BLUEPRINT

Roadmap Pengembangan Teknologi Informasi

2024 - 2027

Institut Agama Islam Negeri Manado

DAFTAR ISI

BAB I : Latar Belakang

Dalam perkembangan dunia Pendidikan terkini, persaingan dan peningkatan Teknologi Informasi Perguruan Tinggi sebagai nyawa dari pengembangan layanan dan kualitas IT. Kedepannya IT akan menjadi faktor penting dalam peningkatan akreditasi serta publisitas Perguruan Tinggi baik secara nasional maupun global.

Beberapa aspek penting dalam pengembangan IT di IAIN Manado dapat kami jabarkan sebagai berikut :

1. Peningkatan Kualitas Layanan Pendidikan: Mengingat peran penting teknologi informasi dalam memberikan layanan pendidikan yang berkualitas, perencanaan sistem teknologi informasi harus didorong oleh tujuan meningkatkan pengalaman belajar mahasiswa, memfasilitasi kegiatan akademik dan administratif, serta mendukung proses pengajaran dan pembelajaran secara efektif.
2. Integrasi Sistem: Dalam lingkungan perguruan tinggi yang kompleks, sering kali ada berbagai sistem informasi yang beroperasi secara terpisah. Roadmap pengembangan harus mencakup upaya untuk mengintegrasikan sistem-sistem ini agar dapat berfungsi secara sinergis dan mengurangi duplikasi data serta kerumitan administrasi.
3. Kepatuhan Terhadap Standar Pendidikan: Perguruan tinggi di Indonesia harus memastikan bahwa sistem teknologi informasi mereka memenuhi standar dan regulasi yang ditetapkan oleh Kementerian Pendidikan, seperti Sistem Informasi Akademik dan Keuangan (SIAK) yang dikelola oleh Direktorat Jenderal Pendidikan Tinggi.
4. Peningkatan Aksesibilitas dan Inklusivitas: Roadmap pengembangan harus memperhitungkan upaya untuk meningkatkan aksesibilitas dan inklusivitas sistem teknologi informasi, termasuk memastikan bahwa platform dan aplikasi yang digunakan dapat diakses dengan mudah oleh semua stakeholder, termasuk mahasiswa difabel.

5. Pengelolaan Data Mahasiswa dan Alumni: Mengingat pentingnya data mahasiswa dan alumni dalam pengelolaan akademik, perekrutan, dan pengembangan jaringan alumni, sistem teknologi informasi harus mampu mengelola data ini dengan efisien dan aman sesuai dengan peraturan perlindungan data pribadi.
6. Peningkatan Keamanan Informasi: Dengan meningkatnya ancaman keamanan cyber, roadmap pengembangan harus memprioritaskan langkah-langkah untuk memperkuat keamanan sistem informasi perguruan tinggi, termasuk penerapan praktik terbaik dalam perlindungan data, deteksi ancaman, dan respons kejadian.
7. Pengembangan Kompetensi SDM: Sistem teknologi informasi hanya akan efektif jika didukung oleh SDM yang kompeten. Oleh karena itu, roadmap harus mencakup inisiatif untuk meningkatkan kompetensi teknis dan manajerial staf IT serta meningkatkan kesadaran tentang keamanan informasi di seluruh perguruan tinggi.
8. Fleksibilitas dan Skalabilitas: Mengingat dinamika perguruan tinggi, roadmap pengembangan harus mempertimbangkan kebutuhan akan sistem yang fleksibel dan dapat diskalakan, sehingga dapat dengan mudah disesuaikan dengan perubahan kebutuhan organisasi dan pertumbuhan jumlah pengguna.

Dengan memperhatikan aspek-aspek ini, roadmap pengembangan sistem teknologi informasi dapat membantu perguruan tinggi di Indonesia meningkatkan efisiensi, kualitas layanan, dan kepatuhan terhadap standar pendidikan yang berlaku.

1.1. Visi & Misi UPT TIPD

Visi:

“Menjadi pusat inovasi teknologi informasi yang memimpin dalam mendukung transformasi digital dan meningkatkan pengalaman teknologi informasi di lingkungan akademik.”

Misi:

1. Menyediakan solusi teknologi informasi yang inovatif dan terjangkau untuk mendukung kegiatan akademik, teknologi, penelitian, dan pengabdian.
2. Meningkatkan aksesibilitas, ketersediaan, dan keamanan infrastruktur IT untuk memastikan penggunaan yang efisien dan efektif.

3. Mengembangkan dan memelihara sistem informasi terpadu yang memungkinkan manajemen data yang akurat dan analisis yang mendalam untuk pengambilan keputusan yang lebih baik.
4. Mengintegrasikan teknologi baru dan tren terkini, seperti kecerdasan buatan dan analitik data, untuk meningkatkan efisiensi dan inovasi dalam pendidikan dan penelitian.
5. Memberikan pelatihan dan dukungan teknis yang berkualitas kepada staf, dosen, dan mahasiswa untuk meningkatkan literasi digital dan pemanfaatan teknologi dalam pembelajaran.
6. Berkolaborasi dengan berbagai pemangku kepentingan di perguruan tinggi untuk memahami dan memenuhi kebutuhan teknologi informasi mereka secara komprehensif.
7. Berkomitmen pada prinsip keberlanjutan dan etika dalam pengelolaan dan penggunaan teknologi informasi, termasuk perlindungan data dan privasi pengguna.

1.2. Tujuan Pengembangan Blueprint Sistem Informasi Manajemen bagi IAIN Manado

1. Meningkatkan Efisiensi Operasional: Tujuan utama dari pembuatan blueprint ini adalah untuk meningkatkan efisiensi dalam operasi sehari-hari di IAIN Manado. Ini termasuk pengelolaan administrasi akademik, keuangan, sumber daya manusia, dan infrastruktur secara lebih efisien melalui penggunaan sistem informasi yang terintegrasi.
2. Meningkatkan Kualitas Layanan Akademik: Sistem informasi yang baik dapat meningkatkan kualitas layanan akademik yang diberikan kepada mahasiswa dan staf akademik. Tujuan ini mencakup penyediaan akses yang lebih mudah terhadap informasi akademik, pembayaran online, pendaftaran kursus, dan pengelolaan jadwal kuliah
3. Meningkatkan Pengambilan Keputusan: Pembuatan blueprint ini bertujuan untuk menyediakan data yang akurat dan terkini kepada para pemangku kepentingan di IAIN Manado untuk mendukung pengambilan keputusan yang lebih baik. Ini mencakup analisis data yang lebih baik untuk keperluan perencanaan strategis, peningkatan kualitas pengajaran, dan pengelolaan sumber daya.
4. Memperkuat Kepatuhan Regulasi: Blueprint ini juga bertujuan untuk memastikan bahwa sistem informasi yang dikembangkan sesuai dengan regulasi dan standar yang berlaku di

bidang Pendidikan tinggi, termasuk regulasi yang dikeluarkan oleh Kementerian Agama dan Direktorat Jenderal Pendidikan Tinggi.

5. Meningkatkan Ketersediaan Informasi dan Transparansi: Salah satu tujuan utama adalah untuk meningkatkan ketersediaan informasi dan transparansi di antara seluruh pemangku kepentingan di IAIN Manado. Hal ini dapat dicapai dengan memberikan akses yang lebih mudah terhadap informasi akademik, keuangan, dan akreditasi melalui portal online yang terintegrasi.
6. Memperbaiki Proses Pengelolaan Data Mahasiswa dan Alumni: Blueprint ini bertujuan untuk meningkatkan pengelolaan data mahasiswa dan alumni, termasuk pendaftaran, pencatatan akademik, pemantauan kemajuan belajar, dan pelacakan alumni. Hal ini akan memungkinkan IAIN Manado untuk memperbaiki layanan yang diberikan kepada mahasiswa dan mendukung hubungan yang lebih baik dengan alumni.
7. Mendorong Inovasi Teknologi: Pembuatan blueprint ini juga bertujuan untuk mendorong adopsi inovasi teknologi terbaru di IAIN Manado, seperti kecerdasan buatan, analitik data, dan teknologi cloud computing. Hal ini akan membantu perguruan tinggi tetap kompetitif dan relevan dalam lingkungan Pendidikan tinggi yang terus berubah.

1.3. Manfaat Hasil Pengembangan Sistem Informasi Manajemen bagi IAIN Manado

Beberapa manfaat hasil pengembangan sistem informasi manajemen bagi IAIN Manado:

1. Peningkatan Efisiensi Operasional: Sistem informasi manajemen yang terintegrasi akan membantu meningkatkan efisiensi dalam berbagai proses operasional di IAIN Manado, seperti administrasi akademik, keuangan, sumber daya manusia, dan infrastruktur. Hal ini akan mengurangi waktu dan sumber daya yang dibutuhkan untuk menjalankan proses-proses tersebut.
2. Peningkatan Kualitas Layanan Akademik: Dengan adanya sistem informasi yang terintegrasi, mahasiswa dan staf akademik akan mendapatkan layanan akademik yang lebih baik dan lebih cepat. Contohnya, mahasiswa dapat dengan mudah mengakses informasi

mengenai jadwal kuliah, hasil ujian, dan perkembangan akademik mereka melalui portal online yang terintegrasi.

3. Pengambilan Keputusan yang Lebih Baik: Sistem informasi manajemen akan menyediakan data yang akurat dan terkini kepada pimpinan dan pengelola IAIN Manado untuk mendukung pengambilan keputusan yang lebih baik dan berbasis data. Dengan adanya informasi yang mudah diakses dan dianalisis, pimpinan dapat membuat keputusan yang lebih tepat dan strategis.
4. Peningkatan Kepatuhan Regulasi: Pengembangan sistem informasi manajemen yang sesuai dengan regulasi dan standar yang berlaku akan membantu IAIN Manado untuk mematuhi peraturan pemerintah dan standar akreditasi. Hal ini akan mengurangi risiko pelanggaran regulasi dan meningkatkan reputasi 5olisti di mata pemangku kepentingan.
5. Peningkatan Ketersediaan Informasi dan Transparansi: Dengan adanya sistem informasi yang terintegrasi, informasi mengenai berbagai aspek operasional dan akademik IAIN Manado akan lebih mudah diakses dan lebih transparan bagi semua pihak yang berkepentingan, termasuk mahasiswa, orang tua mahasiswa, staf, dan pihak eksternal.
6. Peningkatan Hubungan dengan Mahasiswa dan Alumni: Sistem informasi manajemen yang baik akan membantu IAIN Manado untuk memperbaiki hubungan dengan mahasiswa dan alumni. Misalnya, sistem dapat digunakan untuk mengirimkan pengumuman, survei kepuasan, dan informasi alumni secara teratur, sehingga memperkuat keterlibatan dan loyalitas mereka terhadap perguruan tinggi.
7. Peningkatan Inovasi dan Daya Saing: Dengan adanya sistem informasi manajemen yang canggih dan terintegrasi, IAIN Manado akan menjadi lebih inovatif dan kompetitif dalam menghadapi tantangan dan peluang di dunia pendidikan yang terus berubah. Sistem ini akan memungkinkan perguruan tinggi untuk mengadopsi teknologi baru dan praktik terbaik secara lebih cepat dan efektif.

BAB II : Langkah Penyusunan Blueprint Sistem Informasi Manajemen

Beberapa Langkah-langkah dalam penyusunan Sistem Informasi Manajemen di IAIN Manado adalah sebagai berikut :

1. Identifikasi Kebutuhan dan Tujuan yaitu mengidentifikasi kebutuhan dan tujuan dari sistem informasi manajemen. Ini melibatkan pengumpulan informasi dari berbagai pemangku kepentingan di IAIN Manado, termasuk pimpinan, staf akademik dan dosen, mahasiswa, dan pihak eksternal. Pastikan untuk memahami tantangan yang dihadapi dan harapan mereka terhadap sistem baru.
2. Analisis Proses Bisnis yaitu melakukan analisis mendalam terhadap proses bisnis yang ada di IAIN Manado, termasuk administrasi akademik, keuangan, sumber daya manusia, dan infrastruktur. Identifikasi area-area di mana implementasi sistem informasi dapat meningkatkan efisiensi dan produktivitas.
3. Penentuan Ruang Lingkup: Tentukan ruang lingkup dari blueprint sistem informasi manajemen. Pilih komponen-komponen yang akan disertakan dalam sistem, seperti sistem informasi akademik, sistem keuangan, sistem manajemen sumber daya manusia, dan lain-lain. Tentukan juga fitur-fitur yang diinginkan dan prioritas pengembangan.
4. Identifikasi Teknologi dan Sumber Daya: Tinjau teknologi yang tersedia dan sumber daya yang dibutuhkan untuk implementasi sistem informasi manajemen. Pertimbangkan apakah akan menggunakan platform yang sudah ada atau membangun sistem baru dari awal. Pastikan juga untuk memperhitungkan anggaran yang tersedia untuk proyek ini.
5. Rancang Arsitektur Sistem: Rancang arsitektur sistem informasi manajemen yang akan memenuhi kebutuhan dan tujuan yang telah ditetapkan. Ini melibatkan pemilihan teknologi, pembuatan diagram alir data, dan perencanaan integrasi antar sistem.
6. Pengembangan Rencana Implementasi: Buatlah rencana implementasi yang detail, termasuk jadwal waktu, alokasi sumber daya, dan tahapan-tahapan pengembangan.

Pastikan untuk melibatkan semua pemangku kepentingan dalam proses ini dan memberikan pelatihan yang cukup kepada staf yang akan menggunakan sistem baru.

7. Uji Coba dan Evaluasi: Lakukan uji coba terhadap sistem informasi manajemen yang telah dikembangkan untuk memastikan kelayakan dan kinerjanya. Dapatkan umpan balik dari pengguna dan identifikasi area yang perlu diperbaiki sebelum implementasi penuh dilakukan.
8. Implementasi dan Peluncuran: Implementasikan sistem informasi manajemen sesuai dengan rencana yang telah disusun. Pastikan untuk memberikan dukungan teknis yang memadai kepada pengguna selama fase peluncuran dan pemeliharaan sistem.
9. Pemantauan dan Pemeliharaan: Setelah peluncuran, lakukan pemantauan terhadap kinerja sistem informasi manajemen secara teratur. Lakukan pemeliharaan rutin dan perbaikan jika diperlukan untuk memastikan sistem tetap berjalan dengan baik dan memenuhi kebutuhan pengguna.
10. Evaluasi dan Penyempurnaan: Lakukan evaluasi secara berkala terhadap kinerja sistem informasi manajemen dan identifikasi peluang-peluang untuk penyempurnaan. Libatkan pemangku kepentingan dalam proses ini dan terus tingkatkan sistem sesuai dengan kebutuhan yang berkembang.

