PEDOMAN

PENGELOLAAN TEKNOLOGI INFORMASI



RSST

KEMENTERIAN KESEHATAN RI

DIREKTORAT JENDERAL PELAYANAN KESEHATAN

RSUP DR. SOERADJI TIRTONEGORO KLATEN

TAHUN 2022

KEMENTERIAN KESEHATAN REPUBLIK INDONESIA
DIREKTORAT JENDERAL PELAYANAN KESEHATAN
RSUP DR. SOERADJI TIRTONEGORO
Jalan KRT. dr. Soeradji Tirtonegoro Nomor 1 Klaten
Telp : (0272) 321020 Fax : (0272) 321104 E-mail : rsupsoeradji_klaten@yahoo.com
RSST

KEPUTUSAN DIREKTUR UTAMA
RUMAH SAKIT UMUM PUSAT DR. SOERADJI TIRTONEGORO
NOMOR : HK.02.03/III.3.1/ 18256 /2022

TENTANG

PEDOMAN PENGELOLAAN TEKNOLOGI INFORMASI
DI RSUP DR. SOERADJI TIRTONEGORO

DENGAN RAHMAT TUHAN YANG MAHA ESA

DIREKTUR UTAMA RSUP DR. SOERADJI TIRTONEGORO,

Menimbang :

a. bahwa untuk melaksanakan langkah-langkah pemulihan pada insiden maupun bencana yang menimbulkan gangguan pada layanan teknologi informasi di RSUP dr. Soeradji Tirtonegoro Klaten diperlukan adanya Pedoman Pengelolaan Teknologi Informasi;

b. bahwa seluruh kegiatan pemulihan layanan teknologi informasi tersebut harus dilaksanakan berdasarkan pedoman yang mengacu pada kebijakan yang berlaku;

c. bahwa berdasarkan pertimbangan sebagaimana dimaksud pada huruf a dan huruf b, perlu menetapkan Keputusan Direktur Utama tentang Pedoman Pengelolaan Teknologi Informasi di RSUP dr. Soeradji Tirtonegoro.

Mengingat :

1. Undang-Undang Nomor 11 Tahun 2008 tentang lnformasi dan Transaksi Elektronik (Lembaran Negara Republik lndonesia Tahun 2008 Nomor 58);
2. Undang-undang Nomor 14 Tahun 2008 tentang keterbukaan Informasi Publik;
3. Undang-Undang Nomor 44 Tahun 2009 tentang Rumah Sakit (Lembaran Negara Republik lndonesia Tahun 2009 Nomor 153, Tambahan Lembaran Negara Republik lndonesia Nomor 5072);
4. Peraturan Pemerintah Nomor 46 Tahun 2014 Tentang Sistem lnformasi Kesehatan (Lembaran Negara Republik lndonesia Tahun 2014 Nomor 126, Tambahan Lembaran Negara Republik lndonesia Nomor 5542);

5. Peraturan .....

5. Peraturan Pemerintah Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik lndonesia Tahun 2019 Nomor 185, Tambahan Lembaran Negara Republik lndonesia Nomor 6400);
6. Peraturan Menteri Kesehatan Nomor 82 Tahun 2013 tentang Sistem Informasi Manajemen Rumah Sakit;
7. Peraturan Menteri Kesehatan Nomor 92 Tahun 2014 tentang Penyelenggaraan Komunikasi Data Dalam Sistem lnformasi Kesehatan Terintegrasi (Berita Negara Republik lndonesia Tahun 2014 Nomor 1954);
8. Peraturan Menteri Kesehatan Nomor 42 Tahun 2020 Tentang Organisasi dan Tata Kerja RSUP dr. Soeradji Tirtonegoro.
9. Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis;

MEMUTUSKAN:

Menetapkan : KEPUTUSAN DIREKTUR UTAMA TENTANG PEDOMAN PENGELOLAAN TEKNOLOGI INFORMASI DI RSUP DR. SOERADJI TIRTONEGORO.

KESATU : Menetapkan Pedoman Pengelolaan Teknologi Informasi di RSUP dr. Soeradji Tirtonegoro sebagaimana tercantum dalam lampiran yang merupakan bagian tidak terpisahkan dari Keputusan ini.

KEDUA : Pedoman Pengelolaan Teknologi Informasi di RSUP dr. Soeradji Tirtonegoro sebagaimana dimaksud dalam Diktum KESATU, agar dapat dilaksanakan dan digunakan sebagai acuan dalam pelaksanaan kegiatan.

KETIGA : Segala biaya yang timbul terkait dengan Keputusan ini dibebankan pada DIPA RSUP dr. Soeradji Tirtonegoro.

KEEMPAT : Keputusan ini mulai berlaku pada tanggal ditetapkan, dengan catatan apabila dikemudian hari ternyata terdapat kekeliruan dalam penetapan ini, akan diadakan perbaikan sebagaimana mestinya.

