



UMKKT
UNIVERSITAS MUHAMMADIYAH
KALIMANTAN TIMUR

KEBIJAKAN PENGELOLAAN TEKNOLOGI INFORMASI



UNIT TEKNOLOGI INFORMASI

Kata Pengantar

Bismillahirrahmanirrahim.

Segala puji hanya milik Allah Subhanahu wa Ta'ala yang telah melimpahkan rahmat, taufik, dan hidayah-Nya sehingga kami dapat menyusun dokumen “Kebijakan Pengelolaan Teknologi Informasi Universitas Muhammadiyah Kalimantan Timur (UMKT)” ini. Shalawat serta salam semoga senantiasa tercurah kepada junjungan kita, Nabi Muhammad Shallallahu ‘Alaihi Wasallam, yang telah membawa umat manusia dari kegelapan menuju cahaya Islam yang terang benderang.

Kebijakan ini dirancang untuk menyelaraskan kebutuhan bisnis dengan perkembangan teknologi informasi yang dinamis, sekaligus memastikan pengelolaan teknologi informasi yang aman, berkelanjutan, dan sesuai dengan standar internasional, seperti ISO/IEC 38500:2015. Kami berharap implementasi kebijakan ini dapat memberikan manfaat yang signifikan dalam memperkuat kinerja institusi dan meningkatkan kualitas layanan akademik.

Kami mengucapkan terima kasih kepada semua pihak yang telah memberikan dukungan dan kontribusi dalam proses penyusunan dokumen ini. Semoga kebijakan ini dapat diimplementasikan dengan baik dan mendukung pencapaian tujuan strategis UMKT.

Samarinda, 30 Agustus 2024,

Unit IT

Executive Summary

Dokumen “Kebijakan Pengelolaan Teknologi Informasi UMKT” merupakan acuan untuk semua sivitas akademika dalam menyelaraskan kebutuhan bisnis dengan perkembangan teknologi informasi. Kebijakan ini berlaku untuk seluruh sivitas akademika, tidak hanya untuk pengelola TI (teknologi informasi).

Isi dokumen mencakup standar implementasi, struktur dokumen, kebijakan terkait organisasi TI, kebijakan perencanaan TI, realisasi TI, pengoperasian TI, dan pemeliharaan TI.

Dokumen disusun mengacu perundangan yang berlaku, standar ISO/IEC 38500:2015 tentang tata kelola TI untuk organisasi, dan *best practice* di dunia internasional.

Penerapan kebijakan ini mencakup dimasukkannya sasaran kinerja TI ke dalam Renstra UMKT, melengkapi dokumen kebijakan dengan dokumen turunannya (pedoman, standar, dan SOP), menyediakan sumber daya manusia dan aset yang memadai, dan melakukan audit terhadap kinerja tata kelola TI yang dilaporkan dalam rapat tinjauan manajemen. Penerapan tersebut mengikuti siklus PDCA (*plan – do – check – action*) agar terjadi perbaikan yang berkelanjutan.

Perencanaan TI dituangkan dalam *blue print* yang harus disetujui Rektorat sebelum digunakan. Isi *blue print* dilengkapi arsitektur sistem dan jadwal implementasi. *Blue print* diturunkan menjadi Renstra dan tiap tahun dibuat Renop berdasarkan Renstra.

Realisasi (atau pengadaan/pengembangan) dari rencana dilakukan dengan tahapan yang jelas dan dipilah menjadi pekerjaan software/aplikasi, pekerjaan infrastruktur, dan pekerjaan terkait data. Pemilahan sesuai dengan sifat pekerjaan.

Pengoperasian dimulai dengan penetapan *service level* (angka yang menunjukkan target mutu pengoperasian teknologi informasi). Pengoperasian memperhatikan aspek keamanan dan kontinuitas sistem. Setiap software harus memiliki dokumentasi pendukung, mulai dari dokumen pengembangan, manual, dan materi training. Setiap infrastruktur harus memperhatikan aspek keamanan. Data perlu dibackup secara reguler dengan jadwal yang rapi. Software maupun infrastruktur dapat disediakan oleh pihak ketiga dengan manajemen kerjasama yang baik dan jaminan keamanan data milik Universitas.

