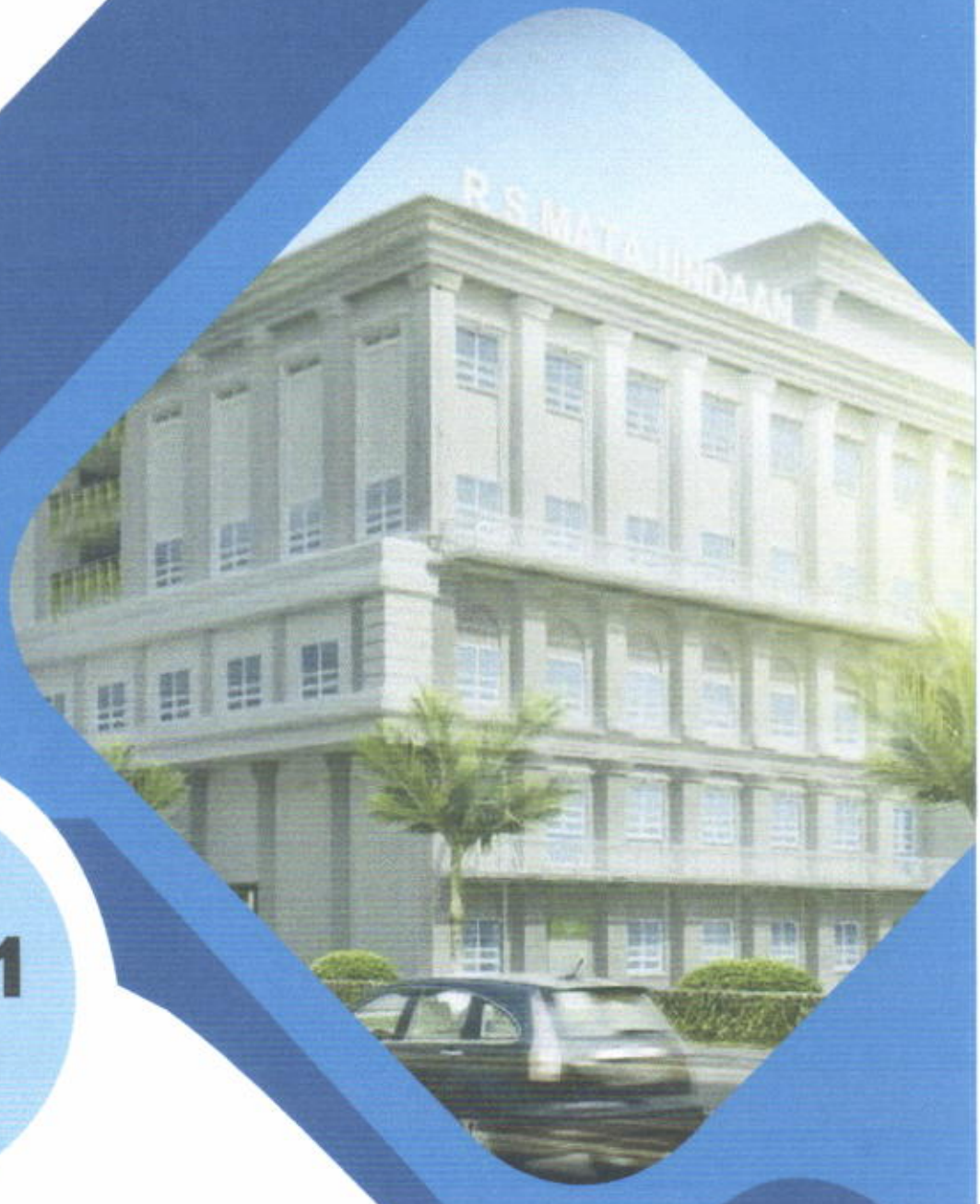
RS Mata Undaan
Care and Smile



Edisi 1
Tahun 2019

PANDUAN KEAMANAN DATA DAN INFORMASI

RS. Mata Undaan Surabaya

Jl. Undaan Kulon No. 17 - 19 Surabaya
Telp. 031 5343 806, 5319 619
Fax. 031 - 5317 503