Ditetapkan di Klaten
Pada tanggal 13 Oktober 2022

DIREKTUR UTAMA

ENDANG WIDYASWATI

LAMPIRAN

KEPUTUSAN DIREKTUR UTAMA

RUMAH SAKIT UMUM PUSAT DR. SOERADJI TIRTONEGORO

NOMOR : HK.02.03/III.3.1/ 18256 /2020

TENTANG

PEDOMAN PENGELOLAAN TEKNOLOGI INFORMASI DI RSUP DR. SOERADJI TIRTONEGORO

DAFTAR ISI

I. PENDAHULUAN 3

A. Latar Belakang 3

B. Dasar Hukum 4

C. Ruang Lingkup 5

D. Definisi 5

II. PEDOMAN PENGELOLAAN PERANGKAT LUNAK 9

A. Pengembangan Sistem Informasi 9

B. Analisis dan Perancangan Sistem Informasi 9

C. Pembuatan Kode Program 10

D. Pengujian Aplikasi 10

E. Serah Terima Aplikasi 11

F. Penggunaan Perangkat Lunak Sistem Operasi 11

G. Penggunaan Aplikasi Pendukung Perkantoran 11

H. Penggunaan Aplikasi Eksternal 12

I. Website Rumah Sakit 12

J. Webservice dan Interoperabilitas Sistem Informasi 14

K. Basis Data Terpusat 15

III. PEDOMAN PENGELOLAAN ALAT PENGOLAH DATA 17

A. Perencanaan dan Pengadaan Alat Pengolah Data 17

B. Pengelolaan Suku Cadang dan Aksesoris Alat Pengolah Data 17

C. Distribusi Perangkat Keras 18

D. Perawatan Alat Pengolah Data 18

E. Perangkat Keras Bersumber Kerja sama Operasi di Luar SIMRS 19

F. Kerja Sama Pemeliharaan Perangkat Keras 19

IV. PEDOMAN PENGELOLAAN INFRASTRUKTUR 20

DAN JARINGAN KOMPUTER 20

A. Pemasangan Jaringan Utama 20

B. Jaringan Distribusi Kabel 20

C. Jaringan Distribusi Nirkabel 20

D. Penggunaan Internet 21

E. Datacenter 21

F. Disaster Recovery Center 22

V. PEDOMAN OPERASIONAL DAN PERAWATAN SISTEM INFORMASI 23

A. Kerahasiaan Data dan Informasi 23

B. Kontrol Akses Pengguna 23

C. Penggunaan SIMRS 23

D. Penanganan Kesalahan Transaksi SIMRS 24

E. Penanganan *Error* dan *Bug* Aplikasi 24

F. Manajemen Data dan Informasi 25

G. Pengubahan dan Penambahan Modul pada Aplikasi 25

VI. PEDOMAN PENGELOLAAN SUMBER DAYA MANUSIA 26

A. Pengembangan SDM Teknologi Informasi 26

B. Kerahasiaan Data dan Informasi oleh Staf 26

C. Resign dan Mutasi 26

VII. PEDOMAN KEAMANAN SISTEM INFORMASI DAN JARINGAN 27

A. Prinsip Kemanan Sistem Informasi 27

B. Identifikasi Pengguna 27

C. Akses Informasi Rumah Sakit 27

D. Keamanan Jaringan 28

E. Bentuk Pelanggaran 28

F. Penanganan Insiden keamanan Informasi 29

VIII. PEDOMAN MANAJEMEN RISIKO 31

A. Pengelolaan Risiko 31

B. Identifikasi Risiko 31

C. Disaster Recovery Plan 31

IX. PENUTUP 32

BAB I
PENDAHULUAN

A. Latar Belakang

Implementasi dan pengembangan teknologi informasi merupakan sesuatu hal yang mutlak bagi sebuah organisasi moderen. Tantangan dan tuntutan yang terus berkembang secara dinamis menuntut tersedianya sistem informasi yang mampu menangani seluruh kebutuhan pengelolaan informasi di dalam organisasi secara cepat, tepat, dan akurat. Di tengah persaingan yang semakin keras dan ketat, sistem informasi menjadi komponen vital yang akan memberikan kekuatan dan keunggulan bagi organisasi.

Rumah sakit sebagai sebuah organisasi besar dengan permasalahan yang sangat banyak dan kompleks harus dikelola secara profesional dan moderen, salah satunya dengan melibatkan dukungan teknologi informasi. Data-data yang terkait dengan proses bisnis, transaksi, dan manajerial rumah sakit harus dikelola secara terstruktur dan sistematis agar dapat menjadi informasi yang berguna bagi kegiatan operasional maupun pengambilan keputusan oleh pihak yang berkepentingan.

Implementasi teknologi informasi juga akan memberikan nilai lebih dalam kegiatan pelayanan yang dilakukan oleh rumah sakit, baik untuk pasien, profesional pemberi asuhan (dokter, perawat, dan penunjang), serta untuk *civitas hospitalia* secara umum.

RSUP dr. Soeradji Tirtonegoro Klaten adalah rumah sakit yang menyadari bahwa teknologi informasi merupakan salah satu unsur penting di dalam kegiatan rumah sakit. Keberadaan teknologi informasi tidak dipandang hanya sebagai komponen pendukung, tetapi sebagai bagian pokok dan vital yang menentukan kelangsungan hidup organisasi. Teknologi informasi yang digunakan selalu dibenahi dan dikembangkan dari waktu ke waktu, hingga mencapai kondisi yang semakin mendekati ideal.

Sistem informasi sudah di gunakan di RSST sejak tahun 2005 dalam bentuk Aplikasi SIMRS. Kemudian dilanjutkan dengan pengembangan SIMRS secara mandiri pada pertengahan tahun 2015 hingga saat ini. Untuk mencapai tingkat implementasi yang maksimal, perlu terus dilakukan upaya pengembangan agar sistem informasi yang digunakan dapat

memenuhi kebutuhan organisasi yang terus bertambah, serta mengikuti perkembangan teknologi mutakhir.

Berdasarkan hal tersebut diatas, maka perlu dibuat sebuah prencana pengembangan SIMRS yang menyeluruh dan terintegrasi dalam bentuk master plan SIMRS. Dokumen ini diharapkan dapat menjadi acuan dan bahan pertimbangan bagi pengambil keputusan dalam melakukan investasi ataupun pemilihan teknologi yang berkaitan dengan penggunaan SIMRS secara internal. Seiring dengan pesatnya perkembangan teknologi informasi serta perkembangan sistem pengelolaan rumah sakit, maka dokumen ini disusun dalam model dinamis, serta diperlukan review ataupun evaluasi secara periodik untuk tetap menjaga aktualitasnya.

B. Dasar Hukum

1. Undang-Undang Nomor 11 Tahun 2008 tentang lnformasi dan Transaksi Elektronik (Lembaran Negara Republik lndonesia Tahun 2008 Nomor 58);
2. Undang-Undang Nomor 44 Tahun 2009 tentang Rumah Sakit (Lembaran Negara Republik lndonesia Tahun 2009 Nomor 153, Tambahan Lembaran Negara Republik lndonesia Nomor 5072);
3. Peraturan Pemerintah Nomor 46 Tahun 2014 Tentang Sistem lnformasi Kesehatan (Lembaran Negara Republik lndonesia Tahun 2014 Nomor 126, Tambahan Lembaran Negara Republik lndonesia Nomor 5542);
4. Peraturan Pemerintah Nomor Tl Tahun 2019 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik (Lembaran Negara Republik lndonesia Tahun 2019 Nomor 185, Tambahan Lembaran Negara Republik lndonesia Nomor 6400);
5. Peraturan Menteri Kesehatan Nomor 24 Tahun 2022 tentang Rekam Medis;
6. Peraturan Menteri Kesehatan Nomor 82 Tahun 2013 tentang Sistem Informasi Manajemen Rumah Sakit;
7. Peraturan Menteri Kesehatan Nomor 42 Tahun 2020 Tentang Organisasi dan Tata Kerja RSUP dr. Soeradji Tirtonegoro (Berita Negara Republik lndonesia Tahun 2020 Nomor 1510).

C. Ruang Lingkup

Kebijakan ini disusun untuk menjadi panduan pengelolan teknologi informasi pada RSUP dr. Soeradji Tirtonegoro Klaten. Substansi materi kebijakan meliputi pengelolaan seluruh aspek teknologi informasi yang terdiri atas: aspek perangkat lunak, aspek perangkat keras dan jaringan, aspek sumber daya manusia, serta aspek regulasi dan tata kelola.

Seluruh ketetapan dalam kebijakan ini mengikat untuk seluruh *civitas hospitalia* serta *stake holder* yang terlibat dalam pemanfaatan sumber daya teknologi informasi di RSUP dr. Soeradji Tirtonegoro Klaten.

D. Definisi

1. Basis Data

   Basis data atau pangkalan data (bahasa Inggris: *database*) adalah kumpulan data yang terorganisir, yang umumnya disimpan dan diakses secara elektronik dari suatu sistem komputer.

2. Data

   Data adalah catatan atas kumpulan fakta yang berasal dari hasil pengukuran atau pengamatan suatu variabel yang bentuknya dapat berupa angka, kata-kata, atau citra.

3. *Data center*

   Data center atau pusat data adalah bangunan fasilitas yang digunakan untuk menempatkan sistem komputer dan komponen-komponen terkaitnya, seperti sistem telekomunikasi dan penyimpanan data.

4. *Disaster Recovery System*

   Disaster Recovery System adalah bangunan beserta infrastruktur yang berfungsi untuk menempatkan perangkat teknologi informasi, sistem, aplikasi, dan data replikasi sebagai sistem cadangan dalam menghadapi bencana teknologi informasi.

5. *Domain*

   Domain adalah nama yang diberikan untuk mengidentifikasi sebuah jaringan tanpa menggunakan *internet protocol/* IP. Biasanya alamat IP menggunakan angka-angka yang sulit dihafal.

6. *Hosting Website*

   Hosting website atau *web hosting* adalah tempat atau media untuk menyimpan seluruh file dan data website sehingga dapat diakses secara

online oleh pengunjung melalui internet. File dan data website tersebut dapat berupa video, gambar, email, script, aplikasi, dan *database*.

7. *Informasi*

   Informasi adalah pesan (ucapan atau ekspresi) atau kumpulan pesan yang terdiri dari order sekuens dari simbol, atau makna yang dapat ditafsirkan dari pesan atau kumpulan pesan.