Daftar Isi

Halaman judul	i
Kata Pengantar	ii
Daftar Isi	iii
Bab 1. UMUM	1
1. Tujuan	1
2. Ruang Lingkup dan Cakupan	1
3. Acuan	1
4. Penerapan	2
Bab 2. Standar Implementasi	3
1. Tujuan	3
2. Kebijakan	3
Bab 3. Struktur Dokumen Pengelolaan Teknologi Informasi	5
1. Tujuan	5
2. Penerapan	5
Bab 4. Organisasi Pengelola Teknologi Informasi	6
1. Tujuan	6
2. Penerapan	6
Bab 5. Kebijakan Umum Pengelolaan Teknologi Informasi	7
1. Tujuan	7
2. Ruang Lingkup	7
3. Kebijakan	7
Bab 6. Kebijakan Perencanaan Teknologi Informasi	10
1. Tujuan	10
2. Ruang Lingkup	10
3. Kebijakan	10
Bab 7. Kebijakan Realisasi Teknologi Informasi	13
1. Tujuan	13
2. Ruang Lingkup	13
3. Kebijakan	13
Bab 8. Kebijakan Pengoperasian Teknologi Informasi	16
1. Tujuan	16
2. Ruang Lingkup	16
3. Kebijakan	16
Bab 9. Kebijakan Pemeliharaan Teknologi Informasi	20
1. Tujuan	20
2. Ruang Lingkup	20
3. Kebijakan	20

Bab 1. UMUM

1. Tujuan

Kebijakan Pengelolaan Teknologi Informasi ini disusun dengan tujuan untuk memberikan acuan yang jelas kepada manajemen dalam mengelola teknologi informasi dalam upaya menyelaraskan antara kebutuhan bisnis dengan perkembangan teknologi informasi terkini dan memberikan dampak positif yang maksimal dalam upaya UMKT mencapai visi dan misinya. Pengelolaan teknologi informasi yang baik menjadikan sistem informasi bekerja secara efisien dan membuat sivitas akademika bekerja dengan optimal.

2. Ruang Lingkup dan Cakupan

1. Kebijakan ini berlaku mulai dari proses perencanaan, realisasi, pengoperasian, dan pemeliharaan teknologi informasi di Universitas Muhammadiyah Kalimantan Timur.
2. Cakupan dari kebijakan ini adalah seluruh aktivitas yang dilakukan oleh Universitas Muhammadiyah Kalimantan Timur.
3. Kebijakan Pengelolaan Teknologi Informasi ini meliputi:
 - a. Umum
 - b. Standar Implementasi
 - c. Struktur Dokumen Pengelolaan Teknologi Informasi
 - d. Organisasi Pengelola Teknologi Informasi
 - e. Kebijakan Perencanaan, Realisasi, Pengoperasian dan Pemeliharaan Teknologi Informasi

3. Acuan

UMKT menyadari bahwa informasi merupakan aset yang harus disimpan, diolah, dan dipelihara. Oleh karena itu UMKT berkomitmen menerapkan tata kelola teknologi informasi yang baik. Untuk mencapai hal tersebut, Manajemen UMKT harus menetapkan kebijakan pengelolaan teknologi informasi yang didasarkan pada:

1. Peraturan Perundangan yang berlaku di Negara Republik Indonesia serta di area tempat dilakukannya kegiatan oleh sivitas akademika UMKT.
2. Peraturan-peraturan terkait yang berlaku di UMKT.
3. Standar ISO/IEC 38500:2015 tentang Information Technology – Governance of Information Technology for Organization yang diadopsi di Indonesia menjadi Standar Nasional Indonesia (SNI) ISO/IEC 38500:2016 tentang Teknologi Informasi – Tata kelola TI untuk Organisasi.
4. Kebutuhan internal UMKT terhadap teknologi informasi dengan sudut pandang bahwa informasi adalah aset yang harus disimpan, diolah secara akurat, dipelihara dan dapat diakses oleh pihak yang berkepentingan.
5. *Best practice* di dunia internasional dalam tata kelola teknologi informasi.

4. Penerapan

Untuk mendukung penerapan tata kelola teknologi informasi yang baik dan memberi nilai tambah yang efektif dan maksimal, Manajemen UMKT perlu melakukan hal-hal berikut.