DAFTAR ISI

RS Mata Undaan
Care and Smile

PERATURAN DIREKTUR RUMAH SAKIT MATA UNDAAN
NOMOR : 547/PER/DIR/RSMU/IV/2019
TANGGAL : 04 APRIL 2019
TENTANG
PANDUAN KEAMANAN DATA DAN INFORMASI
RUMAH SAKIT MATA UNDAAN SURABAYA

DIREKTUR RUMAH SAKIT MATA UNDAAN

Menimbang :
a. Bahwa dalam rangka menyelenggarakan sistem informasi rumah sakit di RS. Mata Undaan Surabaya perlu dibuat Panduan Keamanan Data dan Informasi;
b. Bahwa berdasarkan pertimbangan sebagaimana dimaksud huruf a diatas, maka perlu ditetapkan dengan Peraturan Direktur.

Mengingat :
1. Undang-Undang Nomor 36 Tahun 2009 tentang Kesehatan;
2. Undang-Undang Nomor 44 Tahun 2009 tentang Rumah Sakit;
3. Keputusan Perhimpunan Perawatan Penderita Penyakit Mata Undaan Nomor: 035/P4M/SK/VII/2017 tentang Pengangkatan Direktur Rumah Sakit Mata Undaan Surabaya;
4. Keputusan Perhimpunan Perawatan Penderita Penyakit Mata Undaan Nomor : 014/P4M/SK/II/2019 Tentang Berlakunya Struktur Organisasi, *Job Description* dan *Job Spesification* Rumah Sakit Mata Undaan.
5. Peraturan Direktur Rumah Sakit Mata Undaan Nomor: 432/PER/DIR/RSMU/III/2019 Tanggal 18 Maret 2019 tentang Pedoman Pelayanan Unit SIRS Rumah Sakit Mata Undaan Surabaya.

MEMUTUSKAN

Menetapkan :

Kesatu : Menetapkan dan memberlakukan Panduan Kemanan Data & Informasi di Rumah Sakit Mata Undaan Surabaya.

Kedua : Panduan Keamanan Data & Informasi ini digunakan sebagai acuan dalam penyelenggaraan pelayanan di Rumah Sakit Mata Undaan Surabaya.

Ketiga : Panduan Keamanan Data & Informasi di Rumah Sakit Mata Undaan sesuai pada Lampiran Peraturan Direktur ini.

Keempat : Peraturan Direktur ini berlaku sejak tanggal ditetapkannya dan akan dievaluasi secara berkala bila diperlukan.

Kelima : Apabila di kemudian hari terdapat kekeliruan dalam peraturan ini akan diadakan perbaikan sebagaimana mestinya.

Ditetapkan di Surabaya
Pada tanggal 04 April 2019
Direktur,

dr. Sudjarno, Sp.M (K)

LAMPIRAN
KEPUTUSAN DIREKTUR RUMAH SAKIT MATA UNDAAN
NOMOR : 547/PER/DIR/RSMU/IV/2019
TANGGAL : 04 APRIL 2019
TENTANG
PANDUAN KEAMANAN DATA DAN INFORMASI
RUMAH SAKIT MATA UNDAAN SURABAYA

BAB I
PENDAHULUAN

1.1 Latar Belakang

Masalah keamanan merupakan salah satu aspek penting dari sebuah sistem informasi, sayang sekali masalah keamanan ini sering kali kurang mendapat perhatian dari para pemilik dan pengelola sistem informasi, seringkali masalah keamanan berada di urutan kedua, atau bahkan di urutan terakhir dalam daftar hal-hal yang dianggap penting, apabila menggangu performansi dari sistem, seringkali keamanan dikurangi atau ditiadakan.