8. Jaringan Komputer

   Jaringan komputer (*computer network*) adalah jaringan telekomunikasi yang memungkinkan antar komputer untuk saling berkomunikasi dengan bertukar data. Tujuan dari pembentukan jaringan komputer adalah agar setiap perangkat dalam jaringan komputer dapat meminta dan memberikan layanan (*service*).

9. Keamanan Sistem Informasi

   Keamanan Sistem Informasi adalah manajemen pengelolaan keamanan yang bertujuan mencegah, mengatasi, dan melindungi berbagai sistem informasi dari resiko terjadinya tindakan ilegal seperti penggunaan tanpa izin, penyusupan, dan perusakan terhadap berbagai informasi yang di miliki

10. LAN

    LAN atau *Local Area Network* (LAN) merupakan suatu topologi jaringan komputer yang menghubungkan perangkat pada cakupan wilayah lokal (seluruh perangkat berada pada lokasi yang sama).

11. Perangkat Keras

    Perangkat keras atau *hardware* adalah piranti atau komponen komputer yang memiliki wujud fisik sehingga dapat dilihat atau diraba secara langsung.

12. Perangkat Lunak

    Perangkat lunak adalah kumpulan data elektronik yang berupa perintah/ instruksi untuk program dalam sebuah komputer, yang apabila dieksekusi oleh usernya akan memberikan fungsi dan unjuk kerja seperti yang diharapkan oleh usernya.

13. Sistem Informasi

Sistem informasi adalah kombinasi dari teknologi informasi dan aktivitas manusia yang menggunakan perengkat teknologi informasi untuk mendukung operasi dan manajemen.

14. Sistem Operasi

Sistem operasi adalah perangkat lunak sistem yang mampu mengelola sumber daya (*resources*) dari *software* dan *hardware* agar dapat berjalan dengan baik serta memudahkan proses interaksi dengan pengguna (*brainware*).

15. SIMRS

Sistem Informasi Manajemen Rumah Sakit yang selanjutnya disingkat SIMRS adalah suatu sistem teknologi informasi komunikasi yang memproses dan mengintegrasikan seluruh alur proses pelayanan Rumah Sakit dalam bentuk jaringan koordinasi, pelaporan dan prosedur administrasi untuk memperoleh informasi secara tepat dan akurat, dan merupakan bagian dari Sistem Informasi Kesehatan.

16. *Software Development Life Cycle*

SDLC adalah siklus yang digunakan dalam pembuatan atau pengembangan sistem informasi yang bertujuan untuk menyelesaikan masalah secara efektif. SDLC juga berfungsi membagi peranan dan tanggung jawab yang jelas antara pengembang, desainer, analis bisnis, dan manajer proyek. Fungsi lain dari SDLC ialah dapat memberikan gambaran input dan output yang jelas dari satu tahap menuju tahap selanjutnya

17. *Source code*

Kode sumber (Inggris: *source code*) atau kode program adalah suatu rangkaian pernyataan atau deklarasi yang ditulis dalam bahasa pemrograman komputer yang terbaca manusia. Kode sumber yang menyusun suatu program biasanya disimpan dalam satu atau lebih berkas teks, dan dapat pula ditampilkan dalam bentuk cuplikan kode (*code snippet*) yang dicetak pada buku atau media lainnya.

18. Sumber Daya Manusia Teknologi Informasi

SDM Teknologi Informasi adalah individu yang bertanggung jawab terkait perencanaan dan pengembangan teknologi informasi di perusahaan, seperti Divisi Teknologi Informasi, Departemen Sistem Informasi, ataubagian sejenis lainnya.

19. Teknologi Informasi

Teknologi informasi yaitu suatu teknologi yang mempunyai fungsi dalam mengolah data, memproses data, memperoleh, menyusun, menyimpan, mengubah data dengan berbagai cara untuk mendapatkan informasi yang bermanfaat atau berkualita

20. *Web Service*

Web service merupakan aplikasi yang berisi sekumpulan basis data (*database*) dan perangkat lunak (*software*) atau bagian dari program perangkat lunak yang diakses secara remote oleh piranti dengan perantara tertentu.

21. *Website*

Website adalah kumpulan halaman web yang dapat diakses publik dan saling terkait yang berbagi satu nama domain. *Website* dapat dibuat dan dikelola oleh individu, grup, bisnis, atau organisasi untuk melayani berbagai tujuan.

22. *WiFi*

WiFi adalah teknologi jaringan nirkabel yang menggunakan gelombang radio untuk menyediakan akses internet tanpa kabel dengan kecepatan yang tinggi. Adapun gelombang radio yang digunakan yakni dengan rentang 2,4 GHz hingga 5 GHz

BAB II

PEDOMAN PENGELOLAAN PERANGKAT LUNAK

A. Pengembangan Sistem Informasi

1. Instalasi SIMRS melaksanakan kegiatan pengembangan dan pengelolaan sistem informasi di lingkungan RSUP dr. Soeradji Tirtonegoro yang terdiri atas aplikasi Sistem Informasi Manajemen Rumah Sakit (SIMRS) serta aplikasi lain yang mendukung implementasi SIMRS.
2. Pengembangan sistem informasi oleh Instalasi SIRS dilaksanakan dengan memperhatikan *master plan* pengembangan sistem informasi, kebijakan-kebijakan terkait, serta pertimbangan strategis lainnya.
3. Kegiatan pengembangan sistem informasi dilaksanakan dengan melibatkan unit kerja terkait sebagai pemilik proses bisnis maupun sebagai pengguna akhir sistem informasi.
4. Kegiatan pengembangan sistem informasi dilakukan dengan mengikuti prinsip daur hidup pengembangan perangkat lunak (*Software Development Life Cycle* / SDLC) yang terdiri dari tahap-tahap: perencanaan, analisis, perancangan, pengembangan, pengujian, implementasi, dan perawatan.

B. Analisis dan Perancangan Sistem Informasi

1. Permintaan pembuatan aplikasi oleh unit kerja diajukan melalui usulan tertulis kepada Direksi, dengan melampirkan penjelasan alur aplikasi yang terdiri input, proses, serta output yang diinginkan.
2. Instalasi SIMRS dapat mengundang unit kerja terkait untuk meminta penjelasan lebih mendalam mengenai aplikasi yang akan dikembangkan.
3. Analisis dan perancangan yang dibuat harus memperhatikan proses bisnis yang berjalan saat ini serta kebutuhan data dan informasi yang harus disediakan melalui aplikasi.
4. Setiap aplikasi yang dikembangkan dilengkapi dengan dokumen analisis yang setidaknya memuat rancangan basis data, rancangan tampilan, serta rancangan proses atau alur aplikasi.
5. Instalasi SIMRS membuat urutan prioritas pengembangan terhadap usulan pengembangan aplikasi yang diterima.

6. Sebelum kegiatan pengembangan aplikasi dimulai terlebih dahulu dilakukan pertemuan awal (*kick off meeting*) untuk memaparkan hasil analisis dan perancangan aplikasi kepada seluruh tim yang terlibat.

C. Pembuatan Kode Program

1. Kode sumber yang digunakan dalam pembuatan perangkat lunak ditulis menggunakan bahasa pemrograman dan *framework* yang telah disepakati dan diketahui bersama oleh seluruh Tim Pengembang.
2. Kode program yang dibuat dilengkapi dengan komentar yang dapat mempermudah dalam proses penelusuran ulang, proses *debugging*, serta pembuatan dokumentasi.
3. Kode program yang telah selesai ditulis disimpan pada server repositori khusus yang telah disediakan.
4. Penulisan kode program tidak dilakukan pada file aplikasi *production* atau langsung menyalin file dari server lokal, tetapi harus dilakukan sinkronisasi dan validasi terlebih dahulu dari server repositori.
5. Kode sumber sistem informasi atau aplikasi yang dibuat oleh tim pengembang merupakan milik rumah sakit dan disimpan pada server rumah sakit.
6. Kode sumber yang telah dibuat bersifat tertutup (*closed source*) yang tidak disebarkan secara utuh kepada publik.