1. Manajemen menetapkan sasaran kinerja pengelolaan teknologi informasi dengan mencantumkannya ke dalam Renstra Universitas Muhammadiyah Kalimantan Timur.
2. Manajemen memastikan tersedianya dokumentasi pendukung yang diperlukan untuk mengimplementasikan bab-bab kebijakan pengelolaan teknologi informasi yang tertulis dalam dokumen ini.
3. Manajemen memastikan diikutinya kebijakan pengelolaan teknologi informasi oleh semua pihak yang terkait.
4. Manajemen menyediakan sumber daya yang diperlukan agar implementasi kebijakan ini dapat berlangsung secara efektif.
5. Manajemen melakukan pemantauan terhadap pencapaian sasaran kinerja pengelolaan teknologi informasi.
6. Manajemen memastikan dilakukannya audit tata kelola teknologi informasi secara berkala. Audit internal dilakukan setidaknya satu kali dalam setahun dan audit eksternal setidaknya dilakukan satu kali dalam dua tahun.
7. Manajemen memastikan dilaporkannya butir pengelolaan teknologi informasi dalam rapat tinjauan manajemen setidaknya satu kali dalam setahun.
8. Manajemen memastikan terdapat peningkatan yang berkelanjutan terhadap implementasi kebijakan pengelolaan teknologi informasi.

Bab 2. Standar Implementasi

1. Tujuan

Standar implementasi memberikan panduan dalam melakukan implementasi kebijakan pengelolaan teknologi informasi di lingkungan Universitas Muhammadiyah Kalimantan Timur. Standar implementasi kebijakan ini menggunakan siklus PPEPP (Perencanaan, Pelaksanaan, Evaluasi, Pengendalian, Peningkatan). Implementasi dimaksud mencakup kegiatan perencanaan, pengembangan/pengadaan, pengoperasian, dan perawatan teknologi informasi.

2. Kebijakan

1. Proses perencanaan dalam implementasi kebijakan meliputi kegiatan:
 - a. menentukan isu internal dan eksternal yang mempengaruhi proses implementasi kebijakan,
 - b. menentukan pihak-pihak yang terkait dalam proses implementasi kebijakan,
 - c. menentukan ruang lingkup implementasi kebijakan,
 - d. menetapkan komitmen manajemen yang terkait implementasi kebijakan,
 - e. mengkomunikasikan dan mensosialisasikan pedoman pengelolaan teknologi informasi,
 - f. menyiapkan manajemen perubahan bilamana diperlukan,
 - g. menetapkan sasaran kinerja,
 - h. menentukan sumber daya yang diperlukan dalam implementasi kebijakan,
 - i. mendokumentasikan rancangan implementasi kebijakan dan menyimpannya secara digital pada repositori.
2. Proses pelaksanaan dalam implementasi kebijakan meliputi kegiatan:
 - a. menjalankan kegiatan yang telah direncanakan dalam proses perencanaan,
 - b. melakukan pengadaan dan pengelolaan sumber daya untuk mendukung pelaksanaan kegiatan,
 - c. mendokumentasikan proses pelaksanaan kegiatan,
 - d. mensosialisasikan kegiatan dan prosedur yang berubah akibat implementasi kebijakan,
 - e. melakukan pelatihan kepada pengguna teknologi.
3. Proses evaluasi dalam implementasi kebijakan meliputi kegiatan:
 - a. menilai efektivitas implementasi kebijakan sekurang-kurangnya sekali dalam setahun,
 - b. memantau dan melaporkan pencapaian sasaran kinerja sekurang-kurangnya sekali dalam setahun,
 - c. melakukan survei kepuasan terhadap implementasi kebijakan kepada semua pihak yang terkait,
 - d. melakukan audit internal pengelolaan teknologi informasi sekurang-kurangnya sekali dalam setahun,

- e. melaporkan hasil audit dalam tinjauan manajemen sekurang-kurangnya sekali dalam setahun.
4. Proses pengendalian dalam implementasi kebijakan meliputi:
- a. menindaklanjuti hasil audit mutu internal
 - b. memantau penerapan permintaan tindakan dan perbaikan yang dihasilkan dalam proses audit,
5. Proses peningkatan dalam implementasi kebijakan meliputi:
- a. menyusun strategi dalam pengembangan dan peningkatan berkelanjutan
 - b. melakukan peningkatan berkelanjutan terhadap pengelolaan teknologi informasi dengan melakukan perencanaan yang memperhatikan hasil evaluasi.

Bab 3. Struktur Dokumen Pengelolaan Teknologi Informasi

1. Tujuan

menjabarkan struktur dokumen pengelolaan teknologi informasi yang diterapkan di Universitas.