Informasi saat ini sudah menjadi sebuah komoditi yang sangat penting, bahkan ada yang mengatakan bahwa kita sudah berada di sebuah "*information-based society*". Kemampuan untuk mengakses dan menyediakan informasi secara cepat dan akurat menjadi sangat esensial bagi sebuah organisasi, baik yang berupa organisasi komersial (perusahaan), perguruan tinggi, lembaga pemerintahan, maupun individual (pribadi), hal ini dimungkinkan dengan perkembangan pesat di bidang teknologi komputer dan telekomunikasi

Keamanan Informasi adalah perlindungan informasi terhadap pengungkapan yang tidak disengaja atau berbahaya, modifikasi atau kehancuran. Informasi merupakan aset penting dan berharga bagi RSMU yang harus dikelola dengan hati-hati. Semua informasi memiliki nilai bagi RSMU. Namun, tidak semua informasi ini memiliki nilai yang sama atau membutuhkan tingkat proteksi yang sama . Kontrol akses diletakkan untuk melindungi informasi dengan mengontrol siapa saja yang memiliki hak untuk menggunakan sumber-sumber informasi yang berbeda dan menghindari terjadinya penyalahgunaan. Prosedur harus mengontrol bagaimana hak akses atas informasi diberikan dan bagaimana hak akses tersebut berubah. Kebijakan ini juga mengatur standar untuk membuat sandi yang kuat, perlindungan dan frekuensi perubahan. Kebijakan ini berlaku untuk Departemen TI, pengguna peralatan dan pengguna informasi bertanggung jawab untuk memastikan keamanan dan keselamatan dari peralatan TI.

1.2 Tujuan

Sebagai panduan atau standar dalam rangka melindungi aset informasi Rumah Sakit Mata Undaan (RSMU) dari berbagai bentuk ancaman baik dari dalam maupun luar lingkungan RSMU, dengan tujuan untuk menjamin kerahasiaan, keutuhan, dan ketersediaan aset informasi.

1.3 Definisi Operasional

1. *Physical security* adalah keamanan informasi yang menfokuskan pada strategi untuk mengamankan individu / anggota organisasi dan tempat kerja dari bencana alam, kebakaran, dll. Physical security memfokuskan pada aset fisik dari suatu informasi.
2. *Personal security* adalah keamanan informasi yang memfokuskan pada keamanan personal, berhubungan dengan keamanan physical security

3. *Operation security* adalah keamanan informasi yang membahas mengenai strategi suatu organisasi, agar organisasi tersebut dapat mengamankan kemampuan organisasi untuk berjalan tanpa ada gangguan.
4. *Communication Security* adalah keamanan informasi bertujuan mengamankan media komunikasi dan memanfaatkan media tersebut untuk mencapai tujuan organisasi
5. *Network Security* adalah keamanan informasi yang memfokuskan pada pengamanan peralatan jaringan ataupun data organisasi.

BAB II
RUANG LINGKUP

Ruang lingkup dalam panduan ini meliputi:

2.1 Pengamanan Sistem Informasi Rumah Sakit

Pengamanan sistem informasi rumah sakit terdiri dari:

1. Data/Dokumen

   Pada dasarnya data adalah kumpulan informasi atau keterangan – keterangan dari suatu hal yang diperoleh melalui pengamatan atau pencarian ke sumber – sumber tertentu. Data yang diperoleh dapat menjadi suatu anggapan atau fakta karena memang belum diolah lebih lanjut. Setelah diolah melalui penelitian atau percobaan maka suatu data dapat menjadi bentuk yang lebih kompleks seperti suatu database, informasi atau bahkan solusi untuk masalah tertentu.

   Data/dokumen yang dimaksud meliputi: data medical record pasien, data kunjungan pasien, data kefarmasian, data administrasi, data tata usaha, data kepegawaian, data rumah tangga, data kamar operasi, data keuangan dan data executive summry. Kerusakan data dapat disebabkan oleh beberapa faktor :

