

PEDOMAN PELAYANAN

*Kami Peduli
Kesehatan Ginjal Anda*



RUMAH SAKIT KHUSUS GINJAL NY. R.A. HABIBIE

Jl. Tubagus Ismail No.46 Telephone. (022) 2501985 Fax. (022) 2501984

Website : www.rskghabibie.com Email : rskginjal@yahoo.com

Bandung - Jawa Barat

LEMBAR PENGESAHAN

PEDOMAN PELAYANAN URUSAN IT

Bandung, Februari 2020

Disusun,

Muhammad Amran Hakim Siregar, S.Tr.Kom

Kepala. Urusan IT

Disetujui,

Ditetapkan,

Iwan Kustiwan, S.H

Kabag. Umum dan Keuangan

dr. Qania Mufliani, MM

Direktur

DAFTAR ISI

COVER DEPAN

LEMBAR PENGESAHAN

DAFTAR ISI.....	1
DAFTAR TABEL	4
DAFTAR GAMBAR	5
BAB I	6
PENDAHULUAN	6
1.1. Latar Belakang	6
1.2. Tujuan.....	7
1.2.1. Tujuan Umum	7
1.2.2. Tujuan Khusus	7
1.3. Ruang Lingkup.....	7
1.4. Batasan Operasional	8
1.5. Landasan Hukum	8
BAB II	9
STANDAR KETENAGAAN	9
2.1. Kualifikasi Sumber Daya Manusia	9
2.2.1. Ka. Urusan IT	9
2.2.2. Wakil Ka. Urusan IT	9
2.2.3. Staff IT.....	10
2.3. Distribusi Ketenagaan	10
2.4. Pengaturan Pelayanan	10
BAB III	12
STANDAR FASILITAS	12
3.1. Denah Ruang.....	12
3.1.1. Server	12
3.1.2. Meja Ka. Urusan IT	12
3.1.3. Meja Wakil Ka. Urusan IT	12
3.1.4. Meja Staff Urusan IT	12
3.2. Standar Fasilitas	13
3.2.1. Fasilitas Ruang IT.....	13

3.2.2. Fasilitas Server.....	13
BAB IV	14
TATA LAKSANA PELAYANAN.....	14
4.1. Jenis Pelayanan	14
4.2. Tata Kerja Urusan IT	16
4.2.1. Sistem Jaringan Data	16
4.2.2. Pengukuran Kinerja dan Kapasitas Jaringan Data	17
4.2.3. <i>Back up</i> Jaringan Data	18
4.2.4. Pengendalian Akses terhadap Jaringan Data	18
4.2.5. Penggunaan Jaringan Internet	19
4.2.6. Penggunaan Jaringan Nirkabel	20
4.2.7. Pengelolaan <i>Database</i>	20
4.2.8. Sistem <i>Back up</i>	20
4.2.9. Standar Tingkat Layanan (<i>Service Level</i>)	21
4.2.10. <i>Technical Support</i>	21
4.2.11. IT Logistik.....	21
4.2.12. Penilaian Risiko	22
4.2.13. IT Aset Manajemen.....	22
4.2.14. Pengelolaan Aset <i>Hardware</i>	23
4.2.15. Pengelolaan Aset <i>Software</i> dan <i>License</i>	23
4.2.16. Penghapusan Aset IT.....	24
4.2.17. Manajemen Perubahan Sistem Operasional	24
4.2.18. Manajemen Perubahan Konfigurasi Sistem Jaringan	25
4.2.19. Manajemen Perubahan Konfigurasi Sistem Server Operasional	25
4.2.20. Pengendalian Hak Akses	25
4.3. Tata Kerja IT <i>Development</i>	26
4.3.1. Rencana Kerja Pengembangan Sistem	26
4.3.2. Manajemen Proyek dan Pengembangan Sistem.....	26
4.3.3. Metodologi	27
4.3.4. <i>IT Quality Assurance</i>	27
4.3.5. Pengendalian Pengembangan Sistem	28
4.3.6. Perencanaan / Analisa	28
4.3.7. Pengadaan	28

4.3.8. Perancangan.....	28
4.3.9. Pemrograman	29
4.3.10. Pengujian.....	30
4.3.11. <i>System Deployment</i>	31
4.3.12. Perlindungan Terhadap Program Asli dan <i>Source Code</i> Aplikasi	

32

BAB V	33
LOGISTIK.....	33
BAB VI	34
KESELAMATAN PASIEN	34
6.1. Manajemen Risiko Keselamatan Pasien	34
6.2. Pencegahan dan Pengendalian Infeksi	35
BAB VII	36
KESELAMATAN KERJA	36
7.1. Penggunaan APD sesuai standar	36
7.2. Pembuangan limbah sesuai dengan jenisnya	36
7.3. Pemasangan kabel sesuai dengan prosedur	36
BAB VIII	37
PENGENDALIAN MUTU	37
8.1. Indikator Mutu	37
8.2. Monitoring	37
8.3. Evaluasi	37
8.4. Pelaporan	38
8.5. <i>Continous Improvement</i>	38
BAB IX	39
PENUTUP	39
COVER BELAKANG	

DAFTAR TABEL

Tabel 2. 1 Distribusi Ketenagaan	10
Tabel 3. 1 Fasilitas Ruang IT	13
Tabel 3. 2 Fasilitas Server	13
Tabel 4. 1 Service yang Diberikan oleh Urusan IT	14
Tabel 4. 2 Layanan Urusan IT kepada Urusan/Instalasi Rumah Sakit.....	15
Tabel 4. 3 Tugas dan Layanan IT	16
Tabel 5. 1 Perangkat Keras	33
Tabel 5. 2 Perangkat Lunak	33

DAFTAR GAMBAR

Gambar 3. 1 Denah Ruang.....	12
------------------------------	----

BAB I

PENDAHULUAN

1.1. Latar Belakang

Rumah sakit sebagai salah satu sarana pelayanan kesehatan terus mengalami pertumbuhan baik dari segi populasi rumah sakit, jumlah tempat tidur ataupun tingkat pelayanan. Kebutuhan akan layanan rumah sakit yang bermutu semakin meningkat seiring dengan semakin baiknya perekonomian dan derajat kesehatan masyarakat. Dalam beberapa tahun belakangan ini, industri rumah sakit Indonesia telah mengalami perkembangan yang cukup berarti. Terbukti, tidak saja pemerintah yang memang berkewajiban menyediakan jasa layanan kesehatan kepada masyarakat, para pelaku bisnis pun kini semakin aktif berinvestasi di industri rumah sakit Indonesia. Hal ini yang menjadi mendorong bermunculannya berbagai rumah sakit swasta baru dalam kurun waktu beberapa tahun terakhir ini.

Dengan banyaknya rumah sakit swasta yang bermunculan, sudah pasti tingkat persaingan akan semakin sengit. Rumah sakit dituntut untuk meningkatkan kinerja dan daya saing sebagai badan usaha dengan tidak mengurangi misi sosial yang dibawanya. Rumah sakit harus merumuskan kebijakan-kebijakan strategis antara lain efisiensi dari dalam (Organisasi, manajemen serta SDM) serta harus mampu secara cepat dan tepat mengambil keputusan untuk peningkatan pelayanan kepada masyarakat agar dapat menjadi organisasi yang responsif, inovatif, efektif, efisien dan menguntungkan.

Teknologi merupakan berbagai hal yang dapat membantu kegiatan atau aktivitas manusia. Kemajuan teknologi pada saat ini sudah berkembang pesat. Kemajuan ini mencakup berbagai bidang kehidupan manusia, termasuk pula dalam bidang kesehatan. Saat ini sudah banyak bukti dari peranan teknologi dalam bidang kesehatan. Salah satunya adalah peran dalam meningkatkan mutu pelayanan medis

Peningkatan mutu pelayanan medis tidak terlepas dari ketersediaan fasilitas pelayanan kesehatan, dalam hal ini rumah sakit, untuk menerapkan sistem informasi rumah sakit berbasis komputer. Sistem ini digunakan untuk

mendukung perubahan serta perbaikan bagi semua aspek dan bidang yang terkait, baik dari segi sarana prasarana financial, perlengkapan alat medis maupun sumber daya manusia.