1.4. Landasan Teori

1.4.1. Konsep Strategi

Teori Pengelolaan Strategis (Strategic Management Theory) adalah Teori ini mempelajari bagaimana organisasi merencanakan, menerapkan, dan mengevaluasi keputusan strategis untuk mencapai tujuan jangka panjangnya. Fokus utamanya adalah pada analisis lingkungan eksternal dan internal organisasi, pengembangan strategi yang sesuai, serta implementasi dan evaluasi strategi tersebut (Alfred Chandler, 1962; Henry Mintzberg, 1978; Michael Porter, 1980).

Pemikiran Sistem (Systems Thinking) adalah konsep yang menekankan pandangan sistem terhadap organisasi dan lingkungannya, dengan memandangnya sebagai suatu sistem yang kompleks dan saling terkait. Pemikiran sistem membantu dalam memahami dampak dari

keputusan strategis terhadap seluruh organisasi dan memperhitungkan hubungan antara bagian-bagian organisasi (Ludwig von Bertalanffy, 1968; Peter Senge, 1990).

2.1.2 Perencanaan Strategi Sistem Informasi

Perencanaan sistem informasi adalah proses strategis untuk merencanakan, mengorganisasikan, dan mengelola sumber daya serta aktivitas yang terkait dengan sistem informasi dalam suatu organisasi. Tujuan utamanya adalah untuk memastikan bahwa teknologi informasi digunakan secara efektif dan efisien dalam mendukung tujuan bisnis atau tujuan organisasi secara keseluruhan.

Perencanaan sistem informasi melibatkan identifikasi kebutuhan informasi organisasi, penentuan sumber daya yang diperlukan, dan pengembangan rencana strategis untuk penggunaan teknologi informasi. Proses ini juga mencakup evaluasi lingkungan bisnis eksternal dan internal, analisis sistem informasi yang ada, serta identifikasi peluang dan tantangan dalam penerapan teknologi informasi (Turban, E., Leidner, D., McLean, E., & Wetherbe, J. : 2005).

Perencanaan Strategi Sistem Informasi (PSSI) merupakan suatu pendekatan terstruktur untuk mengelola penggunaan teknologi informasi (TI) dalam mencapai tujuan bisnis organisasi. Teori Turban, Leidner, McLean, dan Wetherbe menawarkan kerangka kerja yang komprehensif untuk merencanakan strategi sistem informasi. Berikut adalah penjelasan tentang perencanaan strategi sistem informasi berdasarkan teori yang mereka kemukakan:

1. Pengenalan dan Evaluasi Sistem Informasi:

   Tahap awal dalam perencanaan strategi sistem informasi adalah pengenalan dan evaluasi sistem informasi yang ada. Ini melibatkan audit dan analisis dari sistem informasi yang sedang berjalan, termasuk infrastruktur TI, aplikasi, dan proses bisnis yang terkait.
2. Identifikasi Kebutuhan Bisnis:

   Setelah mengevaluasi sistem informasi yang ada, langkah berikutnya adalah mengidentifikasi kebutuhan bisnis organisasi. Ini melibatkan pemahaman mendalam tentang tujuan, proses bisnis, dan tantangan yang dihadapi oleh organisasi.

3. Perumusan Strategi TI:

   Berdasarkan kebutuhan bisnis yang teridentifikasi, organisasi kemudian merumuskan strategi TI yang sesuai. Ini melibatkan pemilihan teknologi yang tepat dan pengembangan rencana aksi untuk mengintegrasikan TI ke dalam operasi bisnis.

4. Pembangunan Infrastruktur TI:

   Tahap ini melibatkan pembangunan infrastruktur TI yang diperlukan untuk mendukung strategi TI yang telah dirumuskan. Ini mungkin melibatkan investasi dalam perangkat keras, perangkat lunak, jaringan, dan sumber daya TI lainnya.

5. Pengembangan dan Implementasi Aplikasi:

   Setelah infrastruktur TI dibangun, organisasi kemudian mengembangkan dan mengimplementasikan aplikasi yang diperlukan untuk mendukung proses bisnis. Ini bisa berupa aplikasi internal seperti Sistem Informasi Manajemen (SIM) atau aplikasi eksternal seperti sistem e-commerce.

6. Manajemen Perubahan dan Penggunaan:

   Manajemen perubahan menjadi kunci dalam memastikan keberhasilan strategi sistem informasi. Ini melibatkan pelatihan pengguna, komunikasi yang efektif, dan pemantauan terus-menerus terhadap adopsi dan penggunaan sistem baru.

7. Evaluasi dan Pembaruan

   Evaluasi terus menerus diperlukan untuk memastikan bahwa strategi sistem informasi tetap relevan dan efektif seiring waktu. Organisasi perlu melakukan pembaruan dan penyesuaian sesuai dengan perubahan dalam lingkungan bisnis dan teknologi.

Kajian teori diatas menekankan pentingnya integrasi strategi sistem informasi dengan strategi bisnis yang lebih luas. Pendekatan mereka menyoroti perlunya keterlibatan tingkat tinggi manajemen, kerjasama lintas departemen, dan fokus pada pencapaian tujuan bisnis organisasi melalui penggunaan teknologi informasi yang strategis.

2.1.3 Smart Campus

Smart campus merupakan konsep penggunaan teknologi informasi dan komunikasi (TIK) yang canggih untuk meningkatkan efisiensi, kenyamanan, keamanan, dan keberlanjutan

lingkungan di lingkungan kampus. Smart campus mencakup integrasi berbagai sistem dan layanan, seperti internet of things (IoT), analitika data, kecerdasan buatan (*artificial intelligence*), dan sistem manajemen informasi terpadu, untuk menciptakan lingkungan pembelajaran dan pengelolaan kampus yang lebih efektif.

Teknologi dalam smart campus dapat digunakan untuk berbagai tujuan, termasuk pemantauan dan pengelolaan energi, pengelolaan fasilitas, keamanan kampus, pengumpulan data akademik, dan layanan digital untuk mahasiswa dan staf. Tujuan utamanya adalah untuk menciptakan lingkungan yang mendukung pembelajaran inovatif, penelitian yang berkualitas, dan pengelolaan yang efisien di lingkungan kampus (Sultan, N. : 2019).

2.1.4 Pelayanan

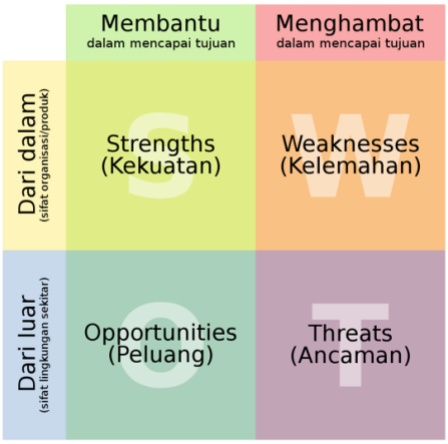
Pelayanan adalah serangkaian tindakan atau kegiatan yang dilakukan oleh individu, organisasi, atau lembaga untuk memenuhi kebutuhan, keinginan, atau permintaan dari orang lain atau pelanggan. Pelayanan dapat berupa penyediaan barang atau jasa, komunikasi, bantuan, atau dukungan yang diberikan dengan tujuan memberikan nilai tambah kepada penerima layanan.

Pelayanan seringkali melibatkan interaksi antara penyedia layanan dan penerima layanan, di mana penyedia layanan bertanggung jawab untuk memastikan bahwa kebutuhan atau permintaan pelanggan dipenuhi dengan baik dan memuaskan. Kualitas pelayanan sangat penting dalam membangun hubungan jangka panjang dengan pelanggan dan menciptakan pengalaman positif yang akan meningkatkan loyalitas pelanggan (Zeithaml, V. A., Bitner, M. J., & Gremler, D. D. : 2006).

2.1.5 Analisis SWOT

SWOT (Strengths, Weaknesses, Opportunities, Threats) adalah sebuah analisis yang digunakan untuk mengevaluasi faktor-faktor internal dan eksternal yang mempengaruhi kinerja atau strategi suatu organisasi. Analisis SWOT digunakan untuk mengidentifikasi kekuatan (strengths) dan kelemahan (weaknesses) internal organisasi serta peluang (opportunities) dan ancaman (threats) eksternal yang ada di lingkungan sekitar organisasi tersebut.

ANALISIS SWOT



Faktor Internal			
No	**Strengths**	**No**	**Weakness**
1	Ketersediaan SDM yang terampil di bidang teknologi informasi di kalangan dosen dan staf.	1	Kurangnya dana yang memadai untuk pengembangan dan pemeliharaan sistem informasi.
2	Infrastruktur teknologi yang sudah ada, seperti jaringan internet yang cepat dan komputer yang memadai.	2	Kurangnya pelatihan dan pemahaman tentang teknologi informasi di kalangan staf non-teknis.
3	Dukungan pimpinan perguruan tinggi terhadap pengembangan sistem informasi untuk meningkatkan efisiensi dan kualitas layanan.	3	Sistem informasi yang belum terintegrasi dengan baik antar departemen atau unit di IAIN Manado.

Faktor Ekternal			
No	**Opportunities**	**No**	**Threat**
1	Adopsi teknologi baru seperti kecerdasan buatan (AI) dan analitika data untuk	1	Persaingan dengan perguruan tinggi lain yang sudah memiliki sistem informasi yang lebih canggih dan terintegrasi.

	meningkatkan pengambilan keputusan dan pelayanan akademik.		
2	Kerjasama dengan industri atau lembaga lain untuk pengembangan sistem informasi yang lebih canggih dan terintegrasi.	2	Ancaman keamanan cyber yang meningkat, seperti serangan peretasan atau pencurian data.
3	Perkembangan teknologi informasi yang cepat di lingkungan industri dan pendidikan tinggi.	3	Perubahan regulasi pemerintah terkait privasi data dan keamanan informasi yang dapat mempengaruhi pengembangan dan implementasi sistem informasi.

2.1.6 Analisa Kebutuhan Aplikasi serta Solusinya

Analisa Kebutuhan Aplikasi serta Solusinya			
No	**Strategi**	**Kebutuhan Informasi**	**Solusi TIK**
1	Promosi produk Akademik IAIN Manado secara offline maupun online	Informasi prodi, sarpras, kurikulum, bahan ajar, ujian, dosen dan pengumuman	Website
2	Peningkatan Layanan Pendidikan	Menghubungkan interkoneksi layanan jaringan internet kampus	Membangaun koneksi fiber optic
3	Kerjasama dengan instansi pemerintah dan swasta	Informasi prodi, sarpras, kurikulum, bahan ajar, ujian, dosen dan informasi umum lainnya	Website
4	Peningkatan layanan Pendidikan melalui sistem informasi	Menggunakan aplikasi terintegrasi dengan data akademik dan administrasi akademik	Mengembangakn aplikasi terintegrasi
5	Mengadakan pelatihan untuk peningkatan kompetensi SDM	Data pegawai, hasil evaluasi, kebutuhan training dan hasil evaluasi setelah training	Dokumentasi daring berbasis multimedia
6	Peningkatan publikasi karya ilmiah di kampus	Data jurnal, pengelola dan dokumen publikasi	e-Journal
7	Akses koleksi buku perpustakaan	Informasi buku dan terbitan ilmiah lainnya	e-Library

8	Keterbukaan informasi	Informasi data surat penting pimpinan dan informasi aturan kampus	e-dokumen

2.1.7 Analisa Kebutuhan Perencanaan Strategis

No	Strategi	Infromasi	Solusi TIK
1	Penggunaan TIK dalam proses penyelenggaraan Pendidikan Tinggi di IAIN Manado	Informasi TIK	IT Master Plan
2	Implementasi Sistem TIK terintegrasi	Informasi IT Master Plan IAIN Manado	Membuat IT Master Plan
3	Standarisasi dan Kelengkapan catatan informasi terkait pengembangan aplikasi dan perangkat keras lainnya	Dokumentasi produk dan kegiatan	Dokumentasi yang terstandarisasi

2.1.8 Analisa Kebutuhan Infrastruktur Strategis

No	Strategi	Kebutuhan Informasi	Solusi TIK
1	Peningkatan jaringan WAN untuk lingkungan kampus IAIN Manado	Interkoneksi WAN (internet)	Infrastruktur jaringan komputer
2	Peningkatan layanan akademik melalui jaringan kabel dan nirkabel	Interkoneksi sarpras di lingkungan kampus	Membangun jaringan fiber optic dan wireless
3	Memiliki server on premises maupun cloud yang reliabel	Sistem server	Membangun server dan mengelola cloud server
4	Sarana pendukung (Gedung) yang terstandarisasi	Gedung yang sesuai dengan keperluan implementasi TIK	Membangan server on premises yang reliabel dan handal

2.1.9 Target yang Dicapai

Blueprint Sistem Informasi Management IAIN Manado dijabarkan sebagai berikut :

1. Target Jangka Panjang untuk setiap aspek yang dikembangkan, indikator keberhasilan serta evaluasinya
2. Melalukan pengembangan yang bertahap
3. Membuat rincian pengembangan

BAB III : Rencana dan Strategi Pengembangan

3.1 Ruang Lingkup Pengembangan

Ruang lingkup pengembangan Teknologi Informasi dan Komunikasi yang akan dilaksanakan dapat dijelaskan sebagai berikut:

3.1.1 Infraastruktur Perangkat Keras Sistem dan Jaringan

1. Perangkat Utama
    a. Pembangunan Data Center (Server on Premis)
    b. Revitalisasi Infratruktur Jaringan
    c. Pemasangan Perangkat Sekuriti
    d. Pemasangan Perangkat Monitoring dan Manajemen Akses Internet
2. Perangkat Pendukung
    a. Perangkat Monitoring
    b. Electronic dan Digital Library
    c. Pemasangan Video Conference
    d. Implementasi CCTV
    e. Digital Printing dan Publikasi

3.1.2 Infrastuktur Perangkat Lunak

1. Aplikasi Utama
    a. Sistem Informasi Akademik
    b. Sistem Informasi Keuangan
    c. Sistem Informasi PMB
    d. Sistem Informasi Tracer Study
    e. Dashboard Sistem Informasi (Laporan)
    f. Website
2. Aplikasi Pendukung
    a. Sistem seleksi beasiswa
    b. Sistem publikasi dokumen kampus

3.1.3 Sertifikasi Produk dan Layanan

Sertifikasi produk dan layanan IT di IAIN Manado merupakan langkah penting dalam memastikan bahwa semua produk dan layanan teknologi informasi yang digunakan dan disediakan oleh institusi tersebut memenuhi standar kualitas yang ditetapkan. Berikut adalah penjelasan lebih rinci tentang sertifikasi produk dan layanan IT di IAIN Manado:

3.1.3.1 Tujuan Sertifikasi

Tujuan utama dari sertifikasi produk dan layanan IT di IAIN Manado adalah untuk memastikan bahwa semua perangkat keras, perangkat lunak, jaringan, dan layanan-layanan TI lainnya yang digunakan atau disediakan oleh institusi memenuhi standar keamanan, kinerja, dan keandalan yang telah ditetapkan.