   a. Terhapus permanen tanpa disengaja atau dengan disengaja.
      Terkadang, kita ingin menghapus data, namun setelah file dihapus bukan data yang dimaksud yang akan dihapus. Sebagai contoh, ketika Anda melakukan pembersihan data secara rutin tiap minggu/bulan, terkadang ada satu kesalahan data penting ikut terhapus.
   b. Virus dan Malware
      Ketika menggunakan perangkat digital, bukan berarti komputer sudah aman dari pencurian data. Program jahat yang dikirimkan ke komputer juga bisa menjadi salah satu hilang/rusaknya data Anda.
   c. Kerusakan Hard Drive
      Hard Drive adalah salah satu komponen komputer yang sangat sensitive dan juga sangat rentan. Alasannya adalah Hard Drive terdiri dari banyak bagian yang berjalan. Meskipun ada cara memulihkan Hard Drive, tetapi data tidak dapat kembali secara utuh.
   d. Pemadaman Listrik Secara tiba-tiba
      Listrik padam secara tiba-tiba sudah sangat sering terjadi. Padamnya listrik ketika PC/Laptop/Server ini dalam posisi hidup, akan membuat data Corrupt atau Error.
   e. Hilangnya Device
      Inilah yang terjadi jika tidak memiliki backup data di Cloud Storage. Ketika kehilangan device seperti Laptop dan Flashdisk, maka data sudah pasti tidak akan bisa dikembalikan.
   f. Device terkena cairan
      Ambil contoh laptop yang kesiram air. Kerusakan pada device juga bisa terjadi akibat hal yang satu ini.
   g. Masalah Firmware
      Firmware pada dasarnya adalah kode yang mengontrol Hard Drive. Hal ini bertanggung jawab untuk mengelola konfigurasi drive dengan komponen system lainnya. Kerusakan pada Firmware juga bisa menghilangkan data

2. Perangkat Lunak

   Pengertian perangkat lunak komputer paling umum adalah piranti atau komponen dari sebuah komputer yang berbentuk data, program dan file digital yang dipasang dan dibaca sertadigunakan di dalam komputer, meliputi: perangkat lunak aplikasi, perangkat lunak sistem, dan perangkat bantu pengembangan system. Kerusakan software dapat disebabkan oleh beberapa hal, antara lain :

   a. Penggunaan software bajakan

      Software yang bajakan karena tidak berasal dari pembuatnya langsung maka kualitas software tersebut tidak dapat dijamin sehingga resiko kerusakan akan besar dan kita tidak dapat melakukan komplain.

   b. Kesalahan prosedur

      Pemasangan/*install* software yang tidak benar dapat menyebakan crash/bertabrakan dengan software lain atau tidak lengkap sehingga menyebabkan software rusak.

   c. Virus

      Virus selain dapat merusak data, dapat juga merusak software dan biasanya menyerang sistem operasi dan aplikasi yang berjalan di system operasi Windows

3. Aset Fisik

   Komponen yang nyata dan dapat dilihat dan disentuh secara langsung, meliputi: perangkat komputer, perangkat jaringan dan komunikasi, removable media, dan perangkat pendukung. Keamanan aset fisik meliputi :

   a. Kelistrikan

      Hardware komputer sangat tergantung pada listrik. Oleh karena itu ketidakstabilan listrik akan mempengaruhi kinerja dan ketahanan hardware. Komputer yang sering mati dengan tiba-tiba akibat kehilangan pasokan listrik dapat memicu kerusakan baik pada hard disk, motherboard bahkan power supply dan perangkat lainnya.

   b. Kesalahan prosedur

      Penggunaan atau penempatan yang tidak sesuai aturan akan menyebabkan memperpendek masa pakai hardware. Menyalakan komputer diruang yang panas atau memaksakan komputer menyala terus menerus dapat menimbulkan kerusakan.

   c. Bencana alam/kerusuhan.

      Faktor ini adalah yang paling sulit dihindarkan karena diluar kemampuan kita. Banjir, gempa atau kerusuhan bila mencapai komputer maka kerusakan parah sangat mungkin terjadi

4. Hak Akses

   Hak akses adalah akses terhadap sistem informasi sensitif, termasuk di dalamnya dan tidak terbatas pada sistem operasi, perangkat penyimpanan, file server, dan aplikasi-aplikasi sensitif. Hanya diberikan kepada pengguna yang membutuhkan, pemakainnya terbatas dan dikontrol

5. Perangkat Jaringan

   Keamanan komunikasi jaringan juga masalah yang penting. Apalagi sekarang teknologi wireless sedang marak-maraknya. Pada saat teknologi wireless masih baru lahir, banyak pakar dan praktisi TIK menilai penggunaan jaringan wireless merupakan jaringan yang paling rentan terhadap gangguan dan perusakan. Terlepas dari itu semua, keamanan jaringan komunikasi ini juga sangat vital. Bentuknya bisa penyusupan ke jaringan, gangguan jaringan (flooding), atau bahkan perusakan sarana dan prasarana komunikasi

jaringan (vandalism). Perangkat jaringan adalah peralatan jaringan komunikasi data seperti: modem, hub, switch, router, dan lain-lain.