Dengan adanya Urusan Teknologi Informasi diharapkan masalah yang timbul karena proses dengan cara konvensional dapat dikurangi yang tentunya berdampak pada peningkatan mutu pelayanan rumah sakit secara keseluruhan. Maka dengan ini disusunlah **“Pedoman Pelayanan Urusan Teknologi Informasi RS. Khusus Ginjal Ny.R.A.Habibie”**.

1.2. Tujuan

1.2.1. Tujuan Umum

Sebagai acuan dalam penyusunan kebijakan, prosedur dan segala proses di bidang *Information Technology* (IT) di RS. Khusus Ginjal Ny. R.A. Habibie.

1.2.2. Tujuan Khusus

Dalam menjalankan kegiatan operasional dan manajemen, rumah sakit didukung oleh sistem *Information Technology* (IT). Penggunaan IT memiliki dampak yang dapat menimbulkan risiko terhadap terganggunya operasional perusahaan, reputasi serta kerahasiaan, integritas dan ketersediaan data dan informasi. Untuk memitigasi hal tersebut, diperlukan suatu proses pengendalian dan pengawasan yang dituangkan dalam suatu Pedoman Tata Kerja yang mengatur penerapan IT dalam kegiatan usaha RS. Khusus Ginjal Ny. R.A. Habibie, untuk itu pedoman ini dibuat bertujuan :

1. Sebagai acuan dalam melaksanakan pelayanan Teknologi Informasi.
2. Sebagai dasar hukum untuk perlindungan terhadap kegiatan yang dilakukan di Urusan Teknologi Informasi.
3. Sebagai dasar dalam setiap prosedur kegiatan yang dilaksanakan di Urusan Teknologi Informasi

1.3. Ruang Lingkup

Ruang lingkup Pedoman Pelayanan Urusan IT di lingkungan RS. Khusus Ginjal Ny. R.A. Habibie meliputi :

1. Sistem Informasi lingkup intranet dan internet serta unsur pendukung aplikasi.
2. Unsur pendukung Manajemen Sistem Informasi.
3. Topologi Jaringan.
4. Standar penggunaan sistem dan operasional komputer.
5. Tugas dan tanggung jawab sistem dengan lingkup intranet, internet dan operasional komputer.

1.4. Batasan Operasional

Pedoman ini mengatur keseluruhan aspek kegiatan pengelolaan sistem IT Operasional yang berada di bawah Urusan IT, serta kegiatan pengembangan sistem yang berada di bawah Urusan IT.

1.5. Landasan Hukum

1. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Peraturan Pemerintah Republik Indonesia Nomor 82 Tahun 2012 Tentang Penyelenggaraan Sistem dan Transaksi Elektronik.
2. Peraturan Menteri Kesehatan Republik Indonesia, Nomor 82 Tahun 2013, Tentang Sistem Informasi Manajemen Rumah Sakit.
3. Standar SNI ISO/IEC 27001:2009 "Teknologi Informasi - Teknik Keamanan - Sistem manajemen keamanan informasi - Persyaratan".
4. Undang- Undang Nomor 44 Tahun 2009 tentang Rumah Sakit, Pasal 52 ayat (1).

BAB II

STANDAR KETENAGAAN

2.1. Kualifikasi Sumber Daya Manusia

2.2.1. Ka. Urusan IT

1. Pendidikan formal minimal : Sarjana (DIV/S1) Teknik Komputer/Teknik Informatika/Sistem Komputer.
2. Menguasai Proses bisnis rumah sakit.
3. Menguasai Proses pembangunan perangkat lunak.
4. Menguasai Proses perencanaan, perancangan dan pengembangan IT *System*.
5. Menguasai Proses *Quality Assurance* (QA) sistem informasi.
6. Pengalaman kerja minimal 1 tahun pada level IT.
7. Dapat bekerja didalam tim.
8. Memiliki kemampuan konseptual, teknis dan hubungan antar manusia yang baik.
9. Memahami bahasa Inggris minimal secara pasif / tulisan.

2.2.2. Wakil Ka. Urusan IT

1. Pendidikan formal minimal : SMK/DIII Teknik Informatika, DIII Teknik Manajemen Informatika, atau DIII Sistem Komputer.
2. Memahami Proses bisnis rumah sakit.
3. Memahami Proses pembangunan perangkat lunak.
4. Memahami Proses perencanaan, perancangan dan pengembangan IT sistem.
5. Memahami dasar operasional komputer (*hardware* dan *software*) dan *troubleshooting*.
6. Memahami dasar sistem operasi, minimal *Windows desktop*.
7. Memahami dasar jaringan komputer.

8. Memahami dasar sistem aplikasi dan *database*.
9. Memahami dasar pengembangan sistem aplikasi.

2.2.3. Staff IT

1. Pendidikan formal minimal : SMK/DIII Teknik Informatika, DIII Teknik Manajemen Informatika, atau DIII Sistem Komputer.
2. Memahami dasar operasional komputer (*hardware* dan *software*) dan *troubleshooting*.
3. Memahami dasar sistem operasi, minimal *Windows desktop*.
4. Memahami dasar jaringan komputer.
5. Memahami dasar sistem aplikasi dan *database*.

2.3. Distribusi Ketenagaan

SDM di Urusan Teknologi Informasi RS. Khusus Ginjal Ny. R.A. Habibie berjumlah 4 orang. Jumlah tersebut sudah termasuk dengan Ka. Urusan IT dan Wakil Ka. Urusan IT.

Adapun distribusi SDM Urusan Teknologi Informasi adalah sebagai berikut :

Nama Jabatan	Kualifikasi Formal dan Informal	Jumlah SDM
Ka. Urusan IT	DIV/S1	1
Wakil Ka. Urusan IT	SMK/DIII	1
Staff IT	SMK/DIII	2
Jumlah		4 Orang

Tabel 2. 1 Distribusi Ketenagaan

2.4. Pengaturan Pelayanan

Pengaturan pelayanan di Urusan IT mempunyai dua pengaturan yaitu :

1. *On Cal*
2. *Email*

Pengaturan ini hanya diperuntukkan bagi Seluruh Tim IT. Adapun pengaturan pelayanan adalah sebagai berikut :

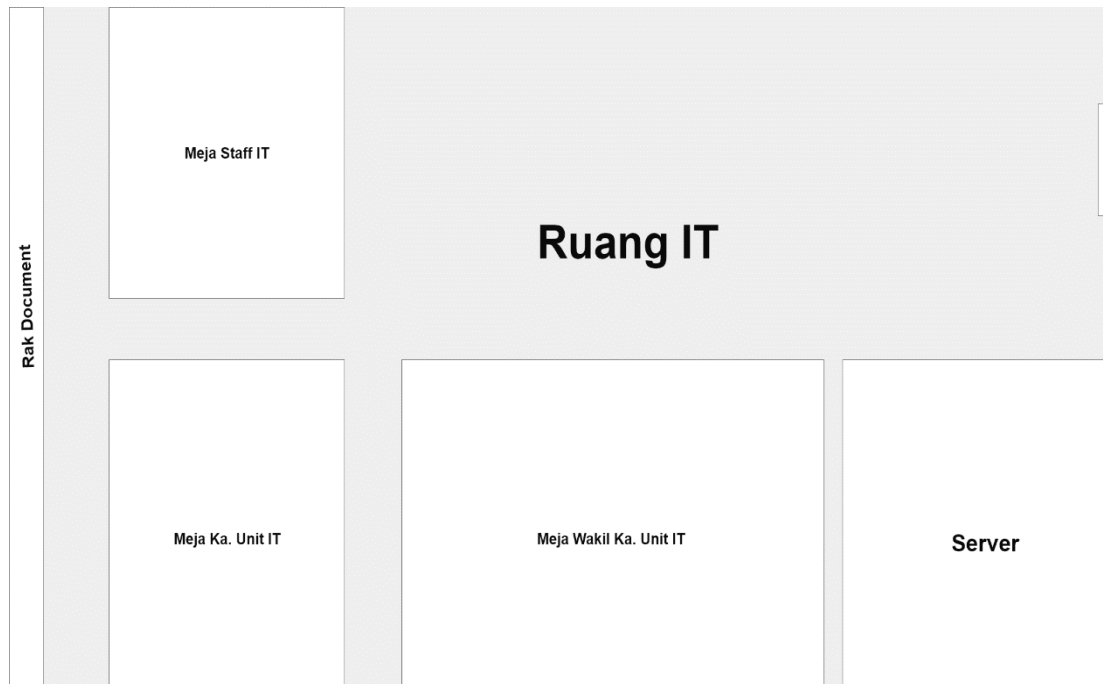
1. Piket diberlakukan dengan ketentuan masuk pukul 08.00 WIB dan pulang 16.30 WIB.
2. Ketentuan on call adalah sebagai berikut:
 - a. *on call* dari jam 08.00 s.d 16.30 WIB
3. Ketentuan email adalah sebagai berikut
 - a. *Email* dari jam 08.00 s.d 16.30 WIB