2. Penerapan

Struktur dokumen pengelolaan teknologi informasi yang digunakan di Universitas Muhammadiyah Kalimantan Timur adalah sebagai berikut.

Jenis dokumen	Definisi
Kebijakan	Dokumen kebijakan teknologi informasi di UMKT
Standar	Dokumen yang berisi persyaratan minimum yang ditetapkan berdasarkan konsensus para pemangku kepentingan
Prosedur	Dokumen yang berisi tata cara dan pedoman dalam menjalankan proses menggunakan teknologi informasi atau mengoperasikan teknologi informasi
Formulir	Dokumen untuk merekam semua kegiatan dalam implementasi teknologi informasi

Bab 4. Organisasi Pengelola Teknologi Informasi

1. Tujuan

Untuk memberikan sebuah bingkai manajemen agar memungkinkan terjadinya implementasi kebijakan pengelolaan teknologi informasi yang efektif.

2. Penerapan

Untuk tersusunnya organisasi pengelolaan teknologi informasi yang efektif, manajemen UMKT perlu melakukan hal-hal berikut.

1. Menetapkan Rektor sebagai pengarah pada proses pengelolaan teknologi informasi dengan pelaksana harian dimandatkan kepada salah seorang wakil rektor.
2. Mengidentifikasi semua tugas dan fungsi yang perlu dilakukan dalam pengelolaan teknologi informasi.
3. Menetapkan penanggung jawab yang melakukan tugas dan fungsi tersebut dalam struktur jabatan.
4. Tugas yang bertentangan harus dipisahkan dan dilakukan oleh orang yang berbeda untuk mengurangi resiko konflik kepentingan.
5. Mengidentifikasi dan menetapkan pola kerjasama dengan pihak lain di luar Universitas.
6. Mengidentifikasi pekerjaan yang bersifat jangka panjang atau jangka pendek dan menetapkan pelaksanaan tugas dalam bentuk struktur jabatan atau tim *ad-hoc*.
7. Mendokumentasikan tugas pokok dan fungsi setiap jabatan dalam dokumen analisis jabatan.

Bab 5. Kebijakan Umum Pengelolaan Teknologi Informasi

1. Tujuan

Menjadi referensi kepada manajemen dan tim pengelola teknologi informasi dalam melakukan penyesuaian strategis antara organisasi dan teknologi informasi.

2. Ruang Lingkup

Ruang lingkup kebijakan ini meliputi:

1. Penyesuaian strategis antara organisasi dan pengelolaan TI (*IT alignment*).
2. Manajemen risiko dan pengendalian risiko
3. Efisiensi dan efektivitas pengelolaan sumber daya

3. Kebijakan

1. Keselarasan strategis antara organisasi Universitas dan teknologi informasi dicapai melalui mekanisme:
 - a. menyesuaikan tujuan pengembangan TI dengan tujuan Universitas, di mana setiap tujuan pengembangan TI harus mempunyai referensi tujuan Universitas.
 - b. menyesuaikan arsitektur bisnis Universitas dengan arsitektur TI (arsitektur informasi, arsitektur aplikasi, dan arsitektur infrastruktur).
 - c. menyesuaikan eksekusi inisiatif TI dengan rencana strategis UMKT.
2. Menyusun manajemen risiko dengan menetapkan risiko prioritas dalam pengelolaan teknologi informasi dan melakukan pengendalian terhadap risiko.
 - a. Risiko prioritas meliputi:
 1. Risiko atas proyek mencakup kemungkinan tertundanya penyelesaian proyek TI, biaya yang melebihi dari perkiraan atau hasil akhir (*deliverables*) proyek tidak sesuai dengan spesifikasi yang telah ditentukan di awal.
 2. Risiko atas informasi mencakup akses yang tidak berhak atas aset informasi, perubahan informasi oleh pihak yang tidak berhak dan penggunaan informasi oleh pihak yang tidak punya hak untuk keperluan yang tidak sebagaimana mestinya.
 3. Risiko atas keberlangsungan layanan mencakup kemungkinan terganggunya ketersediaan (*availability*) layanan TI atau layanan TI sama sekali tidak dapat berjalan.
 - b. Pengendalian risiko meliputi:
 1. Implementasi *Project Governance* untuk setiap proyek TI yang dijalankan.
 2. Implementasi *Security Governance* di manajemen TI dan seluruh sistem TI yang berjalan, khususnya untuk meminimalkan risiko atas informasi dan keberlangsungan layanan.
3. Mengelola sumber daya untuk mencapai efisiensi dan efektivitas penggunaan sumber daya yang mencakup sumber daya finansial, informasi, teknologi dan manusia.