BAB III
TATA LAKSANA

3.1 Pengamanan Secara Fisik

Ada beberapa faktor pengamanan sistem komputer perlu pengawasan secara khusus, diantaranya :

1. Manusia
   a. Merusak secara sengaja maupun tidak sengaja
   b. Menggangu seperti menebar virus, hacker
   c. Mencuri
      1) Fisik: Mencuri peramgkat keras computer
      2) Logic: data dengan menyadap, mengcopy, memotret, dan lainnya

   Penanggulangan:
   a. Merancang area yang terbatas, data tersimpan di server (data central)
   b. Melidungi sebagian peralataan komputer dengan kerangka besi (braket), password, sistem biometric pada pintu masuk ruangan
2. Binatang

   Yang berbahaya dari binatang adalah urine mengandung zat-zat yang bersifat asam, sehingga dapat melarutkan materi yang bersifat logam seperti Tembaga (Cu), Besi (Fe) dan Emas (Au) Motherboard menggunakan tembaga dan emas sehingga harus dilindungi dari urine binatang.

   Penanggulangan:
   a. Menjaga kebersihan komputer
   b. Menghalangi jalan masuk kedalam dengan kasa
   c. Jangan menggunakan kapur barus karena kapur barus akan menyublim pada udara bebas, gas yang dihasilkan dapat menempel pada benda lain dan mengkristal.
3. Tumbuhan

   Ada 3 jenis tumbuhan yang perlu di waspadai, yaitu:
   a. Jamur
   b. Lumut
   c. Ganggang Biru

   Ketiganya mudah tumbuh pada lingkungan yang kelembaban nya tinggi.

   Penanggulangan:
   b. Gunakan AC untuk ruang kerja
   a. Gunakan Silica Gel untuk tempat penyimpanan
4. Cuaca & Iklim
   a. Kelembaban Udara (Kadar Air Udara). Udara yang lembab dapat menyebabkan tumbuhan jamur, lumur, dan ganggang biru.

      Penanggulangan:
      1) Gunakan AC untuk ruang kerja
      2) Gunakan Silica Gel untuk tempat penyimpanan
   b. Angin (udara yang bergerak) Dapat membawa debu, materi-materi kecil, membuat kabel komunikasi bergetar sehingga mengganggu pengiriman data.

      Penanggulangan:

      Bersihkan computer secara berkala

c. Debu lembab cenderung bersifat konduktor (dapat mengakibatkan hubungan singkat). Bila menempel pada head baca tulis, permukaan disket, pita magnetic dapat mengganggu proses baca tulis.
Penanggulangan:
Gunakan penghisap debu, bersihkan computer secara berkala, simpan media penyimpanan dengan media yang tertutup, dan lainnya

d. Cuaca mendung menggakibatkan temperature meningkat
Penanggulangan:
Gunakan AC untuk mengatur suhu udara

e. Hujan mengakibatkan kelembaban udara meningkat
Penanggulangan:
Gunakan AC untuk mengurangi kelembababan udara

f. Petir cenderung menyambar sesuatu yang relative paling tinggi
Penanggulangan:
Gunakan penangkal petir, hindari pemasangan kabel dari logam diudara, dll.

g. Iklim pada suhu panas, material akan memuai, pada suhu dingin akan menyusut. Pemuaian dan penyusutan akan merusak komponen computer.
Penanggulangan:
Gunakan AC untuk mengatur suhu ruangan

5. Fisika & Kimia
   a. Panas
      1) Dapat terjadi dari dalam komputer, ruangan dan luar ruangan
      2) Dari dalam computer disebabkan karena komponen elektronik dialiri arus listrik
      3) Dari ruangan disebabkan karena alat pemanas, seperti pemanas air, kompor
      4) Dari luar ruangan lebih disebabkan dari panas matahari.