BAB III

STANDAR FASILITAS

3.1. Denah Ruang

Ruang Urusan Teknologi Informasi terletak di Gedung Baru Lantai 4 dengan denah ruang sebagai berikut:



Gambar 3. 1 Denah Ruang

3.1.1. Server

Ruangan server dilengkapi dengan rak server dimana isi rak server ini berbentuk lemari terbuka.

3.1.2. Meja Ka. Urusan IT

Tempat berkerja Kepala IT dalam melakukan kegiatan sehari-hari dalam mendukung pelayanan rumah sakit.

3.1.3. Meja Wakil Ka. Urusan IT

Tempat berkerja Wakil Ka. Urusan IT dalam melakukan kegiatan sehari-hari dalam mendukung pelayanan rumah sakit.

3.1.4. Meja Staff Urusan IT

Tempat berkerja staff IT dengan pembagian 2 meja, staff IT akan melakukan kegiatan sehari-hari dalam mendukung pelayanan rumah sakit.

3.2. Standar Fasilitas

3.2.1. Fasilitas Ruang IT

No	Nama Jenis Peralatan/Perlengkapan	Jumlah	Keterangan
1	Komputer PC	7 Set	
2	Laptop	2 bh	
3	Meja kerja	4 bh	
4	Kursi	4 bh	
5	<i>White Board</i>	1 bh	
6	Lemari	1 bh	
7	Telepon	1 bh	
8	Rak Dokumen	2 bh	
9	Printer	1 bh	
10	Lampu	4 bh	

Tabel 3. 1 Fasilitas Ruang IT

3.2.2. Fasilitas Server

No	Nama Jenis Peralatan/Perlengkapan	Jumlah	Keterangan
1	Server	1 Set	
2	AC Gedung	2 Pentilasi	
3	UPS	1 Set	
4	PC	2 set	
5	<i>Switch</i>	2 set	
6	<i>RouterBOARD</i>	1 set	

Tabel 3. 2 Fasilitas Server

BAB IV

TATA LAKSANA PELAYANAN

4.1. Jenis Pelayanan

Urusan IT diperlukan perusahaan untuk memberikan *service* kepada Urusan/Instalasi rumah sakit. Adapun Urusan/Instalasi IT mencakup semua karyawan rumah sakit yang menggunakan fasilitas IT dalam pekerjaannya. Adalah *service-service* ini bervariasi dalam bentuk dan tingkat kepentingannya dan mereka membutuhkan *skill set* yang berbeda-beda. Secara umum berikut adalah *service-service* yang diberikan oleh Urusan IT.

Connectivity	<ol style="list-style-type: none"> 1. Internet / Intranet 2. <i>Printing</i> 3. <i>Storage</i>
Business Application	<ol style="list-style-type: none"> 1. <i>Core/Fore end Application</i> 2. <i>Back end application</i> 3. <i>Management Reporting</i> 4. <i>Integration</i>
Indirect Services	<ol style="list-style-type: none"> 1. <i>IT Security</i> 2. <i>Performance Enhancement</i> 3. <i>Reliability</i> 4. <i>Availability</i> 5. <i>Disaster Recovery</i>
Helpdesk/Support	<ol style="list-style-type: none"> 1. <i>Desktop support</i> 2. <i>Application support</i> 3. <i>Infrastructure system support</i> (email, internet/intranet, printing, storage, network) 4. <i>Data back up</i>
System Implementation	<ol style="list-style-type: none"> 1. <i>System Configuration</i> 2. <i>System Customization</i> 3. <i>System Deployment</i>

Tabel 4. 1 Service yang Diberikan oleh Urusan IT

Nama Layanan	Deskripsi	Scope layanan
<i>LAN connection</i>	Penyediaan akses ke jaringan lokal untuk koneksi ke sistem server, sistem printer atau <i>resource</i> lokal lainnya.	1. Pemasangan port ethernet 2. Akses LAN via <i>wireless</i>
<i>Internet connection</i>	Penyediaan koneksi ke internet untuk mendukung tugas/ pekerjaan.	
<i>Intranet connection</i>	Peyediaan akses ke portal http://rskghabibie.com/	Pembuatan <i>account user</i> untuk akses ke fasilitas intranet
<i>Technical Support</i>	Penyediaan bantuan kepada user dalam hal perbaikan perangkat IT yang bermasalah atau memberikan bantuan dalam hal penggunaannya.	1. Fasilitas <i>hardware client</i> 2. Sistem operasi komputer client 3. Aplikasi <i>office client</i>

Tabel 4. 2 Layanan Urusan IT kepada Urusan/Instalasi Rumah Sakit

4.1.1. Waktu Pelayanan Urusan IT

Untuk men-*support* operasional rumah sakit yang berjalan secara kontinyu Urusan IT memberikan layanan baik dalam jam kerja maupun di luar jam kerja normal. Untuk *support* di luar jam kerja normal, layanan diberikan dalam satu jadwal yaitu email.

1. Email

Email adalah layanan *support* IT yang diberikan di luar jam kantor secara *off site* (dari luar kantor) dengan menugaskan satu orang staf untuk *standby* di rumah masing-masing dan siap menerima permintaan *support* melalui email dan akan merespon melalui *replay* email. Jika *problem solving* bisa dilakukan melalui proses *remote desktop* staff IT akan merespon email tersebut dihari dan jam yang

sama, jika tidak bisa dilakukan *problem solving* dihari yang sama, maka petugas IT akan melakukan pengecekan pada jam kerja sesuai dengan hari dan jam kerja yang berlaku.

Nama Layanan	Deskripsi	Scope layanan
<i>Application Development</i>	Pembuatan/pengembangan sistem aplikasi	Mencakup satu siklus lengkap pengembangan sistem.
<i>System Implementation</i>	Menerapkan sistem aplikasi yang telah dibangun untuk digunakan secara operasional.	Mencakup satu siklus lengkap implementasi sistem.
<i>Application Enhancement / Revision</i>	Menambahkan fitur baru atau merevisi fungsi aplikasi sesuai tuntutan bisnis.	

Tabel 4. 3 Tugas dan Layanan IT

4.2. Tata Kerja Urusan IT

Peranan Urusan IT dalam bagian dari pelayanan rumah sakit terhadap setiap Urusan/Instalasi rumah sakit, untuk menunjang kelancaran pelayanan terkait penggunaan IT, perlu adanya pengaturan tata kerja.

Urusan IT merupakan proses yang kritis dalam penyelenggaraan layanan IT Urusan pelayanan, oleh karena itu Urusan IT harus memiliki suatu panduan berupa kebijakan dan prosedur untuk menjalankan operasional IT. Kebijakan dan prosedur operasional IT yang harus dimiliki Urusan IT sekurang-kurangnya mencakup :

4.2.1. Sistem Jaringan Data

Sistem jaringan data mencakup *hardware*, *software*, dan media yang digunakan untuk mentransmisikan informasi berupa data, suara (*voice*), gambar (*image*) dan video.