3.1.3.2 Proses Sertifikasi

Proses sertifikasi melibatkan serangkaian langkah-langkah evaluasi, pengujian, dan verifikasi untuk memastikan bahwa produk-produk dan layanan-layanan IT memenuhi persyaratan yang ditetapkan. Ini bisa melibatkan pemeriksaan oleh pihak internal atau eksternal, pengujian fungsionalitas, keamanan, serta kompatibilitas dengan infrastruktur TI yang ada.

3.1.3.3 Jenis Sertifikasi

Sertifikasi produk dan layanan IT di IAIN Manado dapat mencakup berbagai jenis teknologi dan layanan, seperti:

a. Sertifikasi perangkat keras seperti komputer, server, perangkat jaringan, dan perangkat penyimpanan data.
b. Sertifikasi perangkat lunak termasuk sistem operasi, aplikasi bisnis, perangkat lunak keamanan, dan perangkat lunak pendukung lainnya.
c. Sertifikasi jaringan termasuk infrastruktur jaringan, perangkat jaringan, dan protokol komunikasi.
d. Sertifikasi layanan IT seperti layanan cloud, manajemen TI, dukungan teknis, dan layanan keamanan.

3.1.3.4 Manfaat Sertifikasi

Sertifikasi produk dan layanan IT di IAIN Manado memiliki beberapa manfaat, antara lain:

a. Memastikan keamanan, keandalan, dan kinerja yang optimal dari infrastruktur dan layanan TI.
b. Menjamin bahwa teknologi yang digunakan mendukung kebutuhan operasional dan akademik institusi dengan baik.
c. Meningkatkan efisiensi dan produktivitas staf dan mahasiswa dengan menyediakan akses yang aman dan lancar ke layanan-layanan TI.
d. Mengurangi risiko keamanan dan kerentanan terhadap serangan cyber dan kegagalan sistem.

3.1.3.5. Pemeliharaan Sertifikasi

Sertifikasi produk dan layanan IT merupakan proses berkelanjutan yang memerlukan pemeliharaan dan pemantauan terus-menerus. Ini mencakup pembaruan perangkat lunak, perbaikan keamanan, peningkatan infrastruktur, serta pelatihan staf untuk memastikan bahwa sistem dan layanan terus memenuhi standar kualitas yang ditetapkan.

Dengan proses sertifikasi produk dan layanan IT yang efektif, IAIN Manado dapat memastikan bahwa infrastruktur dan layanan TI mereka memenuhi standar kualitas yang tinggi, yang pada gilirannya akan mendukung keberhasilan operasional dan akademik institusi.

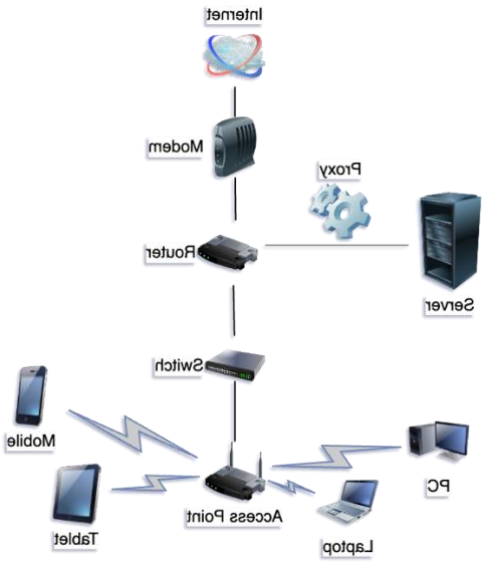
BAB IV : Infrastruktur ICT IAIN Manado Saat Ini

3.2 Internet

Saat ini penggunaan Bandwitdh Internet di IAIN Manado Kerjasama dengan PT. Telkom dengan jumlah total 2400 Mbps yang terdiri dari beberapa macam produk Kerjasama dan tersebar di 12 Titik di seluruh kampus, antara lain :

Penyebaran Titik Internet (Based on Switch per Gedung)

No	Gedung	Besaran	Produk	Satuan
1	Rektorat	200	Astinet	Mbps
2	Rektorat	200	Indibiz	Mbps
3	Fak. Tarbiyah	200	Indibiz	Mbps
4	Fak. Syariah	200	Indibiz	Mbps
5	Fak. EBI	200	Indibiz	Mbps
6	Fak. Ushuluddin	200	Indibiz	Mbps
7	Pascasarjana	200	Indibiz	Mbps
8	Gedung Ormawa	200	Indibiz	Mbps
9	Gedung Kuliah Terpadu	200	Indibiz	Mbps
10	Gedung Kuliah Lama	200	Indibiz	Mbps
11	Gedung Rusunawa Putra	200	Indibiz	Mbps
12	Taman & Gazebo	200	Indibiz	Mbps
Total		**2400**		**Mbps**

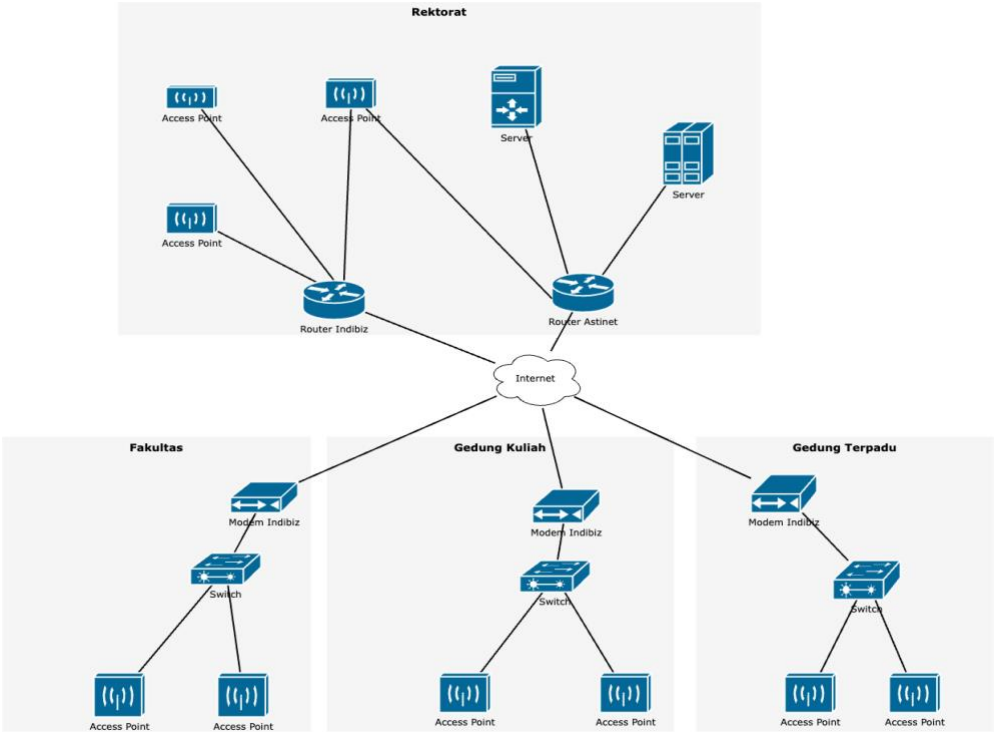


Gambar 1 : Prototipe desain topologi jaringan di IAIN Manado

Dengan jumlah mahasiswa aktif sekitar 3400 mahasiswa, alokasi bandwidth per mahasiswa mencapai 6,11 Mbps per mahasiswa yang sudah termasuk kategori baik.

3.3 Network

Topologi di IAIN Manado saat ini bersifat Desentralisasi yang mana setiap Gedung memiliki bandwidthnya tersendiri.



Gambar 2 : Implementasi topologi jaringan di IAIN Manado

Komponen networking antara lain :

- ONT Telkom
- Router Server
- Switch Rektorat
- Switch Gedung Fakultas/Unit/Lembaga
- Fiber Optik Converter
- Access Point

Konfigurasi pada gambar diatas memiliki beberapa kelemahan sebagai berikut :

- Bottleneck Bandwidth
- Keamanan karena belum SSO
- Belum ada perangkat manajemen akses untuk membagi dan mengontrol bandwidth dan user
- Apabila user semakin banyak maka Access Point akan overload

3.4 Server

Dalam menjalankan aplikasi di kampus IAIN Manado diperlukan server yang handal dan memiliki resource yang baik untuk menjalankan beberapa aplikasi kampus oleh karena itu IAIN Manado memiliki 6 unit server adalah sebagai berikut :

1. Server Aplikasi dan Website
    - CPU Intel Xeon E5-2670
    - 8 GB RAM DDR3
    - Ubuntu Server 20.04.6
    - MySQL 5, PHP 7, Apache
    - AAPanel Based
    - 2TB RAID0
2. Server Repository
    - CPU Intel Xeon E3-1220
    - 4GB RAM DDR3
    - 1 TB HDD
    - Debian 8
    - MySQL 5, PHP 7, Apache
3. Server NAS
    - CPU Intel Xeon E5-2670
    - 8 GB RAM DDR3
    - Ubuntu Server 20.04.6
    - MySQL 5, PHP 7, Apache
    - 4TB RAID0
4. Cloud Server
    - CPU Dual Intel Xeon E5-2620v3

- 32GB RAM
- 500GB SSD
- B/W Up to 1Gbps Unlimited IIX

3.5 Aplikasi

Sistem Informasi Akademik (SISKA) adalah suatu platform atau aplikasi perangkat lunak yang dirancang untuk mengelola dan menyimpan data terkait dengan kegiatan akademik, administrasi, dan manajemen di IAIN Manado. Sistem ini mencakup berbagai fitur dan modul yang membantu dalam pengelolaan informasi terkait mahasiswa, dosen, kurikulum, jadwal kuliah, registrasi, penilaian, dan pelaporan. SISKA saat ini running melalui alamat https://siska.iain-manado.ac.id.

Beberapa fungsi SISKA dalam menjalankan proses administrasi akademik dan keuangan di IAIN Manado sebagai berikut :

1. Pendaftaran Mahasiswa: Memfasilitasi proses pendaftaran mahasiswa baru dan pembaruan data pribadi mahasiswa yang sudah terdaftar.
2. Manajemen Data Mahasiswa: Menyimpan dan mengelola informasi pribadi, akademik, dan keuangan mahasiswa, termasuk riwayat akademik, status pendaftaran, dan pembayaran.
3. Manajemen Kurikulum: Merekam informasi tentang mata kuliah yang ditawarkan, struktur kurikulum, syarat mata kuliah, dan informasi lainnya terkait program studi.
4. Penjadwalan Kuliah: Membantu dalam menyusun jadwal kuliah yang efisien, mengkoordinasikan jadwal dosen dan ruang kelas, serta memberikan akses mudah kepada mahasiswa untuk melihat jadwal mereka.
5. Penilaian dan Nilai: Merekam hasil penilaian mahasiswa, menghitung nilai akhir, dan menyediakan akses kepada mahasiswa untuk melihat nilai-nilai mereka.
6. Pelaporan Akademik: Menghasilkan laporan akademik seperti daftar hadir, kartu studi, transkrip nilai, dan berbagai laporan lainnya yang diperlukan oleh dosen, mahasiswa, dan pihak administrasi.
7. Manajemen Dosen: Merekam informasi pribadi dan profesional dosen, jadwal mengajar, serta penugasan dan penilaian dosen.

8. Manajemen Fasilitas Akademik: Mengelola informasi tentang fasilitas akademik seperti ruang kelas, laboratorium, perpustakaan, dan fasilitas lainnya yang digunakan dalam proses pembelajaran.
9. Integrasi dengan Sistem Lain: Berintegrasi dengan sistem-sistem lain di IAIN Manado seperti sistem keuangan, dan manajemen sumber daya manusia untuk memfasilitasi pertukaran data antar departemen dan penggunaan data yang terkonsolidasi.

Sistem Informasi di IAIN Manado merupakan sistem informasi berbasis Web dengan detail sebagai berikut :

1. Website Institut, Fakultas, Lembaga, Unit, dan Program Studi
2. Sistem Informasi Akademik (SISKA)
    a. Modul Administrasi Aplikasi
    b. Modul Akademik
    c. Modul Keuangan
    d. Modul Penerimaan Mahasiswa Baru
    e. Modul Laporan
    f. Modul Akreditasi
    g. Modul Tracer Study
3. Open Journal System (OJS Based)
4. E-Catalog dan Peminjaman (SLIMS Based)
5. Repository (Eprints Based)
6. E-Document (Laravel Based)

BAB V : Menuju *Community Service University*, IAIN Manado berbasis ICT

Dalam mencapai visi misi kampus yang berbasis pada layanan pengabdian kepada masyarakat multikultural yang dimana salah satunya mencapai kampus yang maju dan kredibel serta berskala Internasional, maka hal tersebut tidak terlepas dari adanya implementasi Teknologi Informasi dan Komunikasi (TIK/ICT), maka perlu adanya tahapan prioritas pengembangan dan komitmen dari para pimpinan, karyawan, dan dosen.

Pengembangan Community Service University IAIN Manado terdiri dari pengembangan :

1. Infrastruktur TIK
2. Layanan Dasar
3. Aplikasi dan perangkat penunjang
4. Penyediaan konten digital
5. Pengelolaan data dan proses bisnis

Berdasarkan 5 pilar diatas yang akan menjadi pondasi dalam mengadakan Community Service University di IAIN Manado yang berbasis ICT sehingga dapat memberikan layanan yang kredibel, handal, tersisistem, efektif, dan efisien.

Selanjutnya adalah pengembangan Infrastruktur dan layanan dasar dalam pengelolaan layanan kampus yang objektif dan terbuka.