D. Pengujian Aplikasi

1. Seluruh perangkat lunak yang telah diselesaikan proses pembuatannya harus diuji coba terlebih dahulu sebelum diupload ke repositori dan digunakan oleh pengguna aplikasi.
2. Pengujian dilakukan untuk menilai tingkat fungsionalitas modul / menu serta kesesuaiannya dengan proses bisnis yang telah ditentukan pada dokumen perancangan.
3. Proses pengujian dilakukan secara bertahap oleh *tester* internal Instalasi SIMRS dan tester dari perwakilan pengguna aplikasi.
4. Hasil pengujian yang telah dilaksanakan dituangkan dalam dokumen uji coba yang setidaknya mencantumkan daftar fitur yang telah dicoba, hasil uji coba, petugas tester, serta waktu pelaksanaan.
5. Aplikasi yang dinyatakan lolos uji coba maka akan dilanjutkan untuk proses implementasi.

6. Aplikasi yang dinyatakan belum lolos uji coba maka akan dikembalikan ke Tim Pengembangan untuk dilakukan perbaikan atau penyesuaian.

E. Serah Terima Aplikasi

1. Aplikasi yang telah dinyatakan selesai dan lolos uji coba akan diserahkan oleh Instalasi SIMRS selaku pengembang aplikasi kepada unit kerja pengelola aplikasi (PIC Aplikasi).
2. Unit kerja pengelola aplikasi melakukan persiapan penggunaan aplikasi oleh pengguna akhir yang terdiri atas kegiatan:
   a. Sosialisasi penggunaan aplikasi
   b. Membuat draft usulan SK Direktur Utama tentang pemberlakuan atau penggunaan aplikasi.
   c. Regulasi penggunaan aplikasi.
   d. Melengkapi master data aplikasi.

F. Penggunaan Perangkat Lunak Sistem Operasi

1. Setiap komputer yang didistribusikan ke unit kerja pengguna sudah terpasang sistem operasi yang siap digunakan.
2. Penggantian (instalasi ulang) sistem operasi komputer dilakukan oleh Instalasi SIMRS.
3. Pengguna yang memerlukan penggunaan sistem informasi khusus dapat mengganti sistem informasi yang sudah terpasang pada komputer dengan terlebih dahulu melaporkan kepada Instalasi SIMRS.
4. Pengguna menyediakan sendiri file *installer* sistem informasi khusus yang tidak terdistribusi secara bebas.

G. Penggunaan Aplikasi Pendukung Perkantoran

1. Instalasi SIMRS menyertakan aplikasi perkantoran standar dan sudah terpasang di dalam komputer pada saat distribusi ke unit kerja pengguna.
2. Aplikasi perkantoran dapat berupa aplikasi pengolah kata, aplikasi lembar kerja, aplikasi presentasi, aplikasi multimedia, serta aplikasi telekonferen.

3. Instalasi SIMRS melakukan pengaturan penggunaan aplikasi perkantoran pada komputer berdasarkan rencana peruntukan alat pengolah data yang telah ditetapkan.

H. Penggunaan Aplikasi Eksternal

1. Aplikasi eksternal diperoleh dari institusi di luar RSUP dr. Soeradji Tirtonegoro Klaten (Kementerian/Lembaga) yang didistribusikan untuk langsung digunakan oleh unit kerja terkait.
2. Aplikasi eksternal yang berupa aplikasi *stand alone* (berdiri sendiri) dipasangkan (*install*) langsung pada komputer pengguna.
3. Aplikasi eksternal yang berbentuk aplikasi terdistribusi dan memerlukan instalasi pada server dapat dipasang pada server rumah sakit.
4. Unit kerja pengguna aplikasi akan bertindak sebagai *Person In Charge* / PIC dan akan berkomunikasi dengan PIC di satuan kerja (Kementerian/Lembaga) pemilik atau pengembang aplikasi.
5. Unit kerja PIC aplikasi memberikan sosialisasi kepada pengguna akhir aplikasi (*end user*) di lingkungan RSUP dr. Soeradji Tortonegoro.
6. Apabila diperlukan, Instalasi SIMRS dapat mengembangkan fitur integrasi antara aplikasi eksternal dengan Aplikasi SIMRS sesuai petunjuk teknis yang diterbitkan oleh pengembangan aplikasi dan sesuai ketersediaan data pada basis data rumah sakit.

I. Website Rumah Sakit

1. Website rumah sakit merupakan website yang dikembangkan dan dikelola secara resmi oleh rumah sakit dan digunakan sebagai media komunikasi digital berbasis internet antara rumah sakit dengan masyarakat umum.
2. Pengembangan website
   a. Aplikasi website rumah sakit disediakan dan dikembangkan oleh Instalasi SIMRS.
   b. Instalasi SIMRS bertugas mengelola *domain* website, *hosting* dan file aplikasi, menangani *error* aplikasi website, serta melakukan backup *file* dan *database* website.

a. Unit kerja dapat mengusulkan penambahan menu pada website rumah sakit atau pembuatan halaman khusus dengan mengajukan usulan yang diketahui kepala unit kerja.

3. Pengelolaan Hosting
   a. *File website* ditempatkan pada hosting yang dapat diakses secara online dan dikelola secara mandiri oleh Instalasi SIMRS dengan akses penuh ke *hosting manager.*
   b. File pada *hosting* di-*backup* secara berkala dan disimpan pada server lokal. Backup yang disimpan terdiri dari file program dan basis data.
   c. Selain berupa file, website juga di-backup sebagai website lokal yang diakses secara *offline* (*localhost*).
   d. Pengadaan hosting dapat diperoleh melalui sewa layanan atau menggunakan infrastruktur mandiri yang tersedia di pusat data rumah sakit dengan memperhatikan kapasitas serta kapabilitas infrastruktur yag tersedia.
   e. Jika hosting diperoleh melalui layanan sewa, maka perpanjangan layanan harus ditinjau ulang sebelum masa sewa atau masa kontrak selesai.
4. Pengelolaan Domain
   a. Nama domain yang digunakan oleh website rumah sakit harus mengandung nama atau identitas yang secara spesifik merujuk ke RSUP dr. Soeradji Tirtonegoro sebagai pemilik website tersebut.
   b. Proses registrasi domain hanya dilakukan satu kali kecuali jika diputuskan untuk melakukan perubahan nama atau perpindahan penyedia domain tersebut.
   c. Domain dikelola secara mandiri oleh Instalasi SIMRS dan memiliki akses penuh ke *domain manager.*
   d. Sewa domain dilakukan secara reguler sesuai dengan anggaran yang ditetapkan. Perpanjangan sewa domain dilakukan sebelum tanggal jatuh tempo.