Penyelenggaraan jaringan data memiliki risiko :

1. Diakses oleh pihak yang tidak berwenang (*unauthorized access*)
2. Terbukanya suatu informasi elektronik dan/atau dokumen elektronik yang bersifat rahasia kepada publik (*exposures*)
3. Keberlangsungan layanan IT (*continuity*) dan,
4. Kinerja (*performance*)

Oleh karena itu IT RSKG harus memiliki kebijakan dan prosedur sebagai pedoman dalam menerapkan teknologi jaringan data untuk meyakinkan bahwa keberlangsungan operasional dan keamanan jaringan data tetap terjaga. Dalam menerapkan pengendalian pada jaringan data untuk melindungi integritas data dan informasi di RSKG, IT RSKG harus memiliki pengelolaan pada jaringan data meliputi :

1. Pengukuran kinerja dan kapasitas jaringan data.
2. *Back up* jaringan data.
3. Pengendalian akses terhadap jaringan data.
4. Penggunaan jaringan internet
5. Penggunaan jaringan nirkabel.

4.2.2. Pengukuran Kinerja dan Kapasitas Jaringan Data

Dalam pengelolaan jaringan komunikasi dibutuhkan pengukuran kinerja dan kapasitas. IT RSKG harus mendesain jaringan yang efisien serta dinamis untuk mengantisipasi perkembangan dimasa yang akan datang. Selain itu IT RSKG juga harus memastikan ketersediaan dan kecukupan kapasitas layanan jaringan komunikasi yang dikelola oleh penyedia layanan.

Untuk memastikan jaringan komunikasi berfungsi sesuai dengan kebutuhan strategis, maka IT RSKG harus menetapkan kebijakan dan prosedur terkait dengan pengukuran kinerja kapasitas jaringan, serta menunjuk personel yang bertanggungjawab. Hal-hal umum yang harus diperhatikan dalam pengukuran kinerja dan kapasitas jaringan komunikasi adalah :

1. Menentukan topologi dan protokol jaringan komunikasi
2. Memilih media jaringan komunikasi sesuai dengan kebutuhan.
3. Adanya kontrak dengan penyedia jasa layanan, serta tersedianya SLA yang sesuai dengan kebutuhan bisnis.

4. Melakukan kajian ulang atas penggunaan jaringan komunikasi minimal setahun sekali.
5. Melakukan pengukuran terhadap kapasitas jaringan komunikasi berdasarkan ketersediaan dan kecukupan kapasitas minimal 1 (satu) tahun sekali.
6. Pengelolaan bandwidth diterapkan untuk membatasi maksimum penggunaan-nya pada masing-masing *workstation*.
7. Melakukan perencanaan kapasitas (*capacity planning*) terhadap jaringan komunikasi.
8. Pemantauan kebutuhan kapasitas, yaitu membandingkan kapasitas yang direncanakan dengan yang digunakan. Pemantauan kapasitas harus dilakukan secara periodik oleh IT RSKG untuk menjaga ketersediaan layanan IT.

4.2.3. Back up Jaringan Data

Jaringan data sangat rentan terhadap gangguan baik dari eksternal maupun internal RSKG. Oleh karena itu IT RSKG menerapkan *back up* jaringan data untuk menjaga ketersediaan layanan data. Dalam menerapkan *back up* jaringan data, RSKG harus memperhatikan hal-hal berikut :

1. Tersedianya *alternative routing* (jalur alternatif)
2. Tersedianya *back up* perangkat jaringan data.
3. Memiliki *incident response plan* terhadap gangguan akses yang tidak berwenang pada komunikasi data.
4. Tersedianya prosedur penanganan masalah (*problem handing*).

4.2.4. Pengendalian Akses terhadap Jaringan Data

Pengendalian akses terhadap jaringan data adalah upaya untuk mengendalikan akses yang masuk serta aktivitas yang dilakukan untuk memperoleh data atau informasi. Pengendalian akses jaringan data sangat penting dan harus diperhatikan karena memiliki resiko perubahan data dari pihak yang tidak berwenang dan terbukanya suatu informasi elektronik dan atau dokumen elektronik yang bersifat rahasia kepada publik.

Dalam menerapkan pengendalian akses, terdapat beberapa hal yang harus diperhatikan oleh IT RSKG, yaitu :

1. Akses ke jaringan data didasarkan kebutuhan dengan memperhatikan aspek keamanan informasi.
2. Akses jaringan data dari lingkungan rumah sakit dari dan ke luar rumah sakit harus melalui izin IT RSKG.
3. Melakukan pemisahan jaringan data berdasarkan segmen, baik secara logis maupun fisik sesuai dengan kebutuhan.
4. Akses ke jaringan data harus dapat dipantau.
5. Konfigurasi perangkat jaringan data harus diatur dengan baik. *Port* dan *services* yang tidak dibutuhkan harus dinonaktifkan.
6. Melakukan kaji ulang pemberian akses ke pengguna secara berkala dan sesuai dengan kebutuhan untuk meyakinkan bahwa akses yang diberikan masih sesuai dengan tugas dan wewenangnya.
7. Penggunaan perangkat pengamanan jaringan data, seperti *firewall*, *Intrusion detection System* dan *Intrusion Prevention System*.

4.2.5. Penggunaan Jaringan Internet

Penggunaan jaringan internet untuk mengakses data atau informasi, memiliki resiko tinggi yang harus diantisipasi oleh IT RSKG. Pengendalian yang memadai terhadap penggunaan internet harus dikelola agar dampak kehilangan data dapat diminimalkan. Oleh karena itu terdapat beberapa hal minimum yang harus diperhatikan oleh IT RSKG, yaitu :

1. Jaringan internet yang digunakan harus menggunakan mekanisme VPN (*Virtual private network*).
2. Lalu lintas data melalui jaringan internet harus dienkripsi.
3. Adanya mekanisme otentifikasi keamanan seperti *username* dan *password*.

Akses internet memiliki keterbatasan baik jumlah *bandwith* yang tersedia dan konten-konten yang diperbolehkan untuk diakses, untuk itu perlu adanya pengaturan terhadap penggunaan internet.

Akses internet digunakan selain untuk mengakses layanan yang disediakan pihak ketiga untuk keperluan bisnis dan transaksi misalnya mesin EDC baik bank maupun asuransi, *webservices* dan informasi lain yang terkait dengan transaksi keuangan.

4.2.6. Penggunaan Jaringan Nirkabel

Penggunaan jaringan nirkabel untuk mengakses data dan informasi memiliki risiko tinggi. Oleh karena itu, penggunaan jaringan nirkabel di lingkungan rumah sakit diperbolehkan selama pengendaliannya memadai. Berikut hal-hal minimum yang harus diperhatikan oleh IT RSKG dalam penggunaan jaringan nirkabel :

1. Adanya metode enkripsi data, otentikasi dan otorisasi terhadap penggunaan jaringan nirkabel dalam mengakses sistem informasi.
2. Melakukan monitoring atas penggunaan koneksi jaringan nirkabel.
3. IT RSKG memiliki mekanisme untuk melakukan konfigurasi perangkat jaringan nirkabel.

4.2.7. Pengelolaan *Database*

Database (basis data) adalah representasi kumpulan fakta yang saling berhubungan disimpan secara bersama sedemikian rupa dan tanpa pengulangan (*redudansi*) yang tidak perlu untuk memenuhi berbagai kebutuhan.

Pengendalian akses dan keamanan database mutlak dilakukan untuk menghindari data-data penting diakses oleh pihak-pihak yang tidak berhak, untuk itu perlu adanya :

1. Kebijakan yang pengaturan akses level dan *security level* terhadap *database*.
2. Personal yang bertanggungjawab terhadap keamanan *database*.
3. Kebijakan perubahan *user* dan *password* secara berkala.