1. Infrastruktur Data Center
2. Infrastruktur Layanan Terintegrasi

BAB VI : Infrastruktur Datacenter

1. Konsep Infrastruktur Datacenter

Pembangunan DC yang baik dan terintegrasi diharuskan mempunyai beberapa sarana penunjang yang dapat diintegrasikan antara peralatan satu dengan peralatan yang lainnya dan berfungsi sesuai dengan standarisasi yang berlaku. Dalam mendesain dan membangun DC yang baik dan terintegrasi diharuskan mengacu pada standarisasi internasional dan implementator yang akan membangun DC harus mempunyai pengalaman yang cukup banyak membangun Data Center sehingga mengerti benar bagaimana mendesain dan membangun DC yang baik dan benar, kriteria dalam membangun Data Center adalah sebagai berikut:

- Perencanaan (Design, Soft Drawing, Time Frame)
- Implementasi (Approval Soft Drawing, Installation Working, Project Control & Management, dan sebagainya),
- Testing & Commissioning (Pengujian secara individual & integrasi)
- Training (Keseluruhan Sarana Penunjang)
- Dokumentasi (As built drawing, Konfigurasi Integrasi, Spesifikasi teknis dan lain-lain)
- Perawatan (Maintenance) sebelum dan setelah masa garansi habis

Manajemen harus dapat memutuskan apa yang akan diinvestasikan untuk keamanan dan kontrol TI dan bagaimana menyeimbangkan risiko dan investasi kontrol dalam lingkungan TI yang seringkali tidak dapat diprediksi. Walaupun keamanan dan kontrol sistem informasi membantu mengatasi risiko, namum tidak berarti risiko dapat dihilangkan. Sebagai tambahan, tingkat risiko secara tepat sulit untuk diketahui karena tidak selalu ada derajat kepastian. Manajemen harus memutuskan tingkat risiko yang dapat diterima perusahaan. Penilaian tentang level risiko yang dapat ditolerir, secara khusus jika dibandingkan dengan biaya, dapat menjadi keputusan manajemen yang sulit. Karena itu, manajemen membutuhkan kerangka kerja yang mengatur praktek keamanan dan kontrol TI untuk membuat standar bagi lingkungan TI yang telah ada maupun yang direncanakan.

Terjadi peningkatan kebutuhan pengguna layanan TI untuk diyakinkan, melalui akreditasi dan audit layanan TI yang disediakan oleh pihak ketiga, bahwa keamanan dan kontrol yang memadai telah tersedia. Implementasi kontrol TI yang baik, secara komersial, non-profit, atau kepemerintahan, masih dilanda kebingungan. Kebingungan itu timbul dari metode evaluasi yang berbeda, seperti evaluai ITSEC, TCSEC, ISO 9000, dan COSO internal control, dan lain-lain. Sebagai hasilnya, pengguna membutuhkan dasar umum untuk dibuat sebagai langkah pertama.

Dunia telah berubah dalam era digital, perubahan besar dapat dilihat pada bidang perekonomian. Transaksi ekonomi yang dilakukan saat ini telah berubah dari transaksi fisik menjadi transaksi elektronik. Penerapan eCommerce atau eBusiness dalam bidang perekonomian merupakan gambaran nyata perubahan perekonomian lama menjadi perekonomian baru atau perekonomian digital. Demikian juga pada bidang lain seperti pendidikan dengan eLearning, pemerintahan dengan eGoverment dan lain sebagainya. Perubahan ke era digital mengubah bentuk data dan media penyimpanan selama ini, data-data yang tersimpan tidak lagi dalam bentuk kertas. Seluruh data elektronik tersimpan dalam media seperti harddisk, CD, DVD, flash memory, dan lainnya. Seiring berjalannya waktu jumlah data akan bertambah besar sehingga dibutuhkan media penyimpanan dengan kapasitas yang besar. Mengolah dan memanajemen data dalam jumlah yang banyak tentulah tidak mudah sehingga pada sebuah organisasi yang besar untuk memanajemen data, mereka memusatkan data pada sebuah Data Center.

Data Center menyimpan semua data yang dibutuhkan oleh organisasi. Data tersebut diambil, diolah, dan disimpan kembali pada Data Center. Supaya Data Center dapat memberikan dukungan yang baik terhadap operasional organisasi, maka perlu manajemen data yang baik. Manajemen data menyangkut hal-hal berikut:

- Penciptaan (create) data terkait dengan elemen: make, receive, replicate
- Definisi data terkait dengan elemen: klasifikasi dan appraise
- Pemeliharaan data terkait dengan elemen: audibility, authenticity, media maintenance, performance, dan reliability.
- Penyimpanan data terkait dengan elemen: format, media, dan sistem penyimpanan

- Pengaksesan data terkait dengan elemen: authorization dan usability
- Disposisi data terkait dengan elemen: destroy dan retain

Data yang disimpan pada Data Center merupakan data yang memiliki nilai bagi organisasi, dengan manajemen data yang baik akan membuat data terlindungi. Manajemen data perlu didukung dengan proteksi data. Pengamanan data perlu dilakukan apalagi pada sebuah Data Center yang menyimpan semua data organisasi. Banyak teknik dan metode yang digunakan untuk melakukan pengamanan pada sebuah Data Center. Hal mengenai keamanan pada Data Center terutama keamanan fisiknya akan dibahas selanjutnya.

2. Sistem Keamanan Datacenter

Sistem pengamanan jaringan memiliki beberapa sub sistem pengaman utama yang masing-masing akan memiliki fungsionalitas pengamanan, yang disesuaikan dengan kebutuhan, tujuan, dan fungsi dari setiap perangkat yang akan dibangun secara bertahap dalam pejalannya.

Dalam bagian ini, pembahasan akan dimulai dengan pandangan umum terhadap keamanan komputer (computer security). Dilanjutkan dengan pembahasan mengenai Data Center secara umum dan ringkasan bagian-bagian keamanan sebuah Data Center yang terdiri dari keamanan fisik, keamanan data/informasi serta kebijakan atau manajemen keamanan Data Center.

Ada empat aspek utama dalam keamanan komputer:

- Privacy/Confidentiality, yaitu usaha menjaga informasi dari orang yang tidak berhak mengakses (mengaransi bahwa data pribadi tetap pribadi).
- Integrity, yaitu usaha untuk menjaga data atau sistem tidak diubah oleh yang tidak berhak.
- Authentication, yaitu usaha atau metoda untuk mengetahui keaslian dari informasi, misalnya apakah informasi yang dikirim dibuka oleh orang yang benar (asli) atau layanan dari server yang diberikan benar berasal dari server yang dimaksud.
- Availability, yaitu berhubungan dengan ketersediaan sistem dan data (informasi) ketika dibutuhkan.

Keempat aspek ini menjadi dasar untuk melakukan pengamanan terhadap sistem atau data. Keamanan komputer adalah sebuah proses, yang harus dijalankan untuk mengamankan sistem dan dalam penerapannya harus dilakukan dengan menyeluruh. Bagian-bagian keamanan yang ada pada Data Center mengacu pada empat aspek dasar keamanan yang disebutkan sebelumnya. Sebagai contoh keamanan fisik untuk pengamanan ruang penyimpanan data digunakan sensor biometric. Pengunaan sensor biometric tersebut menyangkut privacy, integrity, authentication, dan availabilty.

Bagian keamanan yang ada pada Data Center terkait satu dengan yang lainnya. Kita tidak dapat hanya menekankan keamanan terhadap data saja dengan menerapkan teknik dan metoda terbaru tetapi harus pula dibarengi dengan keamanan fisik dan kebijakan dalam rangka pengamanan data. Konvergensi antara keamanan data/informasi dengan keamanan fisik dalam Data Center merupakan hal yang tidak dapat dipisahkan untuk memberikan pengamanan yang terbaik pada sebuah Data Center.

Banyak contoh yang menggambarkan hal ini, misalnya proteksi data dilakukan dengan pengenkripsian 256 bit yang pastinya akan sangat sulit dipecahkan namun data tersebut di simpan dalam ruangan yang lembab atau ruangan yang mudah terbakar, maka bila suatu saat ruangan tempat penyimpanan data tersebut mengalami sesuatu seperti kebakaran, data yang kita proteksi dengan enkripsi 256 bit tidak akan berguna lagi. Contoh lain ruangan server yang ada pada Data Center dibersihkan oleh seorang petugas kebersihan dan tanpa sengaja dia menekan tombol power yang mengakibatkan server mati. Hal ini dapat mengakibatkan kerugian bagi sebuah organisasi, namun penyebab utama terjadinya hal ini karena kurangnya kebijakan keamanan yang tidak mengatur apa, kapan, siapa dan bagaimana pembersihan pada ruang server. Untuk itulah pentingnya juga memperhatikan aspek keamanan lainnya agar data dapat tersimpan dengan aman dan baik. Dalam point ini ditikberatkan pada keamanan fisik pada sebuah Data Center yang seringkali kurang menjadi perhatian penting dalam manajemen data pada Data Center.

2.1 Aspek Keamanan Data/Informasi Datacenter (Vritual)

Aspek keamanan data/informasi atau disebut juga keamanan virtual pada Data Center menyangkut hal-hal sebagai berikut:

- Kontrol akses logikal: menyangkut apa, siapa dan bagaimana data diakses secara virtual. Contohnya seperti password untuk menentukan hak akses.
- Kontrol penyimpan: menyangkut berapa lama data disimpan dan jenis keamanan apa yang digunakan pada media penyimpan dan data yang disimpan. Contohnya sistem backup data yang dipakai dan enkripsi yang digunakan.
- Keamanan jaringan, baik jaringan intranet maupun internet: terkait dengan konfigurasi jaringan, hak akses jaringan, firewall, intrusion detection dan lainnya.
- Keamanan sistem: terkait dengan sistem operasi yang digunakan.

1.5. Kebijakan Keamanan Datacenter

Keamanan fisik dan keamanan virtualisasi dalam Data Center tidak terlepas dari kebijakan keamanan yang diterapkan di sebuah Data Center. Prosedur dan kebijakan yang diterapkan harus dapat berhasil dengan efektif, namun kebijakan dan prosedur yang diterapkan sangat terkait sumber daya manusia yang akan melakukan kebijakan. Secara umum kebijakan keamanan menyangkut pengaturan terhadap sistem, pengaturan terhadap hak akses dan pengguna, pengaturan pengoperasian, prosedur backup dan pengaturan penyimpanan, serta kebijakan yang terkait dengan kontrol akses fisik dan lainnya. Memberikan pelatihan kepada staf tentang pentingnya mematuhi dan menjalankan prosedur serta kebijakan yang berlaku merupakan sebuah cara yang dapat dilakukan agar kebijakan keamanan dapat mencapai tujuannya.

2. Keamanan Fisik Datacenter

Jika dahulu keamanan fisik dianggap tidak penting dan sering diabaikan, namun sekarang pandangan tersebut telah mulai berubah. Ada banyak kejadian yang membuat pandangan ini berubah. Sebagai contoh adanya penelitian dari computer forensics experts Pinkerton bahwa 70% data dicuri dari sebuah perusahaan adalah pencurian fisik, dari laptop dan harddisk ke CD atau peningkatan tinggi kapasistas penyimpanan mini menyebabkan kemudahan dalam pencurian data.

Selain itu juga bencana alam, membuat orang menjadi berubah pandangan akan pentingnya keamanan fisik. Bagaimana menjaga data agar tetap aman jika terjadi bencana

alam, bagaimana strategi pemulihan kembali setelah terjadi bencana adalah topik hangat yang diperbincangkan pada banyak artikel-artikel keamanan di internet.

Hal-hal tersebut di atas menjadi pertimbangan dalam pengamanan fisik Data Center. Keamanan fisik mulai diperhatikan, kebijakan keamanan yang terkait dengan keamanan fisik mulai dilihat ulang dan diperbaiki. Bagaimanan pengontrolan akses fisik, bagaimana standar ruangan server, bagaimana penyimpanan data, bagaimana prosedur backup, bagaimana standar keamanan gedung tempat Data Center dan lainnya, mulai mengimplementasikan aspek-aspek keamanan fisik. Untuk itu perlu mengetahui lebih lanjut mengenai risiko dan ancaman keamanan fisik serta metoda pengamanannya, sehingga dapat dilakukan tindakan pencegahan dan penanggulangan untuk bahaya keamanan fisik.

3.1 Ancaman dan risiko pada Datacenter

- Keamanan fisik dan faktor lingkungan

  Penerapan keamanan fisik harus memperhatikan faktor lingkungan dan menerapkan kontrol keamanan lingkungan. Dari hasil survei yang dilakukan, 70% manajer mengatakan risiko terbesar adalah bahaya lingkungan sebagai ancaman terbesar. Bahaya lingkungan ini berupa kebakaran, banjir, embun, suhu, listrik, gempa bumi dan bentuk-bentuk bencana alam lainnya yang memberikan pengaruh negatif untuk peralatan yang ada dalam Data Center. Namun banyak yang belum siap untuk mengatasi bahaya ini, karena menganggap bahwa bencana belum tentu akan terjadi.

- Keamanan fisik dan faktor manusia

  Manusia merupakan faktor penting dalam keamanan fisik. Eksploitasi keamanan komputer kebanyakan dilakukan oleh manusia. Jika menganggap bahwa sesorang yang tidak sah tidak mungkin masuk ke ruang server atau ruang penyimpanan data adalah sebuah hal yang salah. Hal ini dapat menjadi ancaman terbesar untuk Data Center. Namun demikian kita tidak hanya memperhatikan eksploitasi keamanan oleh orang dari luar, namun harus peduli pula dengan orang yang berasal dari dalam. Hal ini adalah ancaman terbesar karena orang berasal dari dalam dan lebih mengetahui dibandingkan penyusup dari luar.

- Keamanan fisik dan faktor finansial

  Perlu investasi yang cukup lumayan untuk mengimplementasikan keamanan fisik yang terintegrasi di sebuah Data Center. Namun terkadang karena alasan keuangan pengimplementasian tidak jadi dilakukan. Jika para manejer mengabaikan hal tersebut bisa jadi hal tersebut merupakan tindakan yang benar. Namun pandangan yang demikian adalah salah, pengimplementasian keamanan fisik harus diinvestasikan seefisien dan seefektif mungkin, karena jika terjadi sesuatu karena faktor lingkungan atau faktor manusia telah ada pencegahan dan penanggulangannya. Dengan penerapan keamanan fisik risiko kehilangan baik pada data ataupun perangkat keras menjadi lebih kecil, kerugian yang didapat tidak sebesar tanpa penerapan keamanan fisik. Jadi wajar saja jika diinvestasikan untuk keamanan fisik.

3. Metadata Kemanan Fisik Datacenter

   Dalam bagian sebelumnya telah membahas risiko dan ancaman keamanan fisik dari berbagai faktor. Selanjut akan dibahas mengenai metoda keamanan untuk mengatasi dan menanggulangi kerugian serta ancaman dari faktor lingkungan dan faktor manusia. Banyak cara dan metoda yang dapat digunakan mulai dari cara sederhana sampai menggunakan teknologi canggih, namun perlu diingatkan manusia adalah faktor penentu untuk keberhasilan keamanan di sebuah Data Center. Selain itu juga cara yang akan digunakan terkait dengan kebijakan yang akan diterapkan, jadi pada dasarnya penerapan keamanan fisik haruslah terintegrasi dan menyeluruh dengan keamanan informasi.