- a. Untuk mencapai efisiensi dan efektivitas sumber daya finansial perlu dilakukan hal berikut.
1. Kelayakan belanja TI diukur secara rasional dengan metode penganggaran modal
 2. Melakukan prosedur pengadaan yang efisien dengan fokus pada kualitas produk dan jasa teknologi informasi
 3. Memprioritaskan anggaran untuk proyek TI yang bermanfaat bagi banyak pengguna, berbiaya rendah, dan cepat dirasakan manfaatnya
 4. Perhitungan manfaat dan biaya harus memasukkan unsur-unsur yang bersifat kasat mata (*tangible*) dan terukur maupun yang tidak tampak (*intangible*).
 5. Efisiensi finansial harus mempertimbangkan biaya kepemilikan total (*Total Cost of Ownership – TCO*) yang bisa meliputi harga barang/jasa yang dibeli, biaya pelatihan karyawan, biaya perawatan (*maintenance cost*), biaya langganan (*subscription/license fee*), dan biaya-biaya yang terkait dengan pemerolehan barang/jasa yang dibeli.
 6. Efisiensi finansial bisa mempertimbangkan antara keputusan membeli atau membuat sendiri sumber daya TI. Selain itu juga bisa mempertimbangkan antara sewa/outsourcing dengan memiliki sumber daya TI baik dengan membuat sendiri maupun membeli.
- b. Untuk mencapai efisiensi dan efektivitas sumber daya informasi perlu dilakukan hal berikut.
1. Penyusunan arsitektur informasi yang mencerminkan kebutuhan informasi, struktur informasi dan pemetaan hak akses atas informasi oleh peran-peran yang ada dalam manajemen organisasi.
 2. Identifikasi kebutuhan perangkat lunak aplikasi yang sesuai dengan spesifikasi arsitektur informasi, yang memungkinkan informasi diolah dan disampaikan kepada peran yang tepat secara efisien.
- c. Untuk mencapai efisiensi dan efektivitas sumber daya teknologi (yaitu platform aplikasi, software, sistem dan infrastruktur) dapat dilakukan hal berikut.
1. Memberikan *shared service* terhadap software aplikasi jika terdapat kesamaan fitur fungsionalitas.
 2. Memberikan layanan koneksi jaringan intranet dan internet secara bersama dengan pengelolaan terpadu.
 3. Penyimpanan data secara terpadu dengan *data center*, sampai ke proses *backup* dan *disaster recovery*.

Bab 6. Kebijakan Perencanaan Teknologi Informasi

1. Tujuan

Menjadi acuan dalam menetapkan visi dan arsitektur TI dalam hubungannya dengan kebutuhan organisasi dan rencana realisasi atas implementasi visi dan arsitektur TI tersebut. Rencana TI yang telah disusun akan menjadi referensi bersama bagi seluruh unit di Universitas.

2. Ruang Lingkup

Ruang lingkup kebijakan ini meliputi:

1. Sinkronisasi dan integrasi perencanaan
2. Penyusunan blue print teknologi informasi dan komponennya

3. Kebijakan

1. Sinkronisasi dan integrasi
 - a. Sinkronisasi dan integrasi perencanaan sistem dilakukan sejak di level internal institusi maupun hubungan antar institusi.
 - b. Rektor atau Wakil Rektor terkait memberikan persetujuan akhir atas Blue Print Pengembangan Teknologi Informasi jangka panjang yang disiapkan oleh lembaga pengelola TI. Blue print dijadikan acuan dalam menyusun Renstra dan Renop bagi lembaga pengelola TI yang harus disahkan oleh Wakil Rektor.
2. Blue print memiliki perencanaan atas komponen:
 - a. Arsitektur informasi
 - b. Arsitektur aplikasi
 - c. Arsitektur infrastruktur teknologi informasi
 - d. Organisasi dan manajemen
 - e. Roadmap implementasi
3. Arsitektur informasi
 - a. Arsitektur informasi dibuat sebagai referensi model informasi organisasi yang dijadikan rujukan dalam seluruh desain software aplikasi.
 - b. Arsitektur informasi mencakup informasi terstruktur (data mart, database, database tabel, pertukaran data) dan informasi tidak terstruktur (gambar, video, file dokumen).
 - c. Penetapan arsitektur informasi mencakup penetapan klasifikasi ke dalam kelas-kelas data, pemetaan kepemilikan data, dan pendefinisian data dictionary, dan syntax rules.
 - d. Arsitektur informasi juga menetapkan klasifikasi level keamanan data untuk setiap klasifikasi kelas data melalui penetapan kriteria yang tepat sesuai dengan kebutuhan organisasi.
4. Arsitektur aplikasi