4.2.8. Sistem Back up

RSKG harus memiliki kebijakan dan prosedur terkait dengan proses back up dan restore yang mencakup proses di RSKG. Hal-hal yang harus diatur dalam kebijakan dan prosedur ini, namun tidak terbatas pada :

1. Data harus di *back up* secara periodik sesuai dengan kebutuhan.
2. Data *back up* harus disimpan dilokasi terpisah dari lokasi data center.
3. Media *back up* data harus disimpan dilokasi yang, memiliki sistem pengamanan

4. *Full system back up* harus dilakukan secara berkala sesuai dengan kebutuhan. Apabila terjadi perubahan pada *operating system*, aplikasi dan *database* maka *full system back up* harus segera dilakukan sesegera mungkin.
5. Seluruh media *back up* perlu menggunakan penamaan agar mempermudah proses penggunaan, waktu dan jadwal retensi.
6. Seluruh media *back up* harus dikaji secara berkala untuk memastikan dapat digunakan pada saat yang dibutuhkan.
7. Proses *restore* harus melalui persetujuan dari pemilik data/*database* yang terkait.

4.2.9. Standar Tingkat Layanan (*Service Level*)

IT RSKG sebagai penyedia jasa layanan IT di RSKG memiliki resiko terhadap operasional dan reputasi yang timbul karena kegagalan dalam menyediakan jasa. IT RSKG perlu menetapkan *service level* pelayanan. Tujuan penerapan *service level* untuk meyakinkan bahwa pemantauan layanan, pelaporan permasalahan dan dokumentasi terkait layanan dan jasa IT dapat berjalan dengan baik. Oleh sebab itu IT RSKG harus menunjuk personel yang bertanggung jawab dalam memantau dan mengevaluasi kehandalan pihak penyedia jasa dalam menyediakan layanan secara berkala.

4.2.10. *Technical Support*

IT RSKG wajib memiliki kebijakan dan prosedur terkait dengan penanganan kejadian dan masalah. Kebijakan tersebut harus meliputi penanganan *hardware*, sistem aplikasi, perangkat jaringan dan keamanan informasi. Dalam penanganan insiden dan masalah hendaknya terdapat suatu fungsi atau personel yang bertanggung jawab terhadap proses tersebut. insiden dan permasalahan yang terjadi harus didokumentasikan dan dilaporkan kepada pihak-pihak terkait.

4.2.11. *IT Logistik*

IT RS. Khusus Ginjal Ny. R.A. Habibie perlu memiliki kebijakan dan prosedur terkait dengan pengadaan Perangkat IT (*IT Logistik*). Pengelolaan *IT logistik* bertujuan untuk mengoptimalkan sumber daya dan kemampuan infrastruktur IT dalam memfasilitasi ketersediaan sistem yang lebih besar, terutama untuk menjaga tingkat

interoperabilitas dan keterpadduan, ketahanan dan integritas sistem untuk meminimalkan terjadinya masalah pada pelayanan di RSKG, serta dapat membantu menyelesaikan masalah dengan cepat. Hal-hal yang diatur dalam IT Logistik sebagai berikut, namun tidak terbatas pada :

1. Instalasi *hardware*, *software* dan *network*.
2. Pengaturan parameter (*hardening*) *hardware*, *software* dan *network*.
3. Inventaris dan pemutahiran dokumentasi *hardware*, *software* dan *network*, media penyimpanan dan perangkat pendukung lainnya.

4.2.12. Penilaian Risiko

Untuk ketiga layanan utama IT RSKG diatas, IT RSKG harus memiliki prosedur untuk melakukan penilaian risiko. Penilaian resiko (*risk assesment*) merupakan proses analisa terhadap problem yang terjadi dan dampak nya yang mungkin terjadi pada operasional RSKG jika problem tersebut tidak segera ditangani.

Berikut adalah hal-hal yang harus diperhatikan dalam melakukan penilaian risiko, namun tidak terbatas pada :

1. Tingkat potensi masalah yang timbul berdasarkan tingkat kerusakan (*severity*) dan kemungkinan masalah ini timbul.
2. Analisa dampak masalah terhadap RSKG.
3. Gap Analisis yaitu membandingkan kondisi saat ini dengan langkah *corective action* yang harus dilakukan.

4.2.13. IT Aset Manajemen

Aset IT adalah semua perangkat yang meliputi perangkat keras (*hardware*) dan perangkat lunak (*software*) yang menjadi tanggung jawab departmen IT, *hardware* adalah semua perangkat keras yang menjadi tanggung jawab Urusan IT termasuk perangkat komputer (PC dan laptop), perangkat *networking router*, *switch*, *hub* dan semua piranti (periperal) selain mesin khusus yang terhubung dengan komputer seperti printer, *keyboard* dan monitor

Software adalah semua perangkat lunak yang menjadi tanggungjawab departemen IT termasuk yang digunakan didalam komputer yang meliputi sistem operasi (Operatinf system), anti virus,

Bahasa pemrograman, *Database Management System* (DBMS) dan program-program/aplikasi lainnya yang dibuat digunakan dioperasional rumah sakit.

Hal-hal yang diatur di aset *Management* adalah hal-hal berikut namun tidak terbatas pada:

1. Terdapat kebijakan yang menjelaskan tata kelola aset, dari proses pengadaan, instalasi, pemeliharaan dan penghapusan.
2. Prosedur yang mengatur pengelolaan aset-aset yang berada pada area-area yang membutuhkan koordinasi dengan departemen diluar IT.

4.2.14. Pengelolaan Aset *Hardware*

Pengelolaan aset IT yang digunakan oleh user di RSKG baik berupa *personal computer* (PC), Laptop, Tablet dan lain-lainnya, harus dikelola dengan baik untuk menjamin keamanan dan kontinuitas perangkat tersebut. Dalam pengelolaan perangkat komputerisasi yang digunakan oleh user, IT RSKG harus memiliki kebijakan dan prosedur yang menjamin setiap berlangsungnya operasional penggunaan aset IT. Hal-hal yang harus diperhatikan dalam pengelolaan perangkat komputerisasi adalah sebagai berikut, namun tidak terbatas pada :

1. Terdapat kebijakan yang menjelaskan pembagian dan penggunaan perangkat, serta peran dan tanggung jawab atas keamanan perangkat yang digunakan oleh pengguna.
2. Terdapatnya kebijakan dan prosedur yang mengatur *support* baik dari aspek *software*, *hardware* dan konfigurasi dari perangkat yang digunakan oleh *user*.

4.2.15. Pengelolaan Aset *Software* dan *License*

Pengelolaan aset IT yang digunakan oleh *user* RSKG berupa sistem operasi (*Operating system*), anti virus, Bahasa pemrograman, *Database Management system* (DBMS) dan program-program /aplikasi lainnya yang dibuat digunakan dioperasional rumah sakit, harus memenuhi beberapa aspek :

1. Terdapat kebijakan yang menjelaskan pembagian dan penggunaan aset *software* dan *licensi*.

2. Terdapat kebijakan yang menjelaskan dan mengatur kepatuhan terhadap hukum dan menghindari hal-hal yang bisa melanggar hukum, hak paten dan intelektual.

4.2.16. Penghapusan Aset IT

Aset IT sesuai dengan umur dan intensitasnya perlu adanya penghapusan aset, untuk itu perlu adanya kebijakan yang mengatur prosedur penghapusan aset. Untuk mendapatkan informasi terkait aset yang akurat sebaiknya ditunjang oleh data yang dikeluarkan oleh sistem *recording* yang dapat dipertanggungjawabkan, oleh karena itu perlu adanya pencatatan terkait dengan kondisi IT yang dikemudian hari bisa digunakan untuk pengambilan keputusan untuk melakukan pemilahan aset, misalnya:

1. Aset-aset yang sudah pernah di *service* lebih dari 3x.
2. Barang-barang rusak/konsleting/terbakar (akibat arus listrik) dengan kerusakan sampai dengan 70%.
3. Barang yang diservice vendor tetapi biaya *service* diatas 50% dari harga baru.

Prosedur penghapusan ini harus ada kebijakan yang mengatur dan ada koordinasi dengan Urusan-Urusan terkait.

4.2.17. Manajemen Perubahan Sistem Operasional

Manajemen perubahan atau *change management* adalah prosedur yang mengatur penambahan, penggantian, maupun penghapusan objek di lingkungan pelayanan, Objek yang dimaksud dapat berupa data, program, menu dan aplikasi, perangkat komputer, perangkat jaringan dan proses.