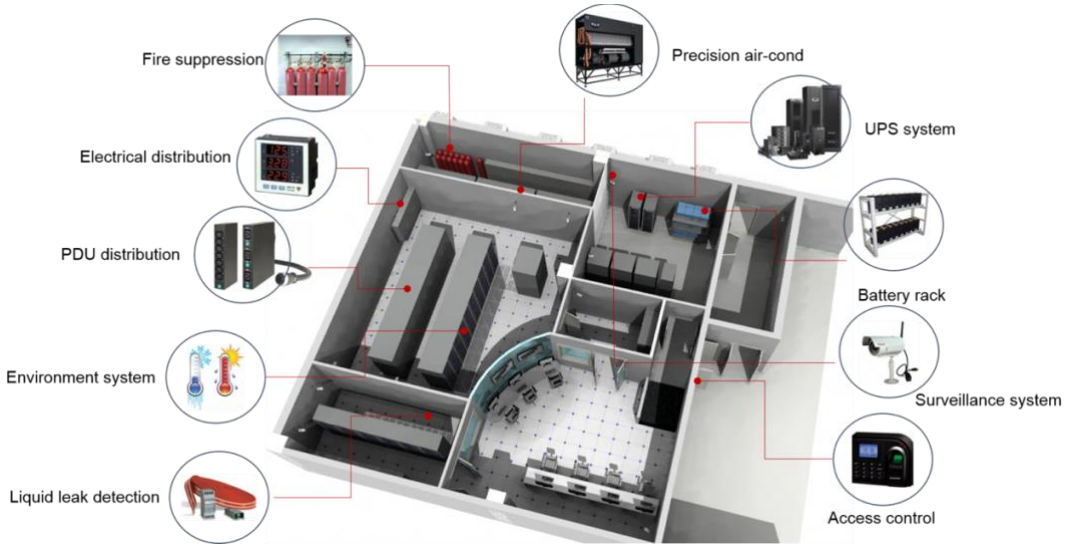
   3.1. Lokasi Datacenter

   Pemilihan lokasi bagunan mejadi hal yang harus diperhatikan. Kesadaran ini muncul sejak peristiwa 11 September, runtuhnya WTC membuat orang menjadi memperhatikan pemilihan lokasi yang tepat untuk Data Center. Hal-hal berikut dapat dijadikan bahan pertimbangan dari segi aspek keamanan dalam pemilihan lokasi. Lokasi yang dipilih sebaiknya yang memiliki sedikit risiko baik dari ancaman bencana alam (jalur gempa, daerah rawan banjir atau daerah rawan tornado) maupun dari ancaman teroris dan vandalisme. Data Center sebaiknya dibangun terpisah dari kantor pusat. Cukup jauh dari jalan raya utama. Tidak bertetangga dengan bandar

udara, pabrik kimia, jalur pipa gas, pusat keramaian (pasar, stadium olahraga) dan pusat pembangkit listrik. Dan juga lokasi memiliki fasilitas yang memadai, seperti kecukupan tenaga listrik.

3.2. Desain Kontruksi Datacenter

Setelah memilih lokasi yang baik selanjutnya kita harus memperhatikan bagunan yang akan didirikan untuk Data Center. Bangunan harus memperhatikan masalah sirkulasi udara karena hal ini terkait dengan suhu, ventilasi udara yang cukup, penggunaan AC yang direncanakan dengan baik. Karena biasanya bangunan Data Center dibuat dengan sedikit/bahkan tidak ada jendela dan tertutup. Bahan bangunan yang dipakai harus tidak mudah terbakar serta kontruksi bangunan yang tahan gempa. Adanya ruangan terpisah antara ruangan administratif dengan ruangan server dan data. Gunakan standar pendingin ruangan seperti TIA-942 dan perhatikan pengaturan kabel yang melalui bawah lantai. Menyiapkan kabel standar untuk instalasi listrik yang dibutuhkan dan konstruksi bangunan harus memperhatikan hal tersebut. Pintu masuk dirancang sangat terbatas. Pintu kebakaran dirancang untuk keluar saja. Segala aspek keamanan dalam bangunan sebuah Data Center harus direncanakan dengan baik. Kontruksi dan arsitektur bangunan harus dapat mengakomodasi semua hal berkaitan dengan keamanan fisik. Layout pada halaman berikut menggambarkan contoh ruangan yang ada dalam Data Center.



Gambar 3 : Layout Datacenter

3.3. Pengamanan Perimeter

Disekeliling bangunan Data Center seharusnya adalah bidang kosong, bangunan Data Center sebaiknya memiliki jarak ± 10 meter dengan bangunan lain atau tanaman dan pohon, hal ini dimaksudkan untuk memudahkan pengawasan. Dinding dan tembok yang ada disekitar Data Center harus dapat dimonitor dengan baik. Penggunaan kamera CCTV sebagai pengawas adalah hal minimal yang harus dilakukan. Selain itu juga kamera yang digunakan sebaiknya memiliki kemampuan terhadap cahaya rendah, tahan terhadap suhu dan cuaca. Selain itu juga penggunaan landscape setelah bidang kosong pada Data Center baik dilakukan, adanya pepohonan dan taman akan membuat Data Center tersembunyi dari orang yang lewat disekitar Data Center serta pengintai.

Pengawasan juga tidak terlepas dari areal parkir yang ada didekat Data Center. Pengawasan orang yang masuk dan keluar di kawasan Data Center harus dimonitor dengan baik. Penggunaan detektor bom perlu dilakukan untuk memeriksa setiap mobil yang masuk ke kawasan Data Center. Penggunaan penjaga atau petugas keamanan yang profesional merupakan sebuah hal yang harus dilakukan. Intinya jadikanlah bangunan Data Center sebagai sebuah benteng yang harus memiliki pengamanan baik diluarnya, agar orang yang tidak berkepentingan tidak mudah untuk masuk kedalam bangunan.

3.4. Pengamanan Indoor

Pengamanan didalam bangunan juga terkait dengan hal-hal lain seperti faktor manusia. Penggunaan kamera pengawas, sensor asap, sensor kebakaran merupakan hal standar yang harus diterapkan. Pengawasan terhadap pintu masuk dan keluar orang harus diperhatikan dengan baik. Pintu masuk yang menggunakan bahan dari baja serta penggunaan kaca dan dinding yang aman akan sulit dilalui. Namun penggunaan pendeteksi penyusup dapat pula diaplikasikan pada bangunan Data Center.

4. Faktor Suhu

Data Center sangat rentan terhadap temperatur yang tinggi. Oleh sebab itu penggunaan sensor suhu yang diletakkan di rack server menjadi sebuah solusi untuk mengendalikan suhu. Selain memperhatikan panas pada server, yang perlu diperhatikan adalah suhu ruangan. Untuk itu diperlukan sistem pendingin yang baik. Sejak mulai awal pembangunan Data Center hendaknya sudah diperhitungkan berapa kapasitas yang diperlukan untuk membuat ruangan tetap dingin, sehingga tidak kesulitan dalam menghitung listrik yang dibutuhkan. Meningkatnya suhu dapat diatasi dengan penambahan AC, namun akan dapat menimbulkan masalah karena membutuhkan listrik yang cukup besar.

Ada beberapa pendekatan yang dikembangkan untuk menghitung besarnya kebutuhan pendinginan. Pada dasarnya hal ini bergantung dari banyaknya jumlah peralatan yang ada didalam ruang komputer yang harus didinginkan. Cara sederhananya mungkin dengan melihat kapasitas ruangan yang dapat menampung berapa banyak rack server kemudian dari hal tersebut dapat diperkirakan berapa kebutuhan pendinginan yang diperlukan.

Sebuah teknologi baru yang dapat diterapkan untuk menyesuaikan kapasitas pendinginan dengan kebutuhan ruang komputer. Lantai terbaru meningkatkan ketepatan sistem pendingin yang secara otomatis menyesuaikan kapasitas dengan kebutuhan ruangan tanpa memutar kompresor dan meningkatkan efisiensi dan realibilitas. Hal ini memungkinkan peningkatan kapasitas ekstra dalam sistem tanpa peningkatan dalam biaya energi. Keuntungan menggunakan pre-piping adalah kemudahan untuk menambahkan atau memindahkan model pendingin, selain itu juga realibilitas akan dapat tercapai.

5. Faktor *Fire Safety*

   Bahaya kebakaran sangat mungkin terjadi di Data Center. Kumpulan peralatan elektronik yang ada berpotensi untuk menyebabkan kebakaran. Suplai tenaga yang baik harus diperhatikan, bangunan yang tidak mudah terbakar, penggunaan sensor asap, sensor panas, pemadam api dan sistem penyemprot air merupakan hal-hal yang harus dilakukan untuk mengurangi dan menanggulangi bahaya kebakaran. Pemasangan detektor dan sensor baik pada rungan komputer maupun di luar ruangan. Penggunaan alarm kebakaran dapat dilakukan baik secara manual maupun otomatis. Selain itu juga gunakan pemadam api yang sesuai dengan jenis kebakaran yang terjadi. Ada dua jenis pemadam api yaitu pemadam kimia kering dan pemadam

dari gas halon. Serta perhatikan juga efek yang dapat ditimbulkan dari penggunaan pemadam api.

Berikut ini langkah-langkah yang ditulis oleh Lance D. Harry seorang manejer pengembang bisnis di Fenwal Protection System, yang dapat dilakukan untuk perencanaan kebakaran.

a. Proteksi = deteksi + supresi

   Idealnya proteksi yang dilakukan yaitu dengan menerapkan deteksi asap dan sistem suppresi kebakaran. Suppresi kebakaran dapat dilakukan dengan pemasangan detektor asap dan sensor udara pada langit-langit. Dan lengkapi dengan sistem penyemprotan baik skala kecil maupun besar seperti gas Inergen.

b. Memahami secara keseluruhan strategi FP perusahaan.
c. Dapatkan ahli yang terpercaya untuk memberikan saran penanggulangan bahaya kebakaran.
d. Pahami kebutuhan lokal
e. Selain menerapkan standar tapi juga melihat kebutuhan perusahaan.
f. Lakukan penilaian risiko yang mencakup analisis TCO dalam fasilitas.
g. Lakukan perawatan sistem supaya dapat bertahan lama.
h. Didik dan latih pekerja.

Diharapkan dengan pendidikan dan latihan pekerja dapat memahami bahaya kebakaran dan peduli untuk mencegah terhadap kemungkinan timbulnya bahaya.

6. Faktor Tenaga Listrik

Kebutuhan listrik merupakan hal yang penting pada sebuah Data Center. Karena semua peralatan komputer, peralatan komunikasi dan jaringan serta pendingin membutuhkan energi. Selain itu juga penggunaan listrik cadangan seperti Genset dan UPS harus dilakukan. UPS yang digunakan harus memenuhi kebutuhan listrik dari semua peralatan yang ada. Batere UPS diharapkan dapat bertahan cukup lama sebelum digantikan dengan listrik cadangan dari Genset. Banyak metoda yang dapat diterapkan untuk menghitung kebutuhan tenaga pada Data Center. Berikut ini contoh penghitungan tenaga listrik yang dibutuhkan.

Data	Value	Units	Comment
Total IT racks available	28	#	Some of the space in the data center is consumed by power and cooling equipment
Total initial power requirement	47	kW	At least 47 kW of power and cooling equipment must be installed initially. Using Figure 1, based the density of Row 1, 2 and 3, the number of IT racks spaces available is 6, 4, and 5 respectively (6 x 2 kW / rack + 4 x 5 kW / rack + 5 x 3 kW / rack = 47 kW)
Total final power requirement	104	kW	The remainder of the power and cooling equipment, as much as 60 kW, is deferred until the remaining rows are determined (28 IT racks x 3.7 kW / rack = 104 kW)
Peak power density	15	kW / rack	Cooling at this high density narrows the options available and increases the cost. A further attempt to spread these peak loads should be considered before committing the design at this density
Average data center power density	3.7	kW / rack	This data center, as specified, is more than twice the density of the average existing data center. Less than 2% of data centers today achieve this density

Gambar 4 : Tabel Kebutuhan Listrik Datacenter

Sekarang ini telah timbul semacam pandangan untuk mengurangi konsumsi energi pada sebuah Data Center, misalnya penggunaan teknologi pendingin terbaru, penggunaan energi lain seperti matahari atau hidrogen. Teknologi untuk hal ini masih terus dikembangkan seiring dengan kesadaran para manajer untuk lebih mengefisiensikan konsumsi energi di sebuah Data Center.

7. Faktor *Disaster Recovery*

Bencana alam memang tak dapat dihindari, namun kita dapat mengantisipasi untuk mengurangi risiko yang disebabkan oleh bencana alam. Pada awal telah disebutkan bangunan Data Center harus jauh dari daerah yang sering dilanda bencana alam seperti gempa bumi, gunung meletus, banjir, tornado dan sebagainya. Kontruksi bangunan yang memiliki ketahanan terhadap gempa adalah suatu cara yang dapat diterapkan. Selain itu juga rak server ditempatkan pada platform isolasi seismic sehingga risiko kerusakan jika terjadi gempa berskala kecil dapat dikurangi.

Namun demikian bencana alam bukan itu saja, untuk itu pentingnya penerapan backup yang kontinu pada sebuah Data Center dan tempat penyimpanan data hasil backup harus terpisah dari Data Center dan disimpan pada tempat yang aman pula. Antisipasi terhadap bencana alam, kebakaran atau kerusakan pada Data Center hanya dengan cara backup data. Teknologi backup

data yang digunakan terkait erat dengan keamanan data secara virtual. Oleh sebab itu konvergensi keamanan fisik dan virtual pada keamanan Data Center merupakan hal yang tidak dapat ditawar. Backup dapat dilakukan langsung di Data Center menggunakan media backup seperti tape, cd, dvd atau alainnya. Namun dapat pula dilakukan secara virtual melalui jaringan. Backup yang dilakukan ini disebut dengan istilah remote replication jadi backup dilakukan dari hard disk ke hard disk. Karena dilakukan melalui jaringan diperlukan bandwidth yang cukup untuk melakukan hal ini dan aspek keamanan virtual harus lebih diperhatikan. Penyimpanan terhadap data hasil backup perlu diperhatikan. Gudang penyimpanan harus aman dari penyusup dan ruangan penyimpan harus baik, bebas debu, tidak lembab dan tidak mudah terbakar agar data tetap terjaga.

Backup yang dilakukan merupakan salah satu cara dalam perencanaan pemulihan bencana atau lebih dikenal dengan disaster recovery planning (DR planing). Dengan adanya perencanaan ini dimaksudkan setelah becana selesai dapat terus melanjutkan operasi bisnis. Data yang telah dibackup akan direstore sehingga bisnis dapat terus berlanjut.