5. Pengelolaan Konten Website
   a. Website rumah sakit menampilkan informasi yang setidaknya terdiri atas profil rumah sakit, pelayanan rumah sakit, serta kegiatan rumah sakit,
   b. Informasi yang dipublikasikan pada website dibuat dengan mengikuti kaidah-kaidah publikasi, baik popular maupun ilmiah, serta tidak melanggar undang-undang yang berlaku.
   c. Informasi pada website dikelola oleh administrator website yang terdiri atas unit kerja yang ditunjuk berdasarkan kesesuaian antara konten informasi dengan tugas dan fungsi unit kerja tersebut.
   d. Administrator website bertugas untuk:
      - Mengumpulkan bahan untuk pembuatan konten website.
      - Membuat konten informasi serta melakukan validasai (*editing*).
      - Melakukan update konten secara berkala maupun insidental sesuai jenis informasi yang ditampilkan.
   e. Masing-masing administrator website memiliki hak akses (*username* dan *password*) untuk masuk ke halaman administrator.
6. Website Pendukung
   a. Website pendukung merupakan halaman website atau aplikasi berbasis web yang terpisah dari website rumah sakit tetapi merupakan bagian dari media publikasi dan pelayanan rumah sakit.
   b. Website pendukung dapat ditampilkan dalam bentuk subdomain dari website utama maupun nama domain lain dengan tetap menyertakan identitas RSUP dr. Soeradji Tirtonegoro.
   c. Pengelolaan website pendukung dilaksanakan oleh unit kerja yang terkait dengan konten atau fungsi yang terdapat pada website tersebut.

J. *Webservice* dan Interoperabilitas Sistem Informasi

1. Seluruh akses basis data internal RSUP dr. Soeradji Tirtonegoro dari sistem di luar SIMRS, baik input maupun output, harus dilakukan melalui web service.
2. Pembuatan *web service* untuk keperluan pihak di luar RSUP dr. Soeradji Tirtonegoro dilaksanakan berdasarkan permintaan resmi dan diketahui oleh direksi.

3. *Web service* rumah sakit dikembangkan dan dikelola secara mandiri oleh Instalasi SIMRS.
4. *Web service* diletakkan pada server lokal di dalam pusat data yang mempunyai IP Publik dan dapat diakses secara *online* melalui jaringan internet.
5. Informasi yang disajikan melalui *web service* harus dievaluasi dan dikonfirmasikan dengan unit kerja yang berwenang terhadap informasi tersebut.

K. Basis Data Terpusat

1. Penyimpanan Basis Data
   a. Basis data disimpan pada media penyimpanan menggunakan perangkat komputer yang secara khusus berfungsi sebagai server.
   b. Basis data transaksi SIMRS ditempatkan pada server khusus yang terpisah dari basis data untuk aplikasi lain, serta terdiri dari server utama dan server *backup.*
   c. Server basis data diletakkan di dalam Ruang Datacenter.
   d. Pengelolaan basis data memperhatikan aspek kemudahan dalam kegiatan pemeliharaan seperti pemantauan, dokumentasi, dan penyimpanan data.
2. Akses Basis Data
   a. Akses pada basis data baik untuk proses *create*, *read*, *update*, dan *delete* hanya dilakukan menggunakan melalui aplikasi yang terhubung dengan basis data tersebut.
   b. Proses transaksi terhadap basis data dilakukan oleh pengguna aplikasi sesuai dengan tugas dan kewenangannya.
   c. Dalam keadaan darurat, misalnya: terjadi kendala atau kerusakan pada aplikasi, basis data dapat diakses secara langsung melalui aplikasi sistem manajemen basis data (*Database Management System* / DBMS) oleh petugas administrator basis data (*Database Administrator*) atau petugas lain yang diberikan wewenang sesuai tugas dan kompetensinya.
   d. Aplikasi DBMS dapat diakses langsung melalui komputer server basis data dengan monitor yang diletakkan pada ruang server atau melalui aplikasi remote seperti *Virtual Privat Network* (VPN) atau Aplikasi *Remote Desktop.*

e. Setelah selesai digunakan, aplikasi DBMS harus ditutup kembali.

3. *Back Up* basis data
   a. Basis data dibackup minimal satu kali dalam sehari.
   b. File backup basis data ditempatkan pada komputer yang terpisah dari server.
   c. Backup basis data terdiri atas replikasi basis data dan file dump.

BAB III

PEDOMAN PENGELOLAAN ALAT PENGOLAH DATA

A. Perencanaan dan Pengadaan Alat Pengolah Data

1. Perencanaan
   a. Instalasi SIMRS mengelola perangkat keras yang digunakan sebagai alat pengolah data di dalam operasional SIMRS dan administrasi perkantoran, baik perangkat input, proses, maupun output.
   b. Unit Kerja menyampaikan usulan kebutuhan alat pengolah data melalui usulan Rencana Kerja Tahunan yang disusun dan dilaporkan setiap tahun.
   c. Perencanaan kebutuhan alat pengolah data oleh unit kerja harus mempertimbangkan: ketersediaan alat pengolah data pada unit kerja, komposisi pegawai, serta rencana kegiatan.
   d. Usulan kebutuhan alat pengolah data yang bersifat khusus (hanya untuk kegiatan pada unit kerja tertentu) harus disertai dengan proposal, justifikasi, spesifikasi, serta referensi harga dari penyedia.
2. Pengadaan
   a. Pengadaan alat pengolah data dilaksanakan sesuai prioritas kebutuhan berdasarkan usulan unit kerja yang tertuang di dalam Rencana Kerja Tahunan (RKT) serta Rencana Belanja dan Anggaran (RBA) yang telah disusun serta tercantum pada RKA K/L tahun berjalan.
   b. Usulan pengadaan alat pengolah data di luar rencana yang telah ditetapkan dapat dilaksanaan dengan sepengetahuan Unit Kerja Penyusun Anggaran dan disetujui oleh Direksi.
   c. Realisasi pengadaan alat pengolah data dilaksanakan sesuai mekanisme pengadaan barang dan jasa yang berlaku.
   d. Pengadaan alat pengolah data yang merupakan peminjaman dari penyedia dilaksanakan sesuai kesepakatan yang diatur dalam kontrak atau perjanjian kerja sama.

B. Pengelolaan Suku Cadang dan Aksesoris Alat Pengolah Data

1. Proses pengadaan suku cadang alat pengolah data dilaksanakan melalui kerja sama dengan rekanan penyedia dalam bentuk kontrak payung/ pembelian satuan.

2. Pemilihan rekanan penyedia dilaksanakan melalui mekanisme pengadaan barang dan jasa yang berlaku.
3. Suku cadang alat pengolah data yang telah diperoleh dari penyedia disimpan dan dikelola oleh Instalasi SIMRS.
4. Instalasi SIMRS melaksanakan pencatatan persediaan suku cadang alat pengolah data yang setidaknya meliputi data pembelian dan pengeluaran atau mutasi.

C. Distribusi Perangkat Keras

1. Instalasi SIMRS menyusun rencana distribusi alat pengolah data bersamaan dengan proses pengusulan anggaran.
2. Distribusi alat pengolah data yang diperoleh dari proses pengadaan dilaksanakan dengan melibatkan penyedia pemenang lelang.
5. Uji fungsi terhadap alat pengolah data yang diistribusikan dilaksanakan dengan melibatkan penyedia pemenang lelang dan unit kerja pengguna.
6. Unit kerja penerima alat pengolah data menyediakan tempat yang cukup dan layak untuk meletakkan alat pengolah data yang akan dipasang.
7. Instalasi SIMRS melaporkan distribusi alat pengolah data kepada unit kerja Pengelola BMN.
8. Masing-masing unit kerja bertanggung jawab terhadap keberadaan, keamanan dan penggunaan alat pengolah data yang telah diterima. Tidak diperkenankan melakukan pengubahan atau penggantian komponen alat pengolah data tanpa seijin Instalasi SIMRS.
9. Alat pengolah data dilarang untuk digunakan dalam segala bentuk kegiatan yang bersifat kontra produktif atau bertentangan dengan peraturan maupun perundang-undangan yang berlaku.