Perubahan diorganisasi yang sedang tumbuh adalah hal yang tidak bisa dihindari, untuk mengantisipasi potensi masalah yang timbul saat dilakukan perubahan maka perlu adanya manajemen perubahan.

Hal-hal yang perlu diperhatikan dalam melakukan manajemen perubahan adalah sebagai berikut, namun tidak terbatas pada :

1. Pengajuan perubahan dilakukan oleh pengguna dan disetujui oleh pihak yang memiliki otorisasi didalam RS. Khusus Ginjal Ny. R.A. Habibie.

2. Staff IT melakukan pengujian untuk memastikan perubahan yang diminta sesuai dan tidak berdampak menimbulkan masalah baru.
3. Pengguna melakukan pengujian hasil perubahan untuk memastikan perubahan dilakukan sesuai dengan permintaan.
4. Pengujian dilakukan berdasarkan skenario yang diminta oleh pengguna.
5. Dokumentasi perubahan harus disimpan dan dikelola dengan baik untuk mempermudah IT RSKG dalam melakukan penelusuran kembali jika terjadi gangguan pada sistem/infrastruktur IT.

4.2.18. Manajemen Perubahan Konfigurasi Sistem Jaringan

Tim IT yang bertanggung jawab terhadap jaringan dalam hal ini network administrator harus membuat dokumentasi terhadap konfigurasi sistem jaringan yang ada, dan mendesain rencana perubahan, sebelum rencana dieksekusi dilingkungan operasional harus melewati prosedur testing. Sistem administrator wajib mendokumentasikan perubahan yang dilakukan. Proses restorasi ke posisi awal wajib disiapkan untuk antisipasi konfigurasi yang baru diterapkan tidak sesuai.

4.2.19. Manajemen Perubahan Konfigurasi Sistem Server Operasional

Setiap server yang digunakan dioperasional harus memiliki dokumentasi konfigurasi, dan disusun rencana untuk menerapkan konfigurasi server yang baru.

4.2.20. Pengendalian Hak Akses

Kewenangan yang diberikan oleh *root/administrator* kepada pihak tertentu, untuk memanfaatkan suatu obyek. Setiap user memiliki akses sendiri – sendiri sesuai dengan wewenang dan Urusan kerjanya. Adapun hak akses *user* terhadap system terbagi dalam dua akses yaitu :

1. Akses terhadap SIMRS
2. Akses terhadap PC (Sistem Jaringan / *Active Directory*)

Sedangkan untuk tingkatan akses terbagi dalam dua tingkatan yaitu :

1. Admin

Hak khusus yang dapat mengakses semua modul SIMRS dan akses semua *feature system* jaringan. Hak ini diberikan kepada administrator/penanggung jawab *software/modul* khususnya TIM IT.

2. User

Hak yang hanya diperuntukkan untuk *user* yang hanya dapat mengakses terhadap modul dan *feature* tertentu.

4.3. Tata Kerja IT *Development*

IT *Development* berperan dalam melakukan pengembangan kebutuhan Sistem Informasi Manajemen Rumah Sakit Khusus Ginjal NY. R.A. Habibie (RSKG). Untuk memenuhi kebutuhannya, IT *Development* melakukan *In House Development* yaitu proses perancangan, pembuatan dan implementasi sistem dilakukan oleh IT *Development*. Hanya beberapa aplikasi yang bersifat khusus dan atas kebijakan yang khusus, pengembangan sistem diserahkan kepada *vendor* dengan syarat tetap terintegrasi dengan sistem yang dibuat oleh Rumah Sakit. Hal ini dapat menghindari ketergantungan Rumah Sakit terhadap *vendor* penyedia program/ aplikasi.

4.3.1. Rencana Kerja Pengembangan Sistem

Dalam melakukan pengembangan sistem informasi manajemen rumah sakit, IT *Development* harus menyiapkan rencana pengembangan berdasarkan plan map yang dibuat Rumah Sakit. Rencana pengembangan sistem harus mendapatkan persetujuan dari Ka. Urusan IT, Kabag. Umum dan Keuangan, Direktur Rumah Sakit dan Yayasan Pembinaan Asushan Bunda.

4.3.2. Manajemen Proyek dan Pengembangan Sistem

Dalam melakukan pengembangan sistem informasi manajemen rumah sakit, IT *Development* harus menerapkan Manajemen Proyek. Penerapan Manajemen Proyek bertujuan untuk memastikan bahwa sistem telah dikembangkan sesuai tujuan pengembangan, waktu yang telah ditentukan, dan biaya yang dianggarkan. Selain itu, penerapan manajemen proyek dapat memastikan bahwa proses pengembangan sistem telah memenuhi kebutuhan pengguna.

Dalam menerapkan Manajemen Proyek pada proses pengembangan sistem, IT *Development* harus menerapkan beberapa hal, yaitu :

4.3.3. Metodologi

Metodologi pengembangan sistem yang digunakan oleh IT *Development* harus sesuai dengan karakteristik dan resiko proyek. Terdapat beberapa metodologi pengembangan yang dapat digunakan, namun tidak terbatas pada :

1. Agile Software Development

Merupakan kerangka pengembangan sistem yang berbasis pada pengembangan secara iterasi/ berulang ulang dalam siklus proyek untuk merespon kebutuhan dan solusi pengembangan yang berubah atau berkembang terus menerus.

2. Rapid Application Development (RAD)

Merupakan metodologi pengembangan dimana *working model system* dikonstruksikan diawal tahap pengembangan dengan tujuan menetapkan kebutuhan pengguna. RAD menekankan pada siklus pembangunan pendek, singkat dan cepat.

3. System Development Life Cycle (SDLC)

Merupakan metodologi pengembangan yang pada umumnya sering digunakan. Adapun tahapan yang diperlukan adalah perencanaan, pengadaan (dilakukan apabila IT menggunakan pihak penyedia barang dan jasa), perancangan sistem, pembuatan aplikasi, pengujian, implementasi, kaji ulang setelah implementasi dan pemeliharaan.

4.3.4. IT Quality Assurance

Dalam pelaksanaan pengembangan sistem informasi manajemen rumah sakit, dibutuhkan aktifitas *Quality Assurance* untuk memastikan bahwa tahapan pengembangan sesuai dengan metodologi yang diterapkan. IT *Quality Assurance* juga membantu tim proyek dalam memastikan *deliverables* setiap tahapan pekerjaan telah sesuai dengan TOR (*Terms of Reference*)

4.3.5. Pengendalian Pengembangan Sistem

Metodologi SDLC merupakan metodologi yang pada umumnya digunakan dalam melakukan pengembangan sistem. Berikut pengendalian yang dapat diterapkan dalam pengembangan sistem dengan menggunakan metodologi SDLC.

4.3.6. Perencanaan / Analisa

IT Development harus melakukan proses identifikasi kebutuhan pengembangan sistem dan melakukan perencanaan untuk melaksanakan proyek. Proses ini didokumentasikan dalam sebuah dokumen proposal dan studi kelayakan yang sekurang-kurangnya mencakup hal-hal berikut:

1. Tujuan pelaksanaan pengembangan system
2. Ruang Lingkup Proyek
3. Manfaat yang diharapkan dari system yang akan dikembangkan, khususnya menjelaskan manfaat bagi efisiensi biaya (*cost efficiency*) dan peningkatan produksi
4. Analisa untuk menentukan pengembangan dilakukan oleh internal IT Development atau menggunakan pihak penyedia barang dan jasa
5. Jadwal proyek
6. Struktur Tim Proyek

Proposal dan hasil dari studi kelayakan harus diajukan Ka. Urusan IT

4.3.7. Pengadaan

Pelaksanaan pengadaan dilakukan apabila IT *Development* menggunakan pihak penyedia barang dan jasa dalam melakukan pengembangan sistem informasi manajemen rumah sakit.

4.3.8. Perancangan

Aktifitas yang dilakukan pada tahap ini yaitu dengan melakukan perancangan sistem berdasarkan identifikasi kebutuhan. Semua kebutuhan pengguna yang telah teridentifikasi dikonversikan menjadi rancangan sistem yang akan menghasilkan suatu dokumen teknis. Dokumen tersebut harus dikaji oleh IT *Quality Assurance* dan IT Operasional sebelum digunakan oleh Programmer.