Berikut ini cek list yang ditulis oleh Denis C. Brewer di newsletter searchdatacenter.com mengenai DR planning.

- Rule 0

  Identifikasi semua proses bisnis kritikal dan aplikasi-aplikasi, bersama dengan perangkat keras, perangkat lunak, bisnis, dukungan staf TI yang menjalankan, dan LAN serta WAN yang mengkoneksikan mereka ke pengguna akhir. Kelanjutan bisnis dan rencana pemulihan TI harus memasukkan semua tindakan dalam setiap elemen yang diidentifikasi.

- Rule 1

  Setiap harinya buat replika (dalam disk atau tape) dari "digital trio", yaitu:

  - Sistem operasi tempat aplikasi berjalan dan patch level saat itu yang ditampilkan pada lingkungan produksi.
  - Aplikasi kritis yang berjalan pada system operasi pada patch saat ini.
  - Data.

  Jangan ada istilah "no data loss." Bit-by-bit backup data adalah berharga.

- Rule 2

Miliki "carbon copy" dari perangkat keras yang dibutuhkan untuk menjalankan tiruan digital. Penggunaan media backup terbaik adalah nilai kecil, jika tidak memiliki perangkat keras yang tepat ketika dan dimana data diperlukan dengan cepat untuk merestore digital trio ke peralatan baru atau yang siap.

- Rule 3

  Tulis langkah demi langkah untuk merestore tiruan digital ke carbon copy perangkat keras.

- Rule 4

  Selalu lakukan percobaan. Baik tiruan digital, perangkat keras dan dokumentasinya.

- Rule 5

  Capai praktek maksimum atau pemisahan yang mampu antar lokasi yang digunakan untuk operasi harian dan tempat penyimpanan tiruan, pemulihan perangkat keras dan dokumentasi. Lokasi backup pada kota yang sama hendaknya dihindari. Perhatikan batasan dari metoda komunikasi yang didukung oleh strategi jalur backup.

- Rule 6

  Respon dengan segera untuk kondisi yang berisiko tinggi. Badai Katrina memberikan pelajaran ketika kota tidak dapat berfungsi. Latihan teknis dan peroses bisnis untuk staf pada lokasi kerja alternatif.

- Rule 7

  Miliki dan sedikitnya identifikasi, koneksi alternatif, rute transmisi data dan sumber tenaga listrik. Bergantung di mana lokasi bisnis, alternatif rute dan sumber mungkin terbatas. Pelajari pilihan yang pada lokasi. Jika kantor cabang terhubung dengan kabel, putuskan investasi lain seperti penggunaan jalur satelit.

- Rule 8

  Aplikasikan konsep "Fort Knox", terapkan keamanan fisik lebih dari satu pada tempat penyimpanan tiruan.

- Rule 9

  Dokuentasi dan latihan perencanan bisnis keseluruhan. Uji coba dan recanakan dan jawab pertanyaan: Apakah proses bisnis operasi staf efisien setelah kejadian kurang baik.

- Rule 10

  Miliki dan operasikan alternative pengganti tenaga. Pertimbangkan tenaga generator listrik multi-fuel.

- Rule 11

  Tetapkan dan uji secara kontinu pada kondisi karantina.

- Rule 12

  Aplikasikan sumber daya yang diperoleh dan dirawat dari aturan 0-11 melalui daur hidup dalam aplikasi kritis.

Selain cek list diatas juga diperlukan strategi untuk menjalankan DR planning yang menyangkut hal- hal berikut: penilaian dampak bisnis, penemuan, anggaran, aturan dasar tim, proteksi data, logistik dan semiannual tes.

8. Faktor *Human Error*

Keberhasilan keamanan sangat bergantung pada faktor manusia, yang juga menjadi target utama dari eksploitasi keamanan. Selain metode yang sudah disebutkan sebelumnya, mengatasi faktor manusia memerlukan metode dan teknik khusus. Salah satu cara umum untuk mengatasi ini adalah dengan menerapkan teknologi biometrik, seperti yang telah dibahas sebelumnya dalam konteks keamanan fisik. Penerapan teknologi biometrik di sebuah Pusat Data bertujuan untuk menjamin privasi, integritas, autentikasi, dan ketersediaan. Namun, keberhasilan penerapan teknologi biometrik juga memerlukan dukungan dari staf serta kebijakan keamanan yang kuat. Staf perlu dilatih dan disadarkan akan pentingnya keamanan untuk mengurangi potensi ancaman.

Keamanan di Pusat Data harus mencakup aspek fisik dan virtual. Salah satu strategi adalah dengan membagi Pusat Data ke dalam beberapa zona keamanan untuk membatasi akses ke ruang komputer dan peralatan vital lainnya, seperti pusat pembangkit dan pendingin. Setiap zona memerlukan kebijakan keamanan yang berbeda, menggunakan peralatan seperti kamera pengawas, teknologi biometrik, dan kata sandi untuk pengamanan fisik. Detektor penyusup juga dapat diterapkan di sini.

- Zona 1: Wilayah sekeliling bangunan Pusat Data

Penggunaan kamera pengawas dan penjaga sangat diperlukan di sini, seperti yang sudah dijelaskan pada bagian pengamanan di sekitar bangunan.

- Zona 2: Wilayah di dalam bangunan Pusat Data

  Pengamanan dalam gedung dapat dibagi menjadi beberapa level:

  - Level pertama: Akses ke gedung memerlukan kode akses tertentu, yang bisa dilakukan melalui perangkat keras untuk memasukkan kata sandi, baik secara manual maupun menggunakan smart card.
  - Level kedua: Akses ke ruang administrasi menggunakan biometrik. Staf harus melewati pemindai biometrik seperti handprint, fingerprint, atau iris scan untuk mendapatkan hak akses. Penggunaan voiceprint dan identifikasi kulit mungkin akan diterapkan di masa mendatang. Data biometrik yang ada juga harus dienkripsi untuk mencegah penyalahgunaan.
  - Level ketiga: Akses ke ruang server memerlukan kombinasi kata sandi, card reader, dan biometrik untuk memastikan hanya orang yang berwenang yang dapat masuk. Pemantauan 24/7 diperlukan di seluruh area gedung, termasuk pintu keluar dan ruang komputer. Pengawasan harus tetap dilakukan meskipun ada kepercayaan terhadap pengguna internal.

Penggunaan teknologi lain yang mendukung keamanan juga layak dipertimbangkan. Penerapan kebijakan keamanan yang tepat menjadi sangat penting dalam menjaga integritas dan keamanan Datacenter.

BAB VII : Infrastruktur *Local Area Network* (LAN) Kampus

1. Layanan-Layanan yang dibutuhkan Jaringan Kampus
   a. Security/Keamanan

      Keamanan merupakan hal yang sangat penting bagi semua layanan jaringan LAN kampus. Akses terhadap jaringan dan aplikasi harus terbuka tetapi juga harus tetap aman dan terkontrol. Jaringan saat ini tidak hanya perlu mangatasi secara efektif terhadap perangkat-perangkat dan user tidak dapat diatur yang mencoba mengakses jaringan kampus, tetapi juga perlu memberikan dukungan terhadap perangkat-perangkat unmanaged, kontrol terhadap post admisi, kontrol terhadap akses aplikasi, visibilitas dan monitoring. Komponen-komponen kunci keamanan dan kebijakan-kebijakan adalah sebagai berikut:

      - Layanan mendeteksi dan manajemen ancaman yang bersifat adaptif
      - Kebijakan keamanan yang mendukung DMZ
      - Kebijakan yang memberikan kepastian atas kualitas layanan (QoS)
      - Meringankan dari serangan-serangan dan ancaman-ancaman Denial of Service (DoS) dan Distributed DoS
      - Memastikan organisasi memenuhi kriteria compliance

   b. Koneksi LAN

      Infrastruktur kampus harus menyediakan konektivitas LAN yang aman baik secara kabel maupun nirkable sejalan adanya peningkatan jumlah perangkat IP, seperti computer, smartphone, smart tablet, kamera survilance, dan lain-lain.

   c. Koneksi WAN

      Kampus seharusnya secara aman dan handal terhubung ke Datacenter terhadap sentralisasi data seperti data-data layanan dan replikasi, dan sebagai tambahan terkoneksi ke cabang-cabang untuk melakukan kolaborasi komunikasi yang menyatu.

   d. Akses Internet

Kampus seharusnya secara aman dan handal terhubung ke Datacenter terhadap sentralisasi data seperti data-data layanan dan replikasi, dan sebagai tambahan terkoneksi ke cabang-cabang untuk melakukan kolaborasi komunikasi yang menyatu.

e. Layanan *Remote Access*

Pertumbuhan populasi remote user, jam operasi, berbagai perangkat endpoint, dan jumlah aplikasi yang diakses menunjukan adany tuntutan baru terhadap akses jarak jauh ke sumber daya LAN. layanan akses remote (RAS) yang diperlukan agar user di cabang atau karyawan yang bepergian, mitra, konsultan, dan pelanggan dapat mengakses dan memproses informasi terpusat seolah-olah mereka berada di kantor. solusi RAS juga harus memastikan bahwa pengguna hanya dapat mengakses informasi yang tepat berdasarkan siapa mereka, apa perangkat yang mereka gunakan, dan jenis jaringan di mana mereka mengakses data.

Solusi RAS harus mudah digunakan untuk mengatasi berbagai pengguna dan berbagai tingkat keahlian mereka. Dalam rangka untuk memastikan produktivitas yang optimal dan pengalaman seolah-olah berada di-kantor bagi pengguna jarak jauh, solusi harus memberikan kinerja terbaik di kelasnya. TI harus mempertahankan kontrol untuk memastikan praktek mapan compliance. Ini juga diperlukan untuk memastikan kebijakan keamanan yang komprehensif yang membahas meningkatnya jumlah dan kecanggihan potensi ancaman dan serangan, karena lebih banyak pengguna mendapatkan akses ke sumber daya kampus. Solusi-solusi minim solusi perawatan RAS dengan klien lebih ringan dan kemudahan akses membantu mengurangi biaya dukungan.

f. High Performance

Jaringan LAN sama seperti performa aplikasi harus tersedia dan dapat diakses setiap saat di seluruh jaringan kampus, sama seperti solusi-solusi akses remote (RAS), kecepatan jaringan LAN juga harus termaintain melalui jaringan WAN ketika user mengakses aplikasi-aplikasi ataupun sumber informasi terpusat.

g. High Availibilty

Terputusnya koneksi jaringan kampus akhir-akhir ini bukan merupakan sebuah pilihan dalam jaringan kampus LAN, tingkat ketersediaan layanan yang harus dicapai adalalah

99,999% dengan tujuan mendekati layanan yang harus disediakan oleh jaringan telepon umum (PSTN). Konsep High Avalibility harus dimasukan pada saat merancang jaringan LAN. Perangkat-perangkat jaringan dan software yang cost-effective, kaya fitur, tangguh dan memberikan kemampuan manajemen terpusat merupakan hal yang sangat penting dalam mengurangi potensi downtime dan biaya operasional.

h. Centered Management

Yang merupakan kunci yang diperlukan dalam jaringan LAN Kampus adalah manajemen terpusat terhadap semua perangkat jaringan switch, firewall, router dan VPN dan perangkat Intrusion Prenvention Sistem (IPS). Solusi Manajemen terpusat mengurangi waktu dan biaya yang diperlukan untuk menkonfigur dan memanage perangkat- perangkat jaringan. Sebagai tambahan lalulintas jaringan dapat lebih mudah dianalisa dengan sistem tersebut, memfasilitasi optimalisasi performa jaringan.

2. Solusi Infrastruktur

Solusi infrastruktur data center untuk skala kecil dan menengah memerlukan perencanaan yang matang dan pemilihan teknologi yang sesuai dengan kebutuhan dan anggaran. Berikut adalah beberapa komponen kunci dan solusi yang dapat diterapkan untuk membangun data center skala kecil dan menengah:

a) Lokasi dan Lingkungan Fisik

Pemilihan Lokasi: Pilih lokasi yang aman dari bencana alam seperti banjir, gempa bumi, atau kebakaran.

Kondisi Lingkungan: Pastikan ruangan memiliki ventilasi yang baik dan suhu yang terkontrol. Penggunaan AC khusus untuk data center (precision air conditioning) sangat dianjurkan.

b) Ruang dan Tata Letak

Rack dan Cabinet: Gunakan rack dan cabinet standar untuk menempatkan server dan perangkat jaringan. Pastikan tata letak memudahkan sirkulasi udara.

Kabel dan Manajemen Kabel: Rencanakan penataan kabel dengan rapi menggunakan manajemen kabel untuk mencegah kekacauan dan mempermudah perawatan.

c) Perangkat Keras (Hardware)

Server: Gunakan server rack-mount atau blade server yang hemat ruang dan mudah untuk diintegrasikan.

Untuk skala kecil, pertimbangkan penggunaan server tower yang lebih ekonomis. Untuk skala menengah, server rack-mount atau blade server lebih disarankan untuk menghemat ruang dan memberikan kinerja yang lebih baik.

Storage: Pilih solusi storage yang sesuai, seperti NAS (Network Attached Storage) atau SAN (Storage Area Network) untuk kebutuhan penyimpanan data.

Jaringan: Gunakan switch gigabit atau 10-gigabit untuk jaringan internal yang cepat. Pertimbangkan penggunaan firewall hardware untuk keamanan.

d) Power Supply dan Cooling

UPS (Uninterruptible Power Supply): Gunakan UPS untuk menyediakan daya cadangan dan melindungi perangkat dari lonjakan Listrik.

Redundansi Daya: Pertimbangkan memiliki sumber daya listrik cadangan (genset) untuk menjaga data center tetap beroperasi saat terjadi pemadaman listrik.

Cooling System: Gunakan precision cooling systems untuk menjaga suhu optimal di dalam data center. Implementasikan sistem pendinginan seperti CRAC (Computer Room Air Conditioning) units atau in-row cooling.

e) Keamanan Fisik

Kontrol Akses: Gunakan sistem kontrol akses yang ketat seperti kunci biometrik atau kartu akses untuk membatasi siapa yang dapat memasuki data center.

Pengawasan: Pasang kamera pengawas (CCTV) dan sistem deteksi penyusup untuk memantau keamanan data center.

f) Manajemen dan Monitoring

DCIM (Data Center Infrastructure Management): Implementasikan software DCIM untuk memantau dan mengelola infrastruktur data center secara efisien.

Pemantauan Jarak Jauh: Gunakan tools monitoring seperti Nagios atau Zabbix untuk pemantauan jarak jauh, yang memungkinkan tim IT untuk memantau kinerja dan kesehatan perangkat dari mana saja.