D. Perawatan Alat Pengolah Data

1. Satuan Kerja yang membutuhkan perbaikan alat pengolah data menyampaikan informasi atau laporan kepada Instalasi SIMRS.
2. Informasi yang disampaikan setidaknya terdiri dari: jenis dan merek alat, gangguan yang terjadi, gejala dan tanda selama gangguan, periode atau frekuensi gangguan, serta tindakan yang pernah dilakukan.
3. Instalasi SIMRS dapat melakukan konfirmasi ulang atau pemeriksaan awal terhadap laporan kerusakan yang diterima.

4. Kerusakan atau kegagalan fungsi alat pengolah data yang diakibatkan oleh kegiatan yang menyimpang dari kebijakan yang berlaku dilaporkan secara tertulis oleh kepala unit kerja.
5. Proses perbaikan alat pengolah data dapat dilaksanakan di ruang Instalasi SIMRS (bengkel hardware) atau di lokasi kerusakan.
6. Alat pengolah data yang sudah tidak layak digunakan dapat dikumpulkan dan dikelola di gudang Instalasi SIMRS sebelum dikembalikan kepada Pengelola BMN.
7. Kegiatan perawatan sarana dan infrastruktur teknologi informasi dilakukan secara rutin maupun insidental serta dilaporkan kepada Kepala Instalasi SIMRS.

E. Perangkat Keras Bersumber Kerja sama Operasi di Luar SIMRS

1. Perangkat keras yang merupakan bagian dari kontrak Kerjasama Operasional (KSO) atau merupakan bagian dari paket alat lain di luar alat pengolah data SIMRS maka pengelolaan dilaksanakan oleh unit kerja PIC alat bersama dengan pihak rekanan kerja sama.
2. Apabila diperlukan atau dalam kondisi mendesak, Instalasi SIMRS akan melakukan tindakan pemeriksaan secara terbatas pada alat tersebut.

F. Kerja Sama Pemeliharaan Perangkat Keras

1. Instalasi SIMRS menjalin Kerjasama dengan pihak ketiga/ rekanan untuk melaksanakan kegiatan pemeliharaan perangkat keras.
2. Kerja sama dilaksanakan dalam bentuk perbaikan alat maupun pengadaan dan penggantian suku cadang.
3. Penunjukan rekanan Kerja sama pemeliharaan perangkat keras dilaksanakan berdasarkan mekanisme pengadaan barang dan jasa oleh Unit Layanan Pengadaan barang dan Jasa.

BAB IV
PEDOMAN PENGELOLAAN INFRASTRUKTUR DAN JARINGAN KOMPUTER

A. Pemasangan Jaringan Utama

1. RSUP dr. Soeradji Tirtonegoro menggunakan jalur fiber optik sebagai Jaringan utama/ *backbone* komunikasi data lokal (*Local Area Network*).
2. Jalur antara datacenter dengan switch utama (*core switch*) pada tiap segmen jaringan dihubungan secara langsung dalam bentuk topologi *star.*
3. Pemasangan kabel fiber optik dilakukan sengan cara ditanam di bawah tanah dengan kedalaman minimal 50 cm. Jika tidak dimungkinkan unuk dibuat jalur di bawah tanah maka dibuat jalur lain tetapi kabel tetap terlindung.
4. Seluruh kabel fiber optik yang terpasang dilindungi dengan kabel pembungkus luar (kabel *subduct*), pipa besi, atau pelindung lain yang kuat dan aman.

B. Jaringan Distribusi Kabel

1. Distribusi jaringan kabel ke pengguna akhir ditarik melalui kabel UTP.
2. Tersedia outlet distribusi yang langsung terhubung dengan switch pada ruang-ruang yang telah direncanakan.
3. Apabila terjadi kekurangan outlet dalam ruangan maka dibuat outlet tambahan dengan switch hub.
4. Dibuat segmentasi jalur berbasis *Virtual LAN* untuk memisahkan akses masing-masing kategori jaringan.
5. Setiap perangkat memiliki alamat IP berdasarkan pembagian segmen jaringan yang ditentukan oleh administrator.
6. Pemasangan kabel jaringan diberi pelindung luar/ pipa dan diletakkan pada jalur yang aman (tidak basah, tidak sejalur dengan aliran listrik).
7. Setiap kabel yang masuk ke switch diberi label/ tag untuk mempermudah melacak jalur pada ujung outlet dan switch.

C. Jaringan Distribusi Nirkabel

1. Distribusi jaringan nirkabel hingga ke pengguna akhir dibuat menggunakan perangkat *access point* yang memancarkan sinyal WiFi.

2. Lokasi hotspot diprioritaskan pada lokasi-lokasi tertentu yang diijinkan untuk mengakses jaringan secara nirkabel, seperti: area pengunjung, ruang perawatan, dan ruang pertemuan.
3. Apabila diperlukan akses nirkabel pada area blank spot (tanpa sinyal WiFi) atau untuk keperluan insidental dan khusus maka akan dipasang access point tambahan.
4. Setiap perangkat yang akan mengakses jaringan melalui jalur nirkabel harus mendapatkan persetujuan dari administrator.
5. Seluruh perangkat *access point* terdaftar dalam *controller* yang dikelola oleh administrator jaringan.

D. Penggunaan Internet

1. Layanan jaringan internet RSUP dr. Soeradji Tirtonegoro tersedia dalam 24 jam sehari dan 7 hari dalam seminggu, baik melalui jalur kabel maupun nirkabel.
2. Instalasi SIMRS memantau penggunaan jaringan internet dan memiliki kewenangan untuk membatasi serta mengatur penggunaan jaringan internet sesuai kebutuhan dan kepentingannya.
3. Setiap pengguna yang akan mengakses Internet harus melakukan registrasi atau melalui perangkat yang telah mendapatkan hak akses dari administrator.
4. Koneksi internet di RSUP dr. Soeradji Tirtonegoro dapat digunakan oleh: Direksi, seluruh pegawai, peserta didik, pasien, pengunjung, dan tamu.
5. Fasilitas koneksi internet yang tersedia dilarang untuk digunakan dalam segala bentuk kegiatan yang bersifat kontra produktif atau bertentangan dengan peraturan maupun perundang-undangan yang berlaku.

E. Datacenter

1. Fisik Bangunan Datacenter
   a. Ruang datacenter dikelola oleh Instalasi SIMRS.
   b. Ruang datacenter dilengkapi dengan fasilitas:
      - Listrik dengan jalur khusus yang terhubung dengan genset
      - Pendingin ruangan
      - Fasilitas pencahayaan yang cukup
      - Sistem pemadam kebakaran
      - Sistem pemantauan keamanan

c. Bangunan datacenter memisahkan susunan perangkat server dengan switch distribusi jaringan.
d. Komputer server yang digunakan mempunyai cadangan catu daya listrik menggunakan UPS minimal 5.000 VA.
e. Pemasangan semua peralatan seperti: rak, server, kabel, pendingin ruangan, panel kelistrikan, serta pemadam api di ruang datacenter harus mengikuti standar baku pemasangan masing-masing peralatan.

2. Akses ruangan datacenter.
   a. Ruang datacenter berada dalam jangkauan pengawasan Instalasi SIMRS.
   b. Ruang datacenter merupakan ruang khusus dan tertutup yang hanya dapat diakses secara terbatas.
   c. Ruang datacenter memiliki sistem keamanan fisik yang terdiri dari kunci ruangan maupun akses pintu berbasis biometrik.
   d. Seluruh aktifitas di dalam ruang datacenter harus sepengetahuan dan seijin dari pengelola

F. *Disaster Recovery Center*

1. Ruang DRC Inhouse berada pada lokasi yang terpisah dengan lokasi Ruang Datacenter tetapi masih dalam jangkauan dan pengamatan Instalasi SIMRS.
2. Ruang DRC Exhouse berada pada lokasi di rumah sakit lain yang berjarak lebih dari 100 kilometer dari lokasi Ruang Datacenter serta dapat diakses secara remote.
3. Penempatan DRC Exhouse di atur secara khusus melalui Perjanjian Kerjasama.
4. DRC menyimpan perangkat aktif yang dapat segera digunakan apabila terjadi masalah pada datacenter.