- a. Arsitektur aplikasi dibuat untuk memperjelas dukungan TI terhadap proses bisnis di mana setiap aplikasi harus berkorelasi dengan proses bisnis yang didukungnya.
 - b. Arsitektur aplikasi memberikan peta tentang aplikasi apa saja yang dibutuhkan sesuai dengan karakteristik konteks organisasi dan manajemen.
 - c. Efisiensi arsitektur teknis aplikasi ditempuh melalui pendekatan “One Stop Window” untuk setiap tipe pengguna, terutama publik dan pihak eksternal. Melalui pendekatan ini, publik hanya perlu mengakses satu sistem (menggunakan beragam delivery channel) untuk mendapatkan layanan TI. Misalnya, mahasiswa hanya perlu menghadapi satu sistem untuk semua kegiatan yang dilakukannya di Universitas.
5. Aplikasi dipilah menjadi kategori.
- a. pendukung tri dharma perguruan tinggi – belajar mengajar, administrasi akademik, dan administrasi penelitian dan pengabdian kepada masyarakat.
 - b. pendukung kegiatan manajemen internal – kepegawaian, keuangan, pengelolaan aset, pengelolaan program kerja, monitoring kinerja.
 - c. Data warehouse dan business intelligence
6. Arsitektur infrastruktur teknologi informasi
- a. Arsitektur infrastruktur teknologi informasi mencakup jaringan komunikasi, perangkat pemrosesan informasi (server, komputer dan perangkat pendukungnya), software untuk sistem (sistem operasi, sistem manajemen basis data baik SQL maupun NoSQL), dan media penyimpanan data.
 - b. Arsitektur infrastruktur diarahkan pada mekanisme *shared-services* untuk meningkatkan efisiensi belanja TI. Mekanisme *shared-service* diimplementasikan pada sumber: (1). infrastruktur komunikasi: jaringan komputer/komunikasi, koneksi internet dan (2) infrastruktur penyimpanan data (*data center*).
7. Organisasi dan Manajemen
- a. Perencanaan organisasi mencakup identifikasi struktur organisasi pengelola yang akan melakukan operasional harian.
 - b. Perencanaan manajemen mencakup pendefinisian prosedur teknis dengan prioritas pada domain: (1) realisasi sistem, (2) operasionalisasi sistem, dan (3) pemeliharaan sistem.
8. Roadmap implementasi
- a. Setiap perencanaan sistem menyertakan skenario *project governance* untuk setiap proyek yang direncanakan, untuk memastikan proyek dapat diselesaikan tepat waktu, tepat sasaran, dan tepat anggaran.
 - b. Setiap pekerjaan yang direncanakan selalu menyertakan proyeksi waktu, kapan benefit yang diharapkan dapat terealisasi (*benefit realization schedule*).
 - c. Setiap perencanaan sistem mempunyai roadmap implementasi yang didasarkan pada analisa kesenjangan arsitektur (informasi, aplikasi dan infrastruktur teknologi) serta kesenjangan manajemen dan organisasi.

- d. Roadmap implementasi terdiri dari portofolio program implementasi (yang dapat terdiri dari beberapa portofolio proyek untuk setiap programnya), penetapan peringkat prioritas portofolio proyek, dan pemetaan dalam domain waktu sesuai dengan durasi waktu yang ditargetkan.
 - e. Penetapan peringkat prioritas portofolio proyek TI dilakukan setidaknya berdasarkan faktor level anggaran yang dibutuhkan, kompleksitas sistem, dan besar usaha yang diperlukan.
9. Indikator keberhasilan
- a. Ketersediaan blue print yang mencakup lima komponen perencanaan
 - b. Tingkat kesesuaian proyek TI yang berjalan dibanding dengan rencana

Bab 7. Kebijakan Realisasi Teknologi Informasi

1. Tujuan

Menjadi acuan dalam mengimplementasikan rencana teknologi informasi, mulai dari pemilihan sistem TI sampai evaluasi pasca implementasi.