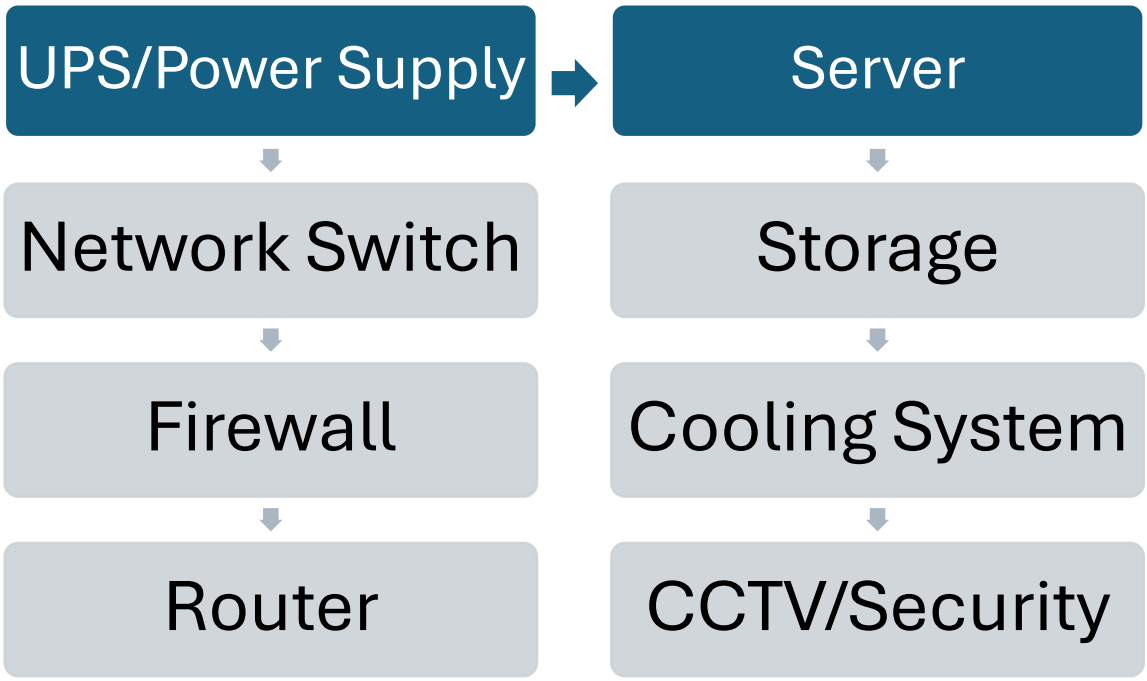
g) Redundansi dan Disaster Recovery

Backup Data: Lakukan backup data secara teratur menggunakan solusi backup yang andal. Pertimbangkan untuk menggunakan cloud backup sebagai cadangan tambahan. Disaster Recovery Plan: Buat dan uji rencana pemulihan bencana untuk memastikan kelangsungan bisnis dalam situasi darurat.

h) Virtualisasi

Virtualisasi Server: Gunakan teknologi virtualisasi seperti VMware, Hyper-V, atau Proxmox untuk meningkatkan efisiensi dan fleksibilitas penggunaan server fisik.

Manajemen Virtualisasi: Gunakan perangkat lunak manajemen virtualisasi untuk mengelola dan mengoptimalkan penggunaan sumber daya.



Gambar 7.1 : Desain Interkoneksi Server Small-Mid Level Enterprise

3. Implementasi Arsitektur Berskala Midsize Enterprise

a. Tujuan

Membangun arsitektur kampus midsize enterprise memiliki berbagai tujuan strategis yang penting untuk mendukung operasional, pendidikan, dan pengelolaan kampus secara keseluruhan. Berikut adalah tujuan-tujuan utama dari arsitektur ini:

1) Meningkatkan Konektivitas dan Jaringan Kampus

   Konektivitas Cepat dan Andal: Menyediakan jaringan dengan kecepatan tinggi dan keandalan tinggi untuk mendukung aktivitas akademik, administratif, dan operasional.

   Akses Tanpa Batas: Menyediakan akses jaringan yang konsisten dan tanpa batas di seluruh area kampus, termasuk di dalam ruangan kelas, laboratorium, kantor, dan area publik.

2) Memfasilitasi Pembelajaran dan Pengajaran

   Dukungan Teknologi Pembelajaran: Mengintegrasikan Learning Management Systems (LMS) dan alat kolaborasi untuk meningkatkan pengalaman belajar mengajar.

   Akses Sumber Daya Akademik: Memastikan bahwa mahasiswa dan staf memiliki akses mudah ke sumber daya akademik seperti perpustakaan digital, database penelitian, dan materi kursus.

3) Meningkatkan Efisiensi Operasional

   Otomatisasi Proses: Mengotomatisasi proses administratif seperti pendaftaran, penjadwalan kelas, manajemen keuangan, dan pelaporan untuk mengurangi beban kerja manual.

   Pengelolaan Data Terpusat: Mengelola data secara terpusat untuk memudahkan akses dan analisis, serta meningkatkan akurasi dan integritas data.

4) Keamanan dan Keandalan

   Keamanan Jaringan: Implementasi firewall, sistem deteksi intrusi, dan protokol keamanan lainnya untuk melindungi data dan infrastruktur dari ancaman eksternal dan internal.

   Keandalan Sistem: Memastikan infrastruktur memiliki redundansi dan rencana pemulihan bencana (Disaster Recovery Plan) untuk menjaga kelangsungan operasional dalam situasi darurat.

5) Skalabilitas dan Fleksibilitas

Skalabilitas Infrastruktur: Merancang jaringan dan data center yang dapat dengan mudah ditingkatkan sesuai dengan pertumbuhan jumlah pengguna dan kebutuhan teknologi.

Fleksibilitas Penggunaan: Menyediakan solusi yang fleksibel yang dapat disesuaikan dengan perubahan kebutuhan akademik dan teknologi masa depan.

6) Pengelolaan Sumber Daya yang Efisien

Efisiensi Energi: Menggunakan teknologi yang hemat energi dan solusi manajemen daya untuk mengurangi konsumsi energi dan biaya operasional.

najemen Infrastruktur: Menggunakan alat manajemen infrastruktur (seperti DCIM) untuk memantau, mengelola, dan mengoptimalkan penggunaan sumber daya IT.

7) Mendukung Inovasi dan Penelitian

Infrastruktur Penelitian: Menyediakan infrastruktur teknologi yang kuat untuk mendukung aktivitas penelitian, termasuk akses ke server berkapasitas tinggi dan storage yang luas.

Kolaborasi Riset: Fasilitasi kolaborasi antar peneliti baik di dalam kampus maupun dengan institusi lain melalui jaringan yang aman dan andal.

8) Pengalaman Pengguna yang Lebih Baik

User Experience: Meningkatkan pengalaman pengguna bagi mahasiswa, dosen, dan staf dengan menyediakan akses yang mudah dan cepat ke aplikasi dan layanan kampus.

Layanan Support: Menyediakan layanan dukungan IT yang responsif untuk membantu pengguna dalam mengatasi masalah teknis.

b. Penerapan Tujuan dalam Arsitektur Kampus

Untuk mencapai tujuan-tujuan tersebut, arsitektur kampus midsize enterprise harus dirancang dengan komponen-komponen berikut:

- Core Network: Backbone jaringan dengan kapasitas tinggi untuk konektivitas andal.

- Data Center: Server, storage, dan sistem virtualisasi untuk mengelola aplikasi kampus dan data.
- Security Systems: Firewall, IDPS, dan kontrol akses untuk melindungi infrastruktur.
- Wireless Infrastructure: Access points yang mendukung jaringan nirkabel di seluruh area kampus.
- Management Tools: Alat-alat untuk pemantauan dan manajemen infrastruktur secara efisien.
- Disaster Recovery Solutions: Rencana pemulihan bencana untuk menjaga kelangsungan operasional.
- Support Systems: Layanan dukungan IT untuk membantu pengguna dan memastikan operasional yang lancar.

Dengan merancang dan mengimplementasikan arsitektur yang memenuhi tujuan-tujuan ini, kampus midsize enterprise dapat memastikan bahwa mereka memiliki infrastruktur teknologi yang mampu mendukung semua aspek operasional, akademik, dan administratif dengan efisiensi dan efektivitas yang tinggi.

c. Tahapan Impelementasi

Arsitektur untuk kampus berskala midsize enterprise yang mencakup berbagai komponen infrastruktur teknologi informasi yang dapat digunakan untuk mendukung operasional dan manajemen kampus secara efisien dan efektif.

1) Jaringan dan Infrastruktur

Core Network: Backbone jaringan yang menghubungkan seluruh bagian kampus. Ini termasuk switch dan router dengan kapasitas tinggi untuk memastikan konektivitas yang andal dan cepat.

Distribution Layer: Menghubungkan core network dengan access layer. Pada lapisan ini, switch distribution mengelola lalu lintas data antara core dan access layer.

Access Layer: Menyediakan akses langsung bagi pengguna di kampus, termasuk dosen, staf, dan mahasiswa. Ini termasuk switch dan access points (AP) untuk jaringan nirkabel.

2) Data Center

Server Farm: Cluster server yang mengelola aplikasi kampus, database, web services, dan sistem informasi akademik.

Storage Solutions: Solusi penyimpanan terpusat seperti NAS (Network Attached Storage) atau SAN (Storage Area Network) untuk penyimpanan data yang efisien dan aman.

Virtualization: Penggunaan teknologi virtualisasi (misalnya, VMware, Hyper-V) untuk meningkatkan penggunaan sumber daya dan fleksibilitas pengelolaan server.

3) Sistem Keamanan

Firewall: Perangkat untuk mengamankan jaringan kampus dari ancaman eksternal.

Intrusion Detection and Prevention Systems (IDPS): Sistem untuk mendeteksi dan mencegah ancaman keamanan jaringan.

Access Control: Sistem kontrol akses untuk memastikan hanya orang yang berwenang yang dapat mengakses fasilitas tertentu, termasuk penggunaan biometrik untuk keamanan fisik.

4) Sistem Manajemen

Network Management Systems (NMS): Solusi untuk memantau, mengelola, dan mengoptimalkan performa jaringan.

Data Center Infrastructure Management (DCIM): Alat untuk memantau dan mengelola infrastruktur fisik dan IT dalam data center.

5) Komponen Khusus Pendidikan

Learning Management System (LMS): Platform untuk manajemen pembelajaran, distribusi materi, dan komunikasi antara dosen dan mahasiswa.

Academic Information System (AIS): Sistem untuk mengelola informasi akademik, pendaftaran, nilai, dan administrasi mahasiswa, biasa dikenal dengan istilah SIAKAD atau Sistem Informasi Akademik.

Collaboration Tools: Alat kolaborasi seperti email kampus, platform komunikasi (misalnya, Microsoft Teams, Zoom), dan forum diskusi online.

6) Keamanan Fisik dan Manajemen Energi

Biometric Access Control: Penggunaan sidik jari, pengenalan wajah, atau identifikasi iris untuk mengakses area sensitif.

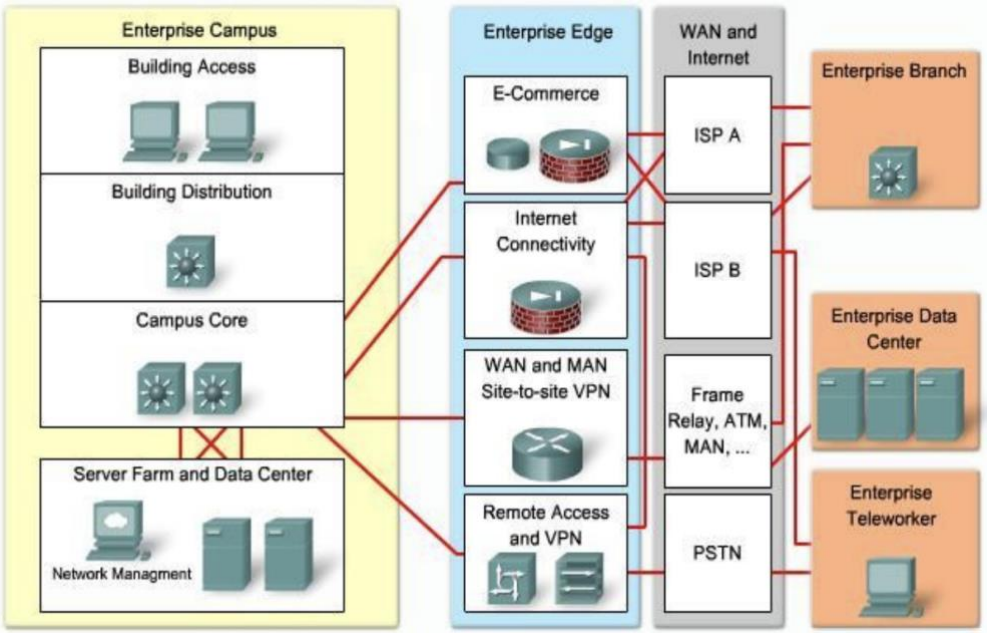
Uninterruptible Power Supply (UPS): Menyediakan cadangan daya untuk perangkat kritis di data center.

Precision Air Conditioning (PAC): Sistem pendingin untuk menjaga suhu optimal di data center.

7) Layanan Tambahan

Cloud Services: Integrasi dengan layanan cloud untuk backup, penyimpanan tambahan, atau pemrosesan data.

Disaster Recovery Plan: Rencana pemulihan bencana untuk memastikan kelangsungan operasional kampus dalam keadaan darurat.



Gambar 7.2 : Desain Interkoneksi Midsize Enterprise

Arsitektur kampus midsize enterprise dirancang untuk menyediakan konektivitas cepat dan andal, mendukung pembelajaran dan penelitian, meningkatkan efisiensi operasional, serta memastikan keamanan data dan infrastruktur. Solusi ini melibatkan core network, data center

dengan server dan storage yang efisien, sistem keamanan yang kuat (firewall, IDPS, dan kontrol akses biometrik), serta alat manajemen infrastruktur yang canggih. Tujuannya mencakup otomatisasi proses administratif, pengelolaan data terpusat, skalabilitas, pengelolaan sumber daya yang efisien, serta pengalaman pengguna yang lebih baik, mendukung kegiatan akademik dan operasional kampus secara keseluruhan.

BAB VIII : Desain Jaringan Wireless Kampus

1. Latar Belakang dan Tantangan

   Didorong oleh peningkatan mobilitas, BYOD, Aplikasi bisnis kritikal, dan harapan-harapan setiap user akan adanya jangkauan koneksi wireless di mana-mana. Kampus berlomba-lomba untuk mengejar kebutuhan performa koneksi untuk menjaga jaringan-jaringan tetap sederhana, fleksibel dan efisien. Menjadikanny mudah untuk diimplementasikan, dimanage dan, skalabilitas.