BAB V

PEDOMAN OPERASIONAL DAN PERAWATAN SISTEM INFORMASI

A. Kerahasiaan Data dan Informasi

1. Seluruh Informasi yang tersimpan pada server basis data hanya boleh diakses pengguna sesuai kewenangan dan hak akses yang dimiliki.
2. Data - data yang bersifat sangat rahasia seperti data pasien dan data transaksi keuangan tidak boleh dipublikasikan tanpa persetujuan pejabat terkait.
3. Mekanisme publikasi data diatur secara terpisah oleh kebijakan yang berlaku pada unit kerja pengelola data.

B. Kontrol Akses Pengguna

1. Seluruh pengguna SIMRS diberikan akses secara berjenjang sesuai tugas dan kewenangan masing-masing serta dilakukan vaidasi secara berkala.
2. Permohonan hak akses pengguna dilakukan secara tertulis kepada Kepala Instalasi SIMRS.
3. Kepala unit kerja wajib menyampaikan update status kepegawaian yang berimbas pada perubahan hak akses kepada Kepala Instalasi SIMRS.

C. Penggunaan SIMRS

1. Masuk ke Aplikasi
   a. Pengguna yang akan mengakses SIMRS harus melakukan proses login ke aplikasi dengan data pengguna (username dan password) yang diperoleh dari Instalasi SIMRS.
   b. Setiap pengguna bertanggung jawab terhadap penggunaan data login yang dimiliki dan tidak diperbolehkan melakukan tukar menukar data login antar pengguna.
   c. Setiap pengguna hanya mendapatkan hak akses transaksi sesuai tugas dan fungsi yang dilaksanakan.
2. *Input* Transaksi
   a. Transaksi dimasukkan (*input*) ke dalam SIMRS menggunakan form yang tersedia di dalam aplikasi sesuai dengan jenis transaksi yang terjadi.

b. Transaksi dimasukkan ke dalam SIMRS oleh petugas yang memiliki hak akses masuk ke aplikasi dan harus berdasarkan bukti transaksi yang valid.
c. Proses input transaksi dilakukan secara realtime atau sesegera mungkin setelah pelayanan dilakukan. Apabila terjadi gangguan yang menyebabkan transaksi tidak dapat dilaksanakan secara realtime maka akan diatur dengan kebijakan tersendiri yang diketahui oleh Direksi.

3. *Output* Transaksi
   a. Aplikasi SIMRS memiliki fasilitas untuk mencetak bukti transaksi yang telah dimasukkan. Bukti transaksi yang telah dicetak disimpan dan dikelola oleh masing-masing unit kerja.
   b. Aplikasi SIMRS memiliki fasilitas untuk melihat dan mencetak laporan transaksi yang telah di masukkan ke dalam aplikasi sesuai format yang digunakan oleh satuan kerja.

D. Penanganan Kesalahan Transaksi SIMRS

1. Pelaporan kesalahan transaksi kepada Instalasi SIMRS harus disertai dengan bukti transaksi.
2. Pengubahan data transaksi dilakukan sesuai bukti transaksi yang diserahkan dan harus diketahui oleh atasan langsung staf.
3. Pengubahan data transaksi, baik berupa penambahan, penggantian, atau pengurangan, yang menyebabkan berubahnya isi laporan keuangan dan pelayanan yang telah disusun maka harus mendapatkan persetujuan dari unit kerja terkait.

E. Penanganan *Error* dan *Bug* Aplikasi

1. Pengguna menyampaikan laporan error aplikasi kepada Instalasi SIMRS dengan melampirkan bukti error.
2. Penanganan error aplikasi dilakukan setelah melalui validasi dan analisa untuk mengetahui sumber kesalahan.
3. Instalasi SIMRS memberikan umpan balik kepada pengguna apabila perbaikan sudah diselesaikan.

F. Manajemen Data dan Informasi

1. Permintaan data dan laporan di luar menu laporan pada Aplikasi SIMRS dajukan melalui permintaan tertulis dan ditandatangani oleh kepala unit kerja.
2. Permintaan laporan harus menyertakan contoh format yang diinginkan serta batas waktu pengumpulan.
3. Instalasi SIMRS memberikan informasi kepada pemohon apabila laporan telah diselesaikan.

G. Pengubahan dan Penambahan Modul pada Aplikasi

1. Usulan pengubahan atau penambahan modul dilakukan secara tertulis oleh kepala unit kerja.
2. Permohonan setidaknya memuat informasi fungsi yang akan ditambahkan, alasan penambahan modul, gambaran proses pada modul yang akan ditambahkan.
3. Usulan akan divalidasi oleh Instalasi SIMRS untuk menentukan kelayakan penambahan modul.

BAB VI
PEDOMAN PENGELOLAAN SUMBER DAYA MANUSIA TEKNOLOGI INFORMASI

A. Pengembangan SDM Teknologi Informasi

1. Aplikasi SIMRS dikembangkan sebagai platform yang mengintegrasikan seluruh layanan teknologi informasi dai rumah sakit, sehingga seluruh staf rumah sakit merupakan pengguna Aplikasi SIMRS.
2. Instalasi SIMRS Bersama PIC Aplikasi melaksanakan bimbingan teknis penggunaan aplikasi kepada pengguna sesuai hak akses yang dimiliki.
3. Instalasi SIMRS Bersama unit kerja pengelola pendidikan dan pelatihan mengadakan pelatihan pengembangan dan pengelolaan teknologi informasi.

B. Kerahasiaan Data dan Informasi oleh Staf

1. Seluruh staf Instalasi SIMRS harus melaksanakan sumpah untuk menjaga kerahasaiaan data serta tidak menyalakgunakan kewenangan serta hak akses yang dimiliki.
2. Seluruh akses ke dalam perangkat lunak, perangkat keras, jaringan, maupun data rumah sakit harus dilakukan dengan mengikuti aspek legalitas administratif maupun teknis.
3. Sosialisasi untuk meningkatkan kesadaran pengguna terhadap pentingnya keamanan informasi beserta tanggung jawab dan konsukuensinya dilakukan secara berkala kepada seluruh pegawai.

C. *Resign* dan Mutasi

1. Staf Instalasi SIMRS yang mutasi ke unit kerja lain atau resign sebagai staf RSUP dr. Soeradji Tirtonegoro Klaten harus membuat surat perjanjian menjaga kerahasiaan (Non-Disclosure Agreement).
2. Setiap terdapat perubahan data personalia dan kepegawaian yang berhubungan dengan operasional SIMRS maka Instalasi SIMRS akan mendapat tembusan pemberitahuan dari unit kerja yang berwenang.

BAB VII

PEDOMAN KEAMANAN SISTEM INFORMASI DAN JARINGAN

A. Prinsip Kemanan Sistem Informasi

1. Kerahasian

   Sistem informasi yang dikembangkan harus menjamin bahwa data dan informasi yang dihasilkan hanya diakses oleh pihak-pihak yang tepat. Kebocoran data dan informasi dapat menciptakan suasana dan situasi yang dapat merugikan organisasi.

2. Ketersediaan

   Sistem informasi yang dimiliki harus mampu menyediakan data dan informasi bagi pihak-pihak yang memerlukan sesuai tugas dan kewenangannya.

3. Integritas

   Sistem dan subsistem yang tersedia harus mampu menyajikan data dan informasi yang lengkap dan valid, sehingga dapat memberikan gambaran yang lengkap dan akurat dari sistem fisik yang diwakilinya.