2. Ruang Lingkup

Ruang lingkup kebijakan ini meliputi:

1. Identifikasi dan pemilihan alternatif sistem
2. Realisasi software/aplikasi
3. Realisasi infrastruktur teknologi
4. Realisasi pengelolaan data

3. Kebijakan

1. Identifikasi dan pemilihan alternatif sistem
 - a. Pemilihan alternatif sistem atau proses pemilihan sistem dari alternatif sistem yang telah ada, dilakukan menggunakan referensi hasil studi kelayakan.
 - b. Pengelola TI melakukan studi kelayakan yang setidaknya terdiri dari aktivitas: (1) penentuan kebutuhan fungsional proses bisnis dan persyaratan teknis, (2) penentuan manfaat (*benefit*) yang hendak dicapai dengan keberadaan sistem, dan (3) analisis risiko terkait dengan proses bisnis
 - c. Untuk sistem TIK berskala besar, strategis, dan berpotensi mempengaruhi sistem TI sebelumnya, pemilihan alternatif sistem dapat dilakukan melalui mekanisme *Proof of Concept* (POC).
 - d. Pelaksanaan pemilihan teknologi dari alternatif yang ada yang melibatkan vendor dilakukan berdasarkan aturan pengadaan barang dengan menggunakan proses lelang.
2. Realisasi software aplikasi
 - a. Pengembangan dan/atau pengadaan (akuisisi) software aplikasi dilakukan berdasarkan metode System Development Life Cycle (SDLC) yang dipergunakan secara luas oleh industri software, yang minimal mencakup kebutuhan akan:
 - (1) Penerjemahan kebutuhan/persyaratan bisnis ke dalam spesifikasi desain
 - (2) Penyusunan desain detail dan teknis software aplikasi, termasuk pengendalian aplikasi (*application control*) (yang memungkinkan setiap pemrosesan dalam software aplikasi akurat, lengkap, tepat waktu, terotorisasi dan dapat diaudit) dan pengendalian keamanan aplikasi (*application security control*) (yang memungkinkan terpenuhinya aspek: kerahasiaan (*confidentiality*), ketersediaan (*availability*), dan integritas (*integrity*)).
 - (3) Implementasi desain detail dan teknis ke dalam kode program (*coding*) yang tersimpan di repositori (misalnya git).

- (4) Manajemen perubahan persyaratan/kebutuhan
 - (5) Pelaksanaan penjaminan mutu (*Quality Assurance*)
 - (6) Uji coba (*testing*): unit testing, system testing, integration testing, User Acceptance Test (UAT)
 - (7) Instalasi (*deployment*) dan Perawatan (*maintenance*)
- b. Metode SDLC juga diimplementasikan untuk proses upgrade atas software aplikasi yang ada (*existing*) jika perubahan bersifat utama (*major*), yang menghasilkan perubahan signifikan atas desain dan fungsionalitas yang ada (*existing*).
 - c. Setiap software aplikasi yang direalisasikan harus disertai dengan training dan/atau transfer pengetahuan kepada pengguna dan administrator sistem.
 - d. Setiap software aplikasi yang direalisasikan harus disertai dokumentasi berikut ini:
 - (1) Dokumentasi hasil aktivitas tahapan-tahapan dalam SDLC
 - (2) Manual Pengguna, Operasi, Dukungan Teknis dan Administrasi
 - (3) Materi transfer pengetahuan & materi *training*
3. Realisasi infrastruktur teknologi. Infrastruktur teknologi mencakup server, komputer, perangkat pendukungnya (seperti printer), jaringan komunikasi, software infrastruktur seperti sistem operasi dan *software tools*.
 - a. Kapasitas infrastruktur disesuaikan dengan kebutuhan sehingga realisasi harus disertai dengan analisis kebutuhan kapasitas.
 - b. Realisasi infrastruktur teknologi harus memperhatikan kontrol terkait keamanan dan *auditability* (audit atas kinerja perangkat dan histori transaksi), dengan tingkat kedalaman spesifikasi tergantung kebutuhan.
 - c. Tahapan testing perlu dilakukan sebelum perangkat dioperasikan, yang dilakukan di lingkungan terpisah (*environment test*) jika memungkinkan.
 4. Realisasi pengelolaan data.
 - a. Setiap langkah pengelolaan data harus memperhatikan tahapan: input, proses, dan output.
 - b. Pada tahapan input, prosedur yang harus dijalankan adalah: prosedur akses data, prosedur transaksi data untuk memeriksa akurasi, kelengkapan, dan validitasnya, serta prosedur pencegahan kesalahan input data.
 - c. Pada tahapan proses, prosedur yang harus dijalankan adalah: prosedur pengolahan data, prosedur validasi dan editing, serta prosedur penanganan kesalahan
 - d. Pada tahapan output, prosedur yang harus dijalankan adalah: prosedur distribusi, penanganan kesalahan, dan keamanan data.
 5. Indikator keberhasilan. Keberhasilan realisasi sistem diukur dengan indikator berikut.
 - a. Jumlah realisasi sistem yang tidak mengalami backlog (tertunda dan mendesak untuk segera diselesaikan).