   Pengadopsian perangkat-perangkat pintar seperti smartphone, tablet, laptop menciptakan dua tantangan bagi tim IT yaitu: akses jaringan dan perangkat sekuriti. Setiap kategori merupakan sesuatu yang unik dan memerlukan seperangkat keahlian dan panduan yang berbeda.

   Koneksi wireless saat ini merupakan hal akses utama bagi setiap user yang menjalan aplikasi bisnis misi kritikal. Setiap pengguna dengan berbagai perangkat mobile mengharapkan akses jaringan yang mudah dan aman di manapun dan kapanpun. Mereka memerlukan jaringan bekerja untuk mereka secara sederhana dan handal. Setiap user menginginkan kualitas pengalaman yang sama tingginya tanpa melihat perangkat yang mereka gunkan, aplikasi yang mereka gunakan atau dimanapun mereka terhubung ke jaringan.

2. Manajemen User Jaringan Wireless Kampus

   Manajemen user pada jaringan WiFi kampus adalah aspek penting untuk memastikan konektivitas yang aman, efisien, dan andal bagi seluruh pengguna, termasuk mahasiswa, dosen, dan staf administratif. Berikut adalah langkah-langkah dan praktik terbaik untuk manajemen user jaringan WiFi kampus:

   a. Autentikasi dan Autorisasi Pengguna

      Portal Captive: Menggunakan captive portal untuk mengautentikasi pengguna ketika mereka pertama kali terhubung ke jaringan WiFi. Pengguna harus memasukkan kredensial yang valid (misalnya, username dan password) yang telah diberikan oleh administrasi kampus.

b. Kontrol Akses Berbasis Peran (Role-Based Access Control - RBAC)

Kategori Pengguna: Membagi pengguna ke dalam berbagai kategori seperti mahasiswa, dosen, staf administratif, tamu, dan lain-lain.

Hak Akses: Menetapkan hak akses jaringan yang berbeda berdasarkan peran pengguna. Misalnya, dosen dan staf mungkin mendapatkan akses lebih luas ke sumber daya internal dibandingkan dengan mahasiswa atau tamu.

c. Pengelolaan Bandwidth dan Kualitas Layanan (QoS)

Pengelolaan Bandwidth: Membatasi penggunaan bandwidth per pengguna atau per kategori pengguna untuk mencegah beberapa pengguna mengonsumsi sebagian besar sumber daya jaringan.

Prioritasi Layanan: Menggunakan QoS untuk memastikan aplikasi yang penting seperti sistem informasi akademik atau platform pembelajaran online mendapatkan prioritas tertinggi dalam jaringan.

d. Keamanan Jaringan

Enkripsi: Menggunakan protokol keamanan seperti WPA2 untuk mengenkripsi lalu lintas WiFi, melindungi data pengguna dari penyadapan.

Pendeteksian dan Pencegahan Intrusi: Mengimplementasikan sistem pendeteksian dan pencegahan intrusi (IDPS) untuk mendeteksi aktivitas mencurigakan dan mencegah akses tidak sah ke jaringan.

e. Monitoring dan Logging

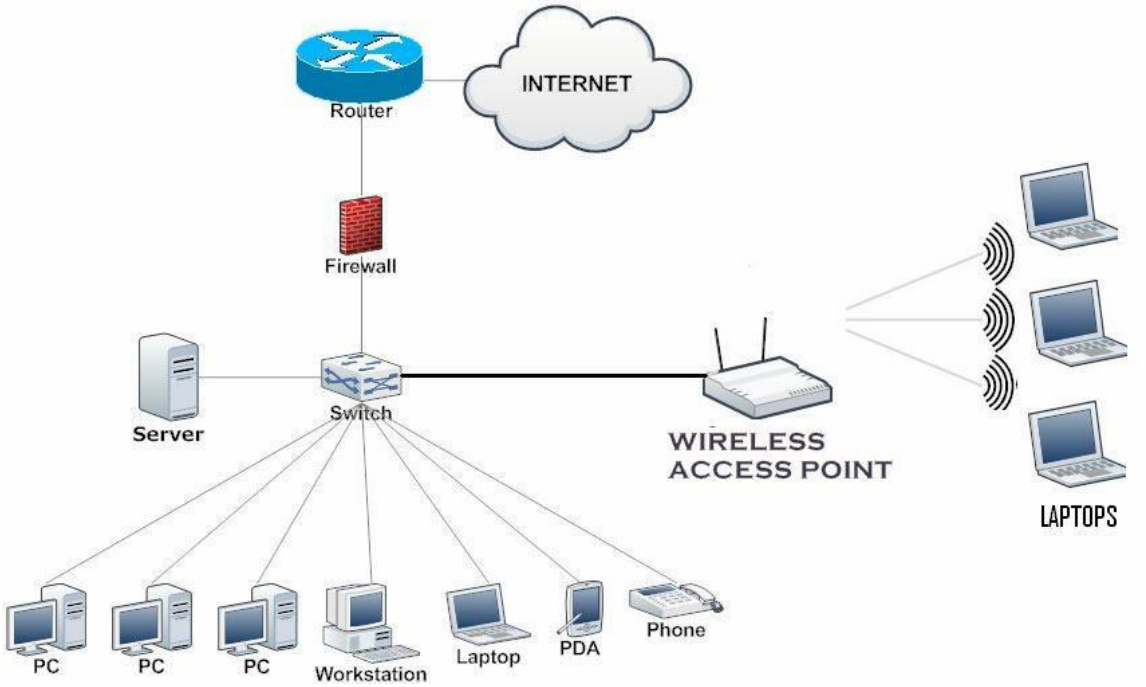
Monitoring Jaringan: Menggunakan alat monitoring jaringan untuk melacak kinerja jaringan, mendeteksi masalah, dan menganalisis penggunaan jaringan.

Logging Aktivitas: Menyimpan log aktivitas pengguna untuk kepatuhan, analisis forensik, dan troubleshooting. Pastikan log mencatat informasi penting seperti waktu login, durasi koneksi, dan situs atau layanan yang diakses.

f. Kebijakan Penggunaan yang Adil (Fair Usage Policy)

Sosialisasi Kebijakan: Menyusun dan mensosialisasikan kebijakan penggunaan yang adil untuk semua pengguna, menjelaskan batasan dan tanggung jawab mereka dalam menggunakan jaringan WiFi kampus.

Penegakan Kebijakan: Menerapkan kebijakan penggunaan yang adil secara konsisten, termasuk memberikan sanksi bagi pengguna yang melanggar aturan.



Gambar 8.1 : Jaringan Interkoneksi Kampus IAIN Manado skala Small to Midsize

Manajemen user jaringan WiFi kampus mencakup autentikasi dan otorisasi pengguna, kontrol akses berbasis peran, pengelolaan bandwidth, keamanan jaringan, monitoring, kebijakan penggunaan yang adil, dan manajemen perangkat. Implementasi yang tepat dari komponen-komponen ini akan memastikan jaringan yang aman, efisien, dan dapat diandalkan, mendukung semua kebutuhan pengguna di lingkungan kampus.

BAB IX : Pengembangan Sistem Informasi Manajemen Kampus

1. Proses Pentahapan

Pengembangan Sistem Informasi Manajemen (SIM) kampus di IAIN Manado dilakukan secara bertahap selama empat tahun. Setiap tahapan mencakup perencanaan, desain, pengembangan, dan implementasi serta evaluasi untuk memastikan sistem berjalan dengan efektif dan efisien. Berikut adalah rincian tahapan pengembangan per tahun:

Tahun 1 (2024) : Perencanaan dan Analisis Kebutuhan

a. Pembentukan Tim
   - Membentuk tim proyek yang terdiri dari anggota dari berbagai departemen termasuk IT, akademik, administrasi, dan manajemen.
   - Penetapan peran dan tanggung jawab masing-masing anggota tim.

b. Studi Kelayakan
   - Melakukan analisis biaya-manfaat untuk menentukan kelayakan proyek.
   - Menyusun laporan studi kelayakan yang mencakup evaluasi teknis, operasional, dan finansial.

c. Analisis Kebutuhan
   - Mengadakan workshop, wawancara, dan survei dengan stakeholders (mahasiswa, dosen, staf) untuk mengidentifikasi kebutuhan.
   - Menyusun dokumen kebutuhan fungsional dan non-fungsional.

d. Perencanaan Proyek
   - Menyusun rencana proyek yang mencakup jadwal, anggaran, dan sumber daya yang dibutuhkan.
   - Menetapkan milestones dan deliverables.

Tahun 2 (2025) : Desain Sistem

a. Desain Arsitektur Sistem

- Menentukan arsitektur sistem, termasuk komponen perangkat keras dan perangkat lunak.
- Desain basis data dan model data sesuai dengan kebutuhan kampus.

b. Desain Antarmuka Pengguna
- Mengembangkan prototipe antarmuka pengguna untuk setiap modul utama (registrasi, keuangan, akademik, perpustakaan, dll.).
- Mengumpulkan umpan balik dari stakeholders dan melakukan iterasi pada desain antarmuka.

c. Dokumentasi Desain
- Menyusun dokumen desain yang mencakup diagram arsitektur, diagram alur data, spesifikasi teknis, dan model basis data.
- Menyusun rencana pengujian untuk memastikan setiap modul berfungsi dengan baik.

Tahun 3 (2026) : Pengembangan dan Pengujian

a. Pengembangan Sistem
- Pengembangan modul-modul utama sistem berdasarkan desain yang telah disusun.
- Melakukan integrasi dengan sistem PDDIKTI dan NEOFEEDER.

b. Pengujian Unit
- Melakukan pengujian unit pada setiap modul untuk memastikan fungsi berjalan sesuai spesifikasi.
- Menyusun laporan pengujian dan melakukan perbaikan jika diperlukan.

c. Pengujian Sistem
- Melakukan pengujian sistem secara menyeluruh untuk memastikan integrasi antar modul berjalan dengan baik.
- Melakukan pengujian keamanan dan performa untuk memastikan sistem siap digunakan.

Tahun 4 (2027) : Implementasi dan Evaluasi

a. Implementasi Sistem
- Pemasangan perangkat keras dan perangkat lunak di lingkungan produksi.
- Migrasi data dari sistem lama ke sistem baru.

b. Pelatihan Pengguna

- Menyusun materi pelatihan dan manual pengguna.
- Melakukan pelatihan untuk dosen, staf administrasi, dan mahasiswa.

c. Sosialisasi Sistem

- Mengadakan sesi sosialisasi untuk memperkenalkan sistem baru kepada seluruh pengguna kampus.
- Menyediakan dukungan teknis selama masa transisi.

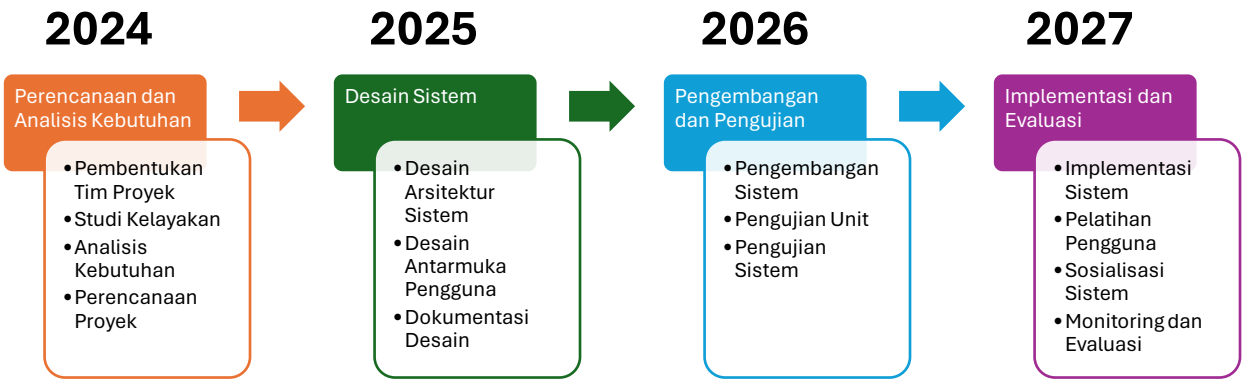
d. Monitoring dan Evaluasi

- Memantau penggunaan sistem dan mengumpulkan umpan balik dari pengguna.
- Melakukan evaluasi kinerja sistem berdasarkan indikator yang telah ditetapkan.
- Menyempurnakan dan mengoptimalkan sistem berdasarkan umpan balik dan hasil evaluasi.
- Menyusun laporan akhir proyek yang mencakup seluruh tahapan pengembangan, hasil evaluasi, dan rekomendasi untuk pengembangan selanjutnya.

Tabel 9.1 : Gant Chart terkait Pengembangan SIM Kampus

Tahun ke-	Tahapan	Q1	Q2	Q3	Q4
1 (2024)	Pembentukan Tim Proyek	■			
	Studi Kelayakan	■	■		
	Analisis Kebutuhan		■	■	
	Perencanaan Proyek			■	■
2 (2025)	Desain Arsitektur Sistem	■	■		
	Desain Antarmuka Pengguna		■	■	
	Dokumentasi Desain			■	■
3 (2026)	Pengembangan Sistem	■	■	■	
	Pengujian Unit			■	■
	Pengujian Sistem				■
4 (2027)	Implementasi Sistem	■	■		

	Pelatihan Pengguna				
	Sosialisasi Sistem				
	Monitoring dan Evaluasi				



Gambar 9.1 : Bagan alur pengembangan SIM Kampus dalam 4 tahun

2. Kesimpulan

Pengembangan Sistem Informasi Manajemen (SIM) di IAIN Manado selama empat tahun bertujuan untuk meningkatkan efisiensi operasional, kualitas layanan, keamanan data, dan mendukung pengambilan keputusan strategis. Tahapan pengembangan meliputi perencanaan dan analisis kebutuhan di tahun pertama, desain sistem pada tahun kedua, pengembangan dan pengujian pada tahun ketiga, serta implementasi dan evaluasi di tahun keempat. Setiap tahapan dirancang untuk memastikan bahwa sistem yang dihasilkan memenuhi kebutuhan kampus secara optimal dan dapat diimplementasikan dengan baik.

Manfaat utama dari pengembangan SIM ini adalah peningkatan efisiensi dan produktivitas melalui otomatisasi proses administrasi, kemudahan akses informasi bagi semua pengguna, peningkatan kualitas layanan pendidikan, dan peningkatan keamanan data. Dengan sistem yang terintegrasi dan mudah diakses, SIM ini akan memfasilitasi komunikasi dan kolaborasi yang lebih

baik antara mahasiswa, dosen, dan staf, serta memberikan dukungan yang kuat bagi manajemen dalam pengambilan keputusan berbasis data.