B. Identifikasi Pengguna

1. Setiap pengguna mempunyai data login yang terdiri dari username dan password pribadi. Tidak diperkenankan melakukan penyebaran (share) atau tukar menukar data login antarpenggua.
2. Penggunaan data login beserta seluruh akibat yang ditimbulkan adalah tanggung jawab masig-masing pengguna.
3. Permintaan data login untuk pengguna dilakukan secara tertulis dengan diketahui oleh pimpinan unit kerja pengguna.
4. Instalasi SIMRS secara berkala melaksanakan pemantauan terhadap penggunaan hak akses oleh pengguna beserta kepatuhan atas kewajiban dan larangannya masing-masing.

C. Akses Informasi Rumah Sakit

1. Setiap pengguna hanya diijijnkan untuk mengakses informasi sesuai wewenang hak akses yang diberikan melalui data login.
2. Semua data dan informasi yang ada dalam perangkat komputer maupun jaringan data rumah sakit adalah milik rumah sakit.

3. Rumah sakit mempunyai hak untuk mengawasi file-file yang disimpan maupun akses internet untuk tujuan perawatan, auditing, keamanan data atau investigasi terhadap fakta-fakta dari pelanggaran hukum atau gangguan terhadap peraturan rumah sakit.
4. Semua pegawai dilarang memberikan informasi apapun kepada pihak luar tanpa ijin dari direksi.

D. Keamanan Jaringan

1. Pengaturan keamanan akses jaringan data rumah sakit dikelola dengan menggunakan perangkat firewall yang dilengkapi dengan antivirus.
2. Instalasi SIMRS telah mengatur konfirgurasi jaringan komputer pada masing-masing perangkat dan tidak diperkenankan untuk diubah oleh pengguna.
3. Setiap pengguna hanya diijinkan untuk menggunakan koneksi internet melalui konfigurasi yang telah diautur oleh Instalasi SIMRS.
4. Koneksi jaringan lokal rumah sakit secara remote melalui jalur Virtual Private Network (VPN) dapat dilakukan setelah mendapat akses dari administrator.
5. Setiap pengguna harus segera melaporkan kepada Instalasi SIMRS apabila menemui peringatan atau tampilan tidak lazim pada komputer yang digunakan.
6. Instalasi SIMRS melakukan pengujian kerentanan (*vulnerability assessment*) secara berkala, baik oleh tim internal maupun bekerjasama dengan pihak eksternal.
7. Hasil pengujian kerentanan didokumentasikan dan dievaluasi secara berkala.

E. Bentuk Pelanggaran

1. *Spoofing*

   Melakukan akses yang tidak sah ke suatu komputer, informasi, atau suatu aplikasi, dengan berpura-pura memalsukan identitas sehingga seolah-olah sebagai host atau pemilik sebenarnya.
2. *Tampering*

   Mengubah data yang ada di dalam database tanpa melalui hak akses yang benar.

3. *Repudiation*

   Membuat sebuah sistem atau *database* dengan sengaja salah, atau sengaja menyisipkan *bugs*, atau menyertakan virus tertentu didalam aplikasi sehingga dapat digunakan untuk mengakses sistem pada suatu saat.

4. *Information disclosure*

   Membuka atau membaca sebuah informasi tanpa memiliki hak akses atau membaca sesuatu tanpa mempunyai hak otorisasi.

5. *Denial of service*

   Melumpuhkan sistem yang dijadikan target sehingga sistem tersebut tidak dapat menyediakan servis-servisnya atau tingkat servis menurun dengan drastis.

6. *Elevation of priviledge*

   Menyalahgunakan wewenang yang dimiliki untuk mengakses sebuah sistem demi kepentingan pribadi.

F. Penanganan Insiden keamanan Informasi

1. Insiden keamanan sistem informasi dapat mengakibatkan berbagai macam risiko, mulai dari yang ringan hingga yang sangat berat atau fatal, sehingga harus dikedepankan upaya-upaya pencegahan dan antisipasi terhadap terjadinya insiden.
2. Teknik-teknik pengendalian risiko keamanan sistem informasi yang dapat dilakukan adalah
   a. Pengaturan hak akses (*Access Control*)

      Seluruh aktivitas pengguna di dalam jaringan sistem informasi harus dibatasi berdasarkan hak akses serta dapat dipantau. Sistem informasi menyediakan fasilitas untuk memantau aktivitas pengguna atau minimal mengetahui jejak pengguna di dalam sistem.

   b. Memasang Proteksi

      Memasang sistem proteksi jaringan sistem informasi untuk memperkecil kemungkinan terjadinya akses dari pihak yang tidak berkepentingan. Metode yang digunakan adalah: pengguaan antivirus pada jaringan, penggunaan perangkat *firewall*, serta optimalisasi sistem sekuriti dari sistem operasi.

   c. Pemantau adanya serangan

Memasang sistem deteksi danpemantauan terhadap serangan yang terjadi pada jaringan sistem operasi.

d. Penggunaan Enkripsi untuk meningkatkan keamanan

   Melakukan enkripsi atau pengacakan pada data yang dikirim melalui koneksi jaringan komputer, sehingga memperkecil kemungkinan penyadapan.

3. Tindakan penanganan pasca-insiden keamanan sisten informasi dilaksanakan mengikuti kerangka kerja (*framework)* forensik digital yang setidaknya meliputi Langkah-langkah: Identifikasi kejadian, Pengumpulan barang bukti, Analisa Barang Bukti, dan Pelaporan.

BAB VIII
PEDOMAN MANAJEMEN RISIKO

A. Pengelolaan Risiko

1. Instalasi SIMRS melaksanakan kegiatan manajemen risiko atas aspek-aspek implementasi teknologi di rumah sakit.
2. Dokumen manajemen risiko disusun sesuai ketentuan dan sandar yang telah ditetapkan dalam kebijakan manajemen risiko di rumah sakit.
3. Kegiatan manajemen risiko terdiri atas kegiatan perencanaan, pengendalian risiko, serta monitoring dan evaluasi.
4. Aspek-aspek risiko yang dikelola mewakili unsur-unsur kegiatan impementasi teknologi insormasi yang terdiri atas: *software*, *hardware*, jaringan, serta tata kelola.

B. Identifikasi Risiko

Risiko yang berpotensi terjadi di instalasi SIMRS serta harus diantisipasi serta ditangani secepat mungkin adalah:

1. Kegagalan Pengembangan Sistem
2. Kegagalan Implementasi Sistem
3. Gangguan Jaringan Komunikasi dan Data Internal
4. Gangguan Jaringan Komunikasi dan Data Eksternal
5. Insiden Keamanan Sistem Informasi
6. Kegagalan Pengadaan Perangkat Keras
7. Kerusakan Infrastruktur
8. Kehilangan Perangkat Keras
9. Kecelakaan Kerja Staf IT

C. *Disaster Recovery Plan*

1. Instalasi SIMRS membuat dokumen rencana pemulihan bencana teknologi informasi (IT-DRP).
2. Dokumen IT-DRP dilakukan uji coba dengan melibatkan seluruh pengguna sistem informasi.
3. Dokumen IT-DRP dievaluasi secara berkala serta disesuiak dengan perkembangan situasi, teknologi, serta kebijakan lain yang berkaitan.

BAB IX
PENUTUP

Demikian dokumen ini disusun sebagai panduan dalam pelayanan teknologi informasi di RSUP dr. Soeradji Tirtonegoro Klaten.

Sebagai sebuah dokumen yang dinamis, maka panduan ini akan terus dikembangkan serta disesuaikan dengan perkembangan situasi, teknologi, serta regulasi lain yang berkaitan dengan substansi dokumen ini.