Hal-hal yang harus diperhatikan dalam proses perancangan sistem adalah sebagai berikut :

1. Deskripsi detkil sistem
2. Diagram alur data dalam sistem yang dikembangkan
3. Rincian Spesifikasi rancangan sistem yang akan dikembangkan harus sesuai dengan kebutuhan
4. Kebutuhan keamanan (*security requirement*) yang mengacu kepada *security* Baseline Divisi IT

Selain itu dalam aktivitas perancangan sistem diperlukan suatu standar pengendalian terkait aktivitas pengguna pada sistem. Standar sistem aplikasi tersebut dapat meningkatkan keamanan, integritas, dan kehandalan sistem dengan memastikan *input*, *process* dan *output* yang akurat, lengkap dan aman. Pengendalian yang harus dilakukan paling kurang meliputi :

1. Pengendalian input

Memastikan pengguna memasukkan informasi secara akurat agar dapat mengurangi kesalahan *input/ human error*. Pengendalian *input* minimal dapat mencakup pengecekan terhadap validitas/kebenaran data, *range* data/ parameter dan duplikasi data yang di-*input*.

2. Pengendalian proses

Memastikan proses bekerja secara akurat dan dapat menyimpan informasi atau menolaknya. Pengendalian proses yang dapat dilakukan secara otomatis oleh sistem mencakup paling kurang *Error Reporting*, *Transaction Log*, pengecekan urutan dan *backup file*.

3. Pengendalian *output*

Memastikan sistem mengelola informasi dengan aman dan mendistribusikan informasi hasil proses dengan tepat serta menghapus informasi yang telah melewati masa retensi

4.3.9. Pemrograman

Pada tahap pemograman, hasil spesifikasi desain dikonversikan menjadi sebuah program yang dapat dijalankan oleh programmer. Pada saat pemograman, koordinator proyek harus memahami secara keseluruhan proses pemograman untuk memastikan tanggung jawab

seorang programmer terhadap data, program dan sistem telah dibatasi untuk menjaga integritas dan keamanan data.

Pada pengembangan sistem diperlukan pengujian internal untuk meminimalkan terjadinya kesalahan pada sistem yang dikembangkan dan memastikan sistem telah berjalan dengan baik. Pengujian internal yang dilakukan adalah dengan melakukan *Urusan Testing*. Pengujian ini dilakukan untuk menilai fungsionalitas dari sebagian kecil modul pada sistem.

Dokumentasi teknis pemograman, data dan program hasil pengembangan harus disimpan dalam media penyimpanan dengan baik oleh *IT Development*.

4.3.10. Pengujian

Pada tahap pengujian, pengguna melakukan beberapa rangkaian uji coba untuk memastikan keakuratan dan berfungsinya sistem sesuai ndengan kebutuhan. Pengujian yang dapat dilakukan antara lain :

1. *System Integration Testing*, dilakukan untuk menilai fungsionalitas seluruh sistem dan integrasi antar modul didalam sistem.
2. *Stress Testing*, dilakukan dalam rangka menilai kinerja sistem pada kondisi penggunaan maksimal untuk mendapatkan batasan kemampuan maksimal dari sistem yang dikembangkan.
3. *User Acceptance Testing (UAT)*, dilakukan untuk menguji fungsionalitas keseluruhan sistem apakah telah sesuai dengan kebutuhan pengguna, baik dariii sisi akurasi, maupun hubungan dengan sistem lain (*interoperability*). Pada saat UAT, terdapat 2 macam pengujian yang dapat dilakukan dengan menggunakan skenario pengujian, yaitu:

a. Positive Test

Merupakan suatu pengujian yang sengaja dirancang untuk menunjukkan bahwa sistem akan menghasilkan *output* yang sesuai jika informasi yang diinput oleh *user* adalah benar. Pengujian ini dilakukan berdasarkan skenario yang telah disusun sebelumnya.

b. Negative Test

Merupakan suatu pengujian yang sengaja dirancang untuk menunjukkan bahwa sistem akan menghasilkan output yang tidak sesuai atau tidak diharapkan jika informasi yang diinput oleh user adalah salah. Pengujian ini dilakukan berdasarkan skenario yang telah disusun sebelumnya.

UAT merupakan ujicoba akhir yang dilakukan oleh pengguna akhir terhadap sistem yang dikembangkan. UAT dilakukan dengan menggunakan skenario pengujian yang sebelumnya disusun dan didokumentasikan oleh pengguna. Hasil dari pelaksanaan UAT harus didokumentasikan dalam Berita Acara dan disetujui oleh pengguna, koordinator proyek dan IT *Quality Assurance*.

4.3.11. System Deployment

Proses *Deployment* adalah tahapan terakhir dari proses *Development*, yaitu fase dimana sistem aplikasi diinstal di server production sehingga bisa digunakan secara operasional. Hal-hal yang harus diperhatikan pada tahap *deployment* adalah :

1. Terdapat rencana *release* sistem untuk menentukan jadwal dan tahapan release sistem ke lingkungan produksi
2. Terdapat rencana rollback untuk mengatasi jika system yang diimplementasikan mengalami kegagalan fungsional atau menyebabkan kinerja aplikasi kritikal lainnya terganggu, sehingga system lama harus digunakan kembali
3. Terdapat rencana migrasi data apabila sistem yang akan diimplementasikan menggantikan sistem lama di lingkungan produksi dan didalamnya terdapat data yang masih digunakan, yang mencakup :
 - a. Pengecekan integritas program, berupa pengendalian yang memadai terhadap konversi *source code* ke *object code* yang akan diimplementasikan.
 - b. Pengecekan akurasi dan keamanan data hasil migrasi perlu dilakukan untuk memastikan integrasi dan validitas data.

- c. Terdapat rencana pelatihan pengguna system untuk pengguna setelah implementasi dilakukan.
- d. Terdapat dokumentasi hasil pelaksanaan implementasi dalam suatu Berita Acara. Berita Acara tersebut harus disetujui personel Operasional, pengguna, koordinator proyek, serta IT *Quality Assurance*.
- e. Dalam proses pengembangan SISTEM IT, spesifikasi sistem penunjang dan spesifikasi SISTEM IT yang akan dikembangkan harus memenuhi prinsip pengamanan informasi dengan menerapkan:
 - 1) Pengendalian akses terhadap layanan SISTEM IT. Memastikan Sistem IT bahwa dapat dilakukan pembatasan terhadap akses logik dan fisik ke dalam SISTEM IT yang akan dikembangkan, sehingga data dan informasi dapat dikelola hanya oleh pihak yang berwenang.
 - 2) Enkripsi untuk penyimpanan data dan informasi yang bersifat rahasia. Memastikan sistem mengelola informasi secara aman dengan menyimpan data dan informasi dalam format yang terenkripsi, sehingga meminimalisir kemungkinan terjadinya kebocoran informasi.

4.3.12. Perlindungan Terhadap Program Asli dan *Source Code* Aplikasi

RSKG harus menerapkan pengendalian keamanan terhadap program asli ataupun *source code*, baik untuk pengembangan aplikasi yang dilakukan secara internal maupun yang dilakukan secara *outsourcing* kepada Vendor dengan metode pembelian aplikasi. *Source code* tersebut harus disimpan pada tempat yang aman dengan menerapkan pembatasan akses logik maupun fisik untuk melindungi dari pihak yang tidak berwenang.

BAB V

LOGISTIK

Data logistik IT tersimpan dalam suatu aplikasi. Sehingga dapat memudahkan TIM IT untuk menginventarisir data apa saja yang terdapat di rumah sakit yang menjadi tanggung jawab Urusan IT.