      Penanggulangan:
      1) Gunakan kipas angin (fan) atau heat sink pada komponen yang mudah panas.
      2) Gunakan kaca film atau Gordeyn, untuk menghindari masuknya sinar matahari.
      3) Gunakan AC untuk mengatur suhu udara ruangan

   b. Listrik
      1) Kelebihan voltase: dapat merusak komponen elektronik
      2) Mati Listrik: membuat sistem operasi rusak

      Penanggulangan
      Gunakan stabilizer untuk menstabilkan voltase

   c. Magnet
      1) Dapat merusak media penyimpanan
      2) Dapat mempengaruhi head pada disk drive

      Penanggulangan:
      Jauhkan dari magnet

   d. Suara
      Getaran suara dapat mempengaruhi head dari disk
      Penanggulangan:
      Jauhkan dari sumber bunyi yang kuat

   e. Kimia
      1) Kebocoran baterai
      2) Bahan kimia yang keluar dari baterai yang bocor dapat merusak motherboard

      Penanggulangan:
      Lakukan pemeriksaan secara berkala

3.2 Pengamanan Akses

Pengamanan akses dikerjakan untuk PC yang memakai system operasi penguncian serta system operasi jaringan. Maksudnya adalah untuk menghadapi peristiwa yang sifatnya disengaja atau tak disengaja, seperti kelalaian atau keteledoran pemakai yang kerapkali meninggalkan komputer dalam kondisi masih tetap menyala atau bila ada pada jaringan komputer masih tetap ada dalam login user. Pada komputer, jaringan pengamanan komputer yaitu tanggungjawab administrator yang dapat mengatur serta mendokumentasi semua akses pada system komputer dengan baik. Akses kontrol di bagi menjadi beberapa kategori, diantaranya :

1. ***Administrative Control***

   Akses ini dimiliki oleh unit IT untuk merubah, menghapus dan mendesign suatu rancangan sistem (full kontrol).

   Yang dapat diakses :

   a. Data Server
   b. Database yang ada di server
   c. Backupdata server
   d. Merubah dan menghapus data
   e. Mendesign maping data

2. ***Physical Control***

   Akses ini difungsikan untuk mengaman fisik server. Ruang server hanya dapat dimasuki oleh kepala SIRS dan orang yang sudah memiliki ijin dari kepala SIRS. Semua aktivitas baik maintenance maupun backup data tercatat dalam form laporan. Adapun pengaman ruang server, diantaranya :

   a. Server pelayanan maupun server data di tempatkan diruangan khusus
   b. Ruang server terkunci, hanya kelapa SIRS dan orang yang memiliki ijin oleh kepala SIRS saja yang dapat mengakses server.
   c. Ruang server termonitoring 24 jam menggunakan CCTV

3. ***Technical Control***

   Akses yang digunakan untuk membatasi akses subjek ke objek. Melindungi integritas dan ketersediaan sumber dengan membatasi jumlah subjek yang bisa mengakses objek. Melindungi kenyamanan sumber dengan mencegah penyingkapan ke subjek yang tidak dikenal. Hak akses ini digunakan oleh setiap unit, artinya setiap unit hanya dapat mengakses data unitnya saja sedangkan data unit lain tidak dapat diakses. Komponen pendukung :

   a. Akses Sistem, sistem akan membatasi hak akses disetiap unit
   b. Akses Jaringan, semua komputer yang ada ri rumah sakit harus terkoneksi dengan jaringan
   c. Enkripsi dan Protokol, setiap mengakses server data wajib memasukkan password sebagai scurity hak akses

3.3 Pengamanan Data

Pengamanan data terbagi menjadi pengaman dari dalam komputer, dari luar komputer dan backup data.

1. Pengamanan data dari dalam komputer
   a. Lindungi komputer dengan cara memeberi password dikomputer kerja. Hal ini dapat mengamankan data di komputer. Untuk pemberian password dapat menggunakan tools yang ada disediakan di windows.

b. Pencegahan virus. Melindungi komputer terhadap virus. Gunakan pelindung virus yang canggih dan diperbarui setiap bulan. Periksa setiap dokumen yang masuk ke komputer menggunakan antivirus yang sudah di perbarui.

2. Pengamanan data dari luar komputer
   Pengamanan file di dalam komputer tidak ada gunanya bila komputer itu rusak atau dicuri. Sebaiknya pula mengamankan file anda di tempat lain.
   a. Backup ke DVD□ROM. DVD□ ROM cocok untuk jumlah data cukup besar (sampai 4,7 GB setiap disk). Ada dua macam DVD□ROM:
      - DVD□R (read only), yang dapat ditulisi sekali saja.
      - DVD□RW (read□write) yang dapat ditulisi berulang□ulang
   b. Simpan ke jaringan (Server data). Menyimpan data penting di simpan didalam server data yang sudah diberikan oleh unit SIRS. Akses ke dalam server data terproteksi oleh password, pengelolahan password dilakukan oleh kepala SIRS dan di distribusikan kepada setiap kepala unit
3. Backup Data
   Proses backup data dilakukan setiap hari dilakukan secara otomatis setiap pukul 12 malam. Data yang dibackup meliputi database server pelayanan, database server BPJS, database server INACBG's, database server Tata Usaha dan server data. Data tersebut tersimpan didalam NAS (Network Attached Storage). NAS memilki fungsi penyimpanan data dengan sistem operasi yang dikhususkan untuk melayani kebutuhan *backup* dan *share* data. NAS dapat di akses langsung melalui jaringan dengan protokol seperti TCP/IP . NAS ini dilengkapi dengan tempat penyimpanan berupa harddisk, memiliki perangkat lunak sendiri untuk pengelolaan dan bertugas untuk menyimpan/backup serta men-*share* file dalam sebuah jaringan. NAS memiliki 4 hardisk masing-masing hardisk memiliki ukuran penyimpanan sebesar 4 tera byte, sehingga total penyimpanan sebesar 16 tera byte.

3.4 Pengamanan Komunikasi Jaringan

Pengamanan komunikasi jaringan dikerjakan dengan memakai kriptografi di mana data yang sifatnya peka di-enkripsi atau disandikan terlebih dulu sebelumnya ditransmisikan lewat jaringan itu. Penggunaan jaringan itu sendiri digunakan untuk mengakses data dari komputer ke komputer lainnya. Adapun proses pengamanan jaringan yang sudah kita lakukan, diantaranya :

1. Membatasi akses ke jaringan
   Pembatasan-pembatasan dapat dilakukan sehingga memperkecil peluang penembusan oleh pemakai yang tak diotorisasi, misalnya :
   a. Pembatasan login. Login hanya diperbolehkan pada terminal tertentu, atau hanya ada waktu dan hari tertentu. Pembatasan dengan call-back (Login dapat dilakukan siapapun. Bila telah sukses login, sistem segera memutuskan koneksi dan memanggil nomor telepon yang telah disepakati, Penyusup tidak dapat menghubungi lewat sembarang saluran telepon, tapi hanya pada saluran telepon tertentu).
   b. Setiap komputer yang ada di rumah sakit wajib di beri TCP/IP. Klasifikasi TCP/IP dibedakan menjadi :
      1) IP server : 192.168.0.201 (server pelayanan), 192.168.0.10 (server tata usaha), 192.168.254 (server data), 192.168.0.3 (server INACBG's), 192.168.0.214 (server akreditasi)
      2) IP lokal : 192.168.10.2 – 254
      3) IP internet Maxindo : - 122.144.1.1, - 122.144.2.2
      4) IP internet Firtsmedia : - 111.94.159.250, - 140.0.223.250

c. Pembatasan jumlah usaha login. Login dibatasi sampai tiga kali dan segera dikunci dan diberitahu ke administrator. Semua login direkam dan sistem operasi melaporkan informasi-informasi berikut :
   1) Waktu, yaitu waktu pemakai login.
   2) Terminal, yaitu terminal dimana pemakai login.
   3) Tingkat akses yang diizinkan (read / write / execute / all)