- b. Persentase realisasi sistem yang disetujui oleh pemilik proses bisnis dan pengelola TI.
- c. Jumlah realisasi software aplikasi yang diselesaikan tepat waktu, sesuai spesifikasi dan selaras dengan arsitektur TI.
- d. Jumlah realisasi software aplikasi tanpa permasalahan integrasi selama implementasi.
- e. Jumlah realisasi software aplikasi yang konsisten dengan perencanaan TI yang telah disetujui.
- f. Jumlah software aplikasi yang didukung dokumentasi memadai dari yang seharusnya.
- g. Penurunan jumlah *downtime* infrastruktur.

Bab 8. Kebijakan Pengoperasian Teknologi Informasi

1. Tujuan

Menjadi acuan dalam menjalankan teknologi informasi sebagai bagian dari dukungan kepada proses bisnis sesuai spesifikasi yang ditentukan sebelumnya.

2. Ruang Lingkup

Ruang lingkup kebijakan ini meliputi:

1. Manajemen tingkat layanan (*service level*)
2. Keamanan dan keberlangsungan sistem
3. Manajemen software aplikasi
4. Manajemen infrastruktur
5. Manajemen data
6. Manajemen layanan oleh pihak ketiga

3. Kebijakan

1. Manajemen tingkat layanan (*service level*).
 - a. Pengelola TI bertanggung jawab atas penyusunan dan update daftar layanan TI, yang berisi sistem yang beroperasi dan layanan-layanan TI yang menyusunnya.
 - b. Layanan TI (diprioritaskan yang kritis) harus memiliki angka persetujuan tingkat layanan (SLA – *service level agreement*) yang ditetapkan oleh pemilik proses bisnis dan disetujui oleh Pengelola TI.
 - c. Aspek minimal yang harus tercakup dalam setiap SLA adalah:
 - (1) Waktu yang diperlukan untuk setiap layanan TI diterima oleh konsumen.
 - (2) Prosentase tingkat ketersediaan (*availability*) sistem TI.
 - (3) Waktu yang diperlukan untuk penyelesaian pengaduan jika terjadi insiden atau permasalahan (dengan beberapa tingkatan kritis jika diperlukan).
 - d. Pencapaian semua SLA dilaporkan secara reguler oleh Pengelola TI kepada pimpinan untuk di-*review*.
2. Keamanan dan keberlangsungan sistem.
 - a. Setiap operasi sistem TI harus memperhatikan persyaratan minimal aspek keamanan sistem dan keberlangsungan sistem, terutama sistem TI yang memfasilitasi layanan kritis.
 - b. Aspek keamanan dan keberlangsungan sistem minimal yang harus terpenuhi mencakup hal-hal berikut:
 - (1) Confidentiality: akses terhadap data/informasi dibatasi hanya bagi mereka yang punya otoritas.
 - (2) Integrity: data tidak boleh diubah tanpa ijin dari yang berhak

- (3) Authentication: untuk meyakinkan identitas pengguna sistem
- (4) Availability: terkait dengan ketersediaan layanan, termasuk *up-time* dari situs web.
- c. Mekanisme dasar yang harus dipenuhi untuk memastikan tercapainya aspek-aspek keamanan dan keberlangsungan sistem mencakup hal-hal berikut:
 - (1) Untuk pengamanan dari sisi software aplikasi dapat diimplementasikan komponen standar sebagai berikut:
 - (a) Teknik penulisan kode program aplikasi yang aman
 - (b) Implementasi mekanisme otentikasi dan otorisasi di dalam software aplