi yang berlaku	UU Kesehatan, UU Perlindungan Data Pribadi, Peraturan Menteri Kesehatan dan standarisasi ISO 27001:2022
--------------------	--	---

Tabel 1: Implementasi pengamanan informasi di RSNU Tuban

d. Monitoring Keamanan Digital

Monitoring keamanan digital dilakukan untuk mendeteksi potensi ancaman atau insiden sejak dini. RSNU Tuban menggunakan sistem pemantauan jaringan, *endpoint security* dan *log* monitoring untuk memantau aktivitas tidak wajar pada infrastruktur teknologi informasi. Pemantauan ini bersifat berkelanjutan (*continuous monitoring*) dengan pelaporan rutin kepada Tim SMKI. Hasil monitoring menjadi dasar pengambilan keputusan dalam penanganan insiden dan perbaikan sistem.

e. Sistem Manajemen Insiden

Manajemen insiden dirancang untuk menangani gangguan keamanan informasi secara cepat, tepat dan terkoordinasi. Proses ini mencakup deteksi, pelaporan, analisis, penanganan dan dokumentasi insiden. RSNU Tuban menerapkan prosedur *Incident Response* yang dilengkapi dengan regulasi internal dan formulir pelaporan insiden sehingga tujuan akhir dari sistem manajemen insiden untuk meminimalkan dampak operasional dan sarana pembelajaran dari setiap insiden dapat tercapai.

f. Monitoring dan Evaluasi

Monitoring dan evaluasi bertujuan memastikan implementasi SMKI berjalan sesuai rencana dan mencapai sasaran. Penilaian risiko keamanan informasi dilakukan secara berkala menggunakan metode *risk assessment* berbasis ISO 27005. Proses ini meliputi identifikasi aset informasi, ancaman, kerentanan, analisis dampak dan kemungkinan terjadinya risiko. Pendekatan ini memastikan penggunaan sumber daya yang efektif untuk mengatasi risiko paling kritis. Evaluasi mencakup peninjauan efektivitas kontrol, kepatuhan terhadap SPO, serta hasil audit internal. Laporan evaluasi digunakan untuk mengidentifikasi area yang perlu perbaikan dan untuk mengukur pencapaian indikator kinerja, seperti waktu respons insiden dan tingkat kepuasan pengguna. Berdasarkan hasil penilaian, selanjutnya dibuat rencana mitigasi risiko yang memprioritaskan tindakan sesuai tingkat risiko.

g. Internal Audit dan Tinjauan Manajemen

Tahap terakhir adalah internal audit untuk memastikan kesesuaian SMKI dengan persyaratan ISO 27001:2022. Audit dilakukan oleh auditor internal yang kompeten dan independen, mencakup pemeriksaan dokumen, wawancara, serta verifikasi bukti implementasi. Hasil audit kemudian dibahas dalam rapat Management Review untuk mengevaluasi pencapaian, hambatan dan kebutuhan perbaikan. Tinjauan manajemen menjadi dasar penetapan kebijakan, sasaran baru, serta rencana peningkatan berkelanjutan.

4. Hasil

Penerapan langkah SMKI menghasilkan perubahan signifikan dalam tata kelola keamanan informasi di RSNU Tuban. Implementasi SMKI dapat meningkatkan kepercayaan pasien, efektivitas operasional dan kemampuan rumah sakit dalam menghadapi ancaman siber.

a. Kepatuhan terhadap Standar Internasional

Melalui gap analysis dan tindak lanjutnya, RSNU Tuban berhasil menutup celah sistem yang berpotensi sebagai pintu masuk gangguan. Seluruh kebijakan, prosedur dan dokumen pendukung SMKI telah disusun, disahkan dan dijalankan sesuai klausul yang berlaku. Hasilnya, manajemen memiliki dasar hukum dan prosedural yang jelas dalam mengelola keamanan informasi.

b. Peningkatan Koordinasi dan Tanggung Jawab Tim

Dengan adanya Tim SMKI yang dibentuk pada tahap kick-off, koordinasi antar unit menjadi lebih efektif. Setiap anggota memahami perannya, mulai dari pemantauan keamanan digital, pengelolaan risiko, hingga penanganan insiden. Hal ini mengurangi risiko miskomunikasi dan mempercepat pengambilan keputusan ketika terjadi ancaman.

c. Deteksi Dini Ancaman Siber

Perbandingan sebelum dan sesudah penggunaan sistem dapat dituangkan dalam tabel dibawah ini:

ASPEK	BEFORE	AFTER
Kecepatan Deteksi	Ancaman terdeteksi beberapa jam atau beberapa hari setelah masuk, sering terlambat mengambil upaya perbaikan.	Ancaman terdeteksi dalam hitungan menit atau detik berdasarkan <i>continuous monitoring</i> dan sistem peringatan otomatis.
Jumlah insiden	Tinggi, termasuk insiden yang menyebabkan gangguan operasional.	Menurun signifikan, insiden besar yang mengganggu layanan dapat diminimalisir.
Jenis Ancaman Terdeteksi	Terbatas kepada ancaman yang menimbulkan dampak mayor.	Lebih luas, mencakup anomali jaringan sampai dengan percobaan peretasan, akses ilegal dan serangan malware.
Respons Tim IT	Respons lambat karena ancaman sering diketahui setelah terjadi kerusakan.	Respons cepat karena notifikasi real-time, memudahkan penanganan segera.
Keberlangsungan Operasional	Sering terganggu akibat serangan yang terlambat ditangani.	Operasional tetap stabil karena ancaman ditangani sebelum mengganggu layanan.
Kepuasan Pengguna	Rendah, sering terjadi gangguan layanan.	Meningkat berkat layanan yang lebih andal dan aman.

Tabel 2: Perbandingan Sebelum & Sesudah Implementasi Sistem Deteksi Dini Ancaman Siber

d. Respons Cepat terhadap Insiden

Dengan adanya Incident Management System yang terstandarisasi, waktu respons terhadap insiden berkurang secara signifikan. Setiap kejadian, mulai dari gangguan

jaringan hingga kebocoran data, dapat ditangani sesuai prosedur yang telah ditetapkan. Dokumentasi insiden juga memastikan pembelajaran dari setiap kasus untuk perbaikan berkelanjutan.

e. Pengelolaan Risiko yang Lebih Matang

Pendekatan sistematis dalam penilaian dan pengelolaan risiko menghasilkan peta risiko yang jelas. RSNU Tuban kini dapat memprioritaskan upaya mitigasi pada ancaman dengan tingkat risiko tertinggi, memastikan sumber daya digunakan secara efisien. Perubahan ini meningkatkan resiliensi rumah sakit terhadap serangan siber maupun kegagalan sistem.

f. Peningkatan Kesadaran Karyawan

Program Security Awareness yang dijalankan berhasil membangun budaya keamanan informasi di seluruh lapisan organisasi. Karyawan menjadi lebih disiplin dalam menggunakan kata sandi, waspada terhadap phishing dan mematuhi SOP perlindungan data pasien. Efeknya, potensi kebocoran informasi akibat kelalaian manusia dapat ditekan secara signifikan.

g. Evaluasi dan Perbaikan Berkelanjutan

Monitoring dan evaluasi rutin memberikan gambaran jelas mengenai efektivitas SMKI. Hasil evaluasi digunakan untuk memperbaiki prosedur dan memperkuat kontrol keamanan, menciptakan siklus peningkatan berkelanjutan (continuous improvement).

RSNU Tuban membuktikan bahwa dengan implementasi sistem manajemen keamanan informasi, telah menghasilkan beberapa manfaat nyata:

- 1) Keamanan data pasien terjaga melalui kontrol teknis dan prosedural yang ketat.
- 2) Kepuasan pasien meningkat karena layanan lebih andal dan privasi terjaga.
- 3) Efisiensi operasional meningkat berkat koordinasi tim yang lebih baik.
- 4) Ketahanan terhadap ancaman siber meningkat melalui deteksi dini dan respons cepat.
- 5) Budaya keamanan informasi terbentuk di seluruh level organisasi.

Dengan capaian ini, RSNU Tuban tidak hanya menunjukkan kepatuhan terhadap regulasi, namun juga membangun reputasi sebagai rumah sakit yang mengutamakan perlindungan informasi dan keselamatan pasien.

LAMPIRAN

SURAT PENGESAHAN



**Rumah Sakit
Nahdlatul Ulama Tuban**
the traditional green hospital



SURAT PENGESAHAN

Nomor : 0575.4/RSNU/A.1/K-3/VIII/2025

Saya yang bertanda tangan di bawah ini:

Nama : dr. Didik Suharsoyo, M.ARS., MM., FISQua., FRSPH
Jabatan : Direktur
NIK : 101 08 003
Alamat : Jl. Letda Sucipto 211 Tuban

Dengan ini menyatakan bahwa

Tema Makalah: ***Innovation in Healthcare IT***

Judul Makalah:

**"RSNU Tuban Merawat Raga Menjaga Data, Implementasi Sistem Manajemen Keamanan
Informasi di RSNU Tuban"**

Penyusun :

1. Nama : Sulistyowati, S.Tr, Kes.
Jabatan : Kepala Unit Manajemen Rekam Medik, Informasi dan Komunikasi
Unit : Manajemen Rekam Medik, Informasi dan Komunikasi
2. Nama : Dhanis Ardianto Putra, S.KOM
Jabatan : Koordinator Unit IT
Unit : Informasi Teknologi

Telah diperiksa, ditelaah dan disahkan untuk dapat digunakan sebagai salah satu media informasi tentang kegiatan pelayanan di Rumah Sakit Nahdlatul Ulama Tuban.

Ditetapkan di: TUBAN
pada tanggal: 14 Agustus 2024
Direktur


dr. Didik Suharsoyo, M.ARS., M.M., FISQua., FRSPH.
NIK: 101 08 003

Jl. Letda Sucipto no. 211 Tuban
(0356) 328299 | (0356) 328244
info@rsnutuban.com
www.rsnutuban.com
(0356) 712072

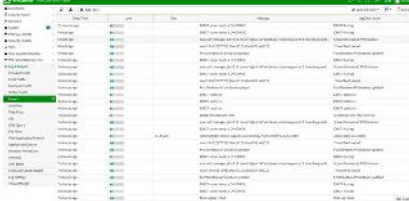


Gambar 1: Surat Pengesahan

**LAMPIRAN FOTO KEGIATAN
SISTEM MANAJEMEN KEAMANAN INFORMASI
ISO 27001:2022**

FOTO	KEGIATAN	KETERANGAN
	Menyusun <i>Gap analysis</i> untuk membandingkan kondisi eksisting manajemen keamanan informasi di RSNU Tuban dengan persyaratan ISO 27001:2022	Gambar 2: Menyusun <i>Gap analysis</i>
	Penetapan Tim SMKI	Gambar 3: <i>Kick-Off</i>
	<i>Awerness</i> karyawan terkait sistem manajemen keamanan informasi	Gambar 4: <i>Awerness</i> karyawan
	Pelatihan sistem manajemen keamanan informasi ISO 27001:2022	Gambar 5: Pelatihan SMKI
	Audit eksternal ISO 27001:2022	Gambar 6: Sertifikasi ISO 27001:2022

**LAMPIRAN FOTO KEGIATAN
IMPLEMENTASI SISTEM
ISO 27001:2022**

FOTO	KEGIATAN	KETERANGAN
	Ruang server akses biometrik, CCTV 24/7, sensor kebakaran, sistem pendingin khusus	Gambar 7: Perlindungan hardware dan infrastruktur
	Penempatan server di pusat data pihak ketiga dengan fasilitas keamanan dan infrastruktur standar	Gambar 8: Collocation
	Pengamanan lalu lintas data dari akses atau serangan tidak sah	Gambar 9: Firewall
	Monitoring keamanan datacenter rumah sakit terhadap ancaman siber	Gambar 10: Monitoring Keamanan Datacenter
	Sertifikat ISO 27001:2022 dan Sertifikat Trustmark Bintang 3	Gambar 11: Sertifikat ISO 27001:2022 dan Sertifikat Trustmark Bintang 3