Selain dari itu memudahkan TIM dalam hal maintenance baik *maintenance* perangkat lunak maupun perangkat keras. Adapun data logistik tersebut adalah sebagai berikut :

No	Nama Barang	Jumlah	Keterangan
1	PC		
2	<i>Printer</i>		
3	Monitor		
4	<i>Devices</i>		DVD, Modem, <i>Scanner Print</i> Server, UPS dll
5	Telepon		

Tabel 5. 1 Perangkat Keras

No	Nama Barang	Jumlah	Keterangan
1	Windows		Server, Professional OLP
2	Linux		Server, Professional OLP
3	SQL		Server

Tabel 5. 2 Perangkat Lunak

BAB VI

KESELAMATAN PASIEN

6.1. Manajemen Risiko Keselamatan Pasien

Manajemen risiko adalah pendekatan proaktif untuk mengidentifikasi, mengevaluasi dan memprioritaskan risiko untuk mengurangi risiko cedera dan kerugian pada pasien.

Manajemen risiko dibuat berdasarkan Alur Pelayanan Teknologi Informasi. Kerugian pada pasien disebut Insiden keselamatan pasien yang terdiri dari :

1. Kejadian Tidak Diharapkan (KTD) : insiden yang mengakibatkan cedera pada pasien.
2. Kejadian Nyaris Cedera (KNC): terjadinya insiden yang belum sampai terpapar ke pasien.
3. Kejadian Tidak Cedera (KTC) : insiden yang sudah terpapar ke pasien, tetapi tidak timbul cedera.
4. Kejadian Potensial Cedera (KPC) : kondisi yang sangat berpotensi untuk menimbulkan cedera, tetapi belum terjadi insiden.
5. Kejadian Sentinel : insiden yang mengakibatkan kematian atau cedera yang serius.

Langkah langkah untuk melakukan manajemen risiko adalah sebagai berikut :

1. Identifikasi Risiko

Identifikasi risiko dilakukan dengan melihat pada alur pelayanan Urusan setiap Urusan, yang dapat menyebabkan kerugian kepada pasien.

2. Analisa Risiko

Analisis risiko menggunakan metode *Failure Mode and Effect Analysis* (FMEA), yaitu identifikasi sumber kesalahan potensial dan menentukan bagaimana kegagalan tersebut memengaruhi sistem. Beberapa hal yang termasuk dalam FMEA adalah :

- a. Menemukan sumber masalah
- b. Menentukan probabilitas dan konsekuensi setiap kegagalan

- c. Menguraikan/membuat pengukuran untuk mendeteksi dan mencegah kegagalan
- 3. Pengelolaan Risiko
- 4. Menentukan Prioritas Risiko
- 5. Monitoring Pengelolaan Risiko yang sudah dibuat
- 6. Evaluasi Pengelolaan Risiko yang sudah dibuat

Bila masih terjadi insiden tersebut diatas, Urusan Teknologi Informasi melaporkan kepada Komite Keselamatan Pasien Rumah Sakit untuk ditindak lanjuti.

6.2. Pencegahan dan Pengendalian Infeksi

Pencegahan dan pengendalian infeksi rumah sakit Urusan merupakan bagian dari pencegahan dan pengendalian infeksi rumah sakit secara umum. Hal utama yang dilakukan oleh Urusan Teknologi Informasi adalah penerapan kewaspadaan isolasi yang terdiri dari kewaspadaan standar dan kewaspadaan transmisi.

Hal-hal terkait Pencegahan dan Pengendalian Infeksi (PPI) yang dilakukan oleh Urusan Teknologi Informasi adalah sebagai berikut :

1. Kebersihan Tangan
2. Penggunaan APD
3. Etika batuk
4. Pemrosesan peralatan pasien
5. Pembuangan/pengelolaan limbah
6. Pengendalian lingkungan
7. Praktek menyuntik/tindakan invasif yang aman
8. Penempatan pasien infeksius dan *immunocompromised*
9. Perawatan pasien berdasarkan transmisi infeksi
10. Transpor pasien infeksius *immunocompromised*

BAB VII

KESELAMATAN KERJA

Keselamatan yang berkaitan dengan tenaga kerja, pekerjaan dan lingkungan kerja yang meliputi segala upaya untuk mencegah dan menanggulangi segala sakit dan kecelakaan akibat kerja.

7.1. Penggunaan APD sesuai standar

Menggunakan sepatu jika melakukan pemasangan alat atau kabel, dapat terhindar korsleting listrik (kesetrum).

7.2. Pembuangan limbah sesuai dengan jenisnya

Pembuangan limbah padat dengan limbah cair harus dibuang sesuai dengan jenisnya. Contohnya seperti: sisa pembuangan tinta di printer sebagai limbah cair, pembuangan alat suntikan tinta sebagai limbah padat.

7.3. Pemasangan kabel sesuai dengan prosedur

Apabila pemasangan kabel harus sesuai dengan prosedur yaitu :

1. Pemasangan kabel harus tersembunyi dan jauh dari akses jalan
2. Penyambungan kabel harus di tutup rapat dengan isolasi
3. Setiap pemasangan kabel harus rapi dan tertutup oleh *Cable Deck*

BAB VIII

PENGENDALIAN MUTU

8.1. Indikator Mutu

Indikator mutu di Urusan Teknologi Informasi dipergunakan untuk menilai mutu Urusan Teknologi Informasi. Komite / Tim PMKP melakukan koordinasi dan mengorganisasi pemilihan indikator mutu di Urusan Teknologi Informasi sehingga indikator yang dipilih tersebut valid, *reliable*, *sensitive*, dan spesifik. Pengukuran mutu perlu juga memperhatikan dimensi mutu dari WHO, yaitu *effective*, *efficient*, *accessible*, *accepted (patient - centered)*, *equity and safe*.

Dicantumkan indikator - indikator yang menunjukkan keberhasilan Urusan tersebut.

8.2. Monitoring

Monitoring adalah proses yang dilakukan oleh Urusan Teknologi Informasi dalam memantau pelaksanaan pengukuran indikator dan proses peningkatan mutu di Urusan Teknologi Informasi. Contoh Urusan Teknologi Informasi memastikan bahwa seluruh sumber daya yang dibutuhkan dalam proses pengukuran indikator tersedia, Urusan memastikan proses pengukuran indikator sudah sesuai dengan prosedur yang ditetapkan, Urusan memastikan / memonitor proses rekapitulasi, analisa, validasi dan evaluasi dilakukan dan sesuai dengan ketentuan yang berlaku, Urusan Teknologi Informasi memonitoring pelaksanaan perbaikan dan pelaporan.

8.3. Evaluasi

Evaluasi adalah proses dan langkah - langkah yang dilakukan oleh Urusan Teknologi Informasi dalam melakukan analisa mendalam terhadap proses dan hasil pengukuran indikator serta proses perbaikan dan peningkatan mutu. Mencakup standar acuan dan pengolahan data.

8.4. Pelaporan

Tatacara dan alur pelaporan hasil pengukuran indikator mutu dan hasil peningkatan mutu di Urusan Teknologi Informasi mencakup media, periode, PIC dan bentuk pelaporannya.

8.5. *Continous Improvement*

Countinuous improvement adalah proses perbaikan dan peningkatan mutu yang dilakukan oleh Urusan Teknologi Informasi yang merupakan upaya untuk memastikan bahwa setiap proses perbaikan dan peningkatan mutu dapat dilakukan secara berkesinambungan dan berkelanjutan.

BAB IX

PENUTUP

Sistem Informasi Rumah Sakit merupakan aplikasi yang di develop untuk kebutuhan management Rumah Sakit, dimana sistem ini sudah di dukung dengan fitur dan modul yang lengkap untuk operasional Rumah Sakit dengan adanya aplikasi ini di harapkan dapat membantu operasional rumah sakit dan dapat meningkatkan pelayanan rumah sakit. *Hardware* dan *software* adalah aplikasi pendukung kinerja sehingga dapat meningkatkan mutu pelayanan Rumah Sakit Khusus Ginjal NY. R.A Habibie.

Pedoman Pelayanan Urusan Teknologi Informasi ini diharapkan dapat meningkatkan kinerja sesuai dengan standar operasional yang sudah disesuaikan dan ditetapkan. Sehingga dapat tercipta keseragaman dalam melakukan tindakan.

Kami menyadari bahwa Buku Pedoman ini masih jauh dari kesempurnaan, sehingga kritik dan saran sangat kami harapkan untuk penyempurnaan dari waktu ke waktu.

Code-IT002#