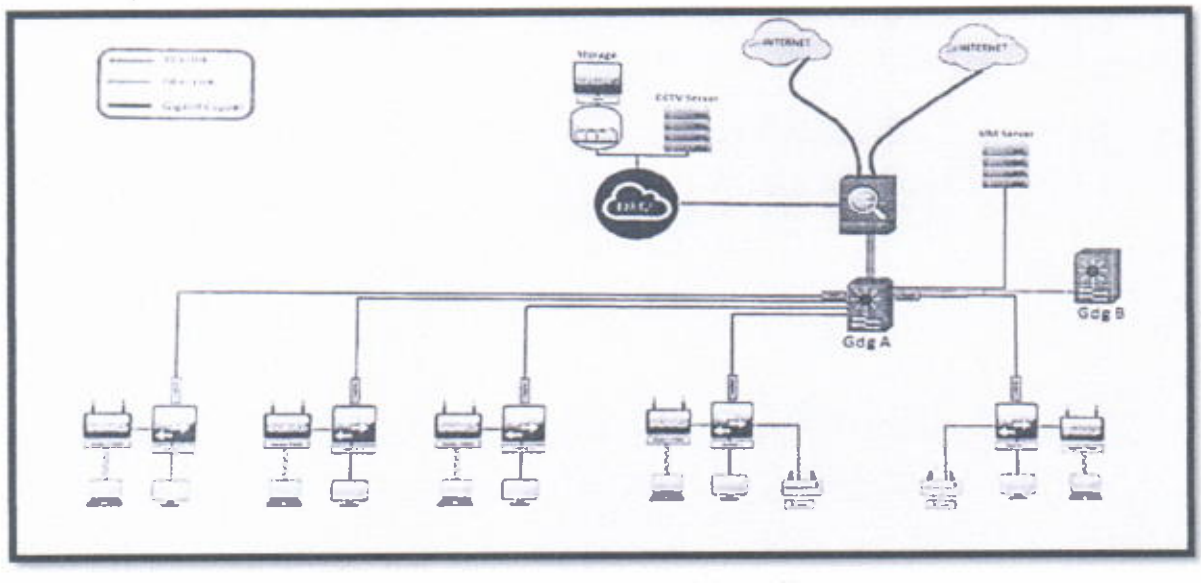
2. Penerapan Firewall

Secara prinsip, firewall dapat dianggap sebagai sepasang mekanisme : yang pertama memblok lalu lintas, yang kedua mengijinkan lalu lintas jaringan. Firewall dapat digunakan untuk melindungi jaringan dari serangan jaringan oleh pihak luar, namun firewall tidak dapat melindungi dari serangan yang tidak melalui firewall dan serangan dari seseorang yang berada di dalam jaringan anda, serta firewall tidak dapat melindungi dari program-program aplikasi yang ditulis dengan buruk.

Secara konseptual, terdapat dua macam firewall yaitu network level dan application level. Firewall network level mendasarkan keputusan mereka pada alamat sumber, alamat tujuan dan port yang terdapat dalam setiap paket IP. Network level firewall sangat cepat dan sangat transparan bagi pemakai. Application level firewall biasanya adalah host yang berjalan sebagai proxy server , yang tidak mengijinkan lalu lintas antar jaringan, dan melakukan logging dan auditing lalu lintas yang melaluinya. Application level firewall menyediakan laporan audit yang lebih rinci dan cenderung lebih memaksakan model keamanan yang lebih konservatif daripada network level firewall.

a. Packet Filtering

   Sistem paket filtering atau sering juga disebut dengan screening router adalah router yang melakukan routing paket antara internal dan eksternal network secara selektif sesuai dengan security policy yang digunakan pada network tersebut. Informasi yang digunakan untuk menyeleksi paket-paket tersebut adalah :
   1) IP address asal
   2) IP address tujuan
   3) Protocol (TCP, UDP, atau ICMP)
   4) Port TCP atau UDP asal
   5) Port TCP atau UDP tujuan



Gambar 3.1 Arsitektur Firewall

Sistem kerja firewall sebagai berikut :

1) IP Firewall https://172.16.16.1, dapat di akses melalui broser
2) Bloking 2 jalur provider internet, Maxindo dan Firstmedia. Mengamankan jaringan dari luar ke dalam maupun dari dalam keluar, sehingga dapat memblock akses dari virus dan dari hacker
3) Bloking Cloud CCTV
4) Mengcover seluruh jaringan local, firewall akan blok akses yang mencurigakan (yang tidak memilki akses)

BAB IV
DOKUMENTASI

1. Form Backup Data Base Server RS. Mata Undaan Surabaya
2. Topologi Jaringan
3. Pengamanan Ruang Server (pintu terkunci)
4. Pengaman Fisik Server (Rak Server)

Ditetapkan di Surabaya
Pada tanggal 04 April 2019
Direktur,

dr. Sudjarno, Sp.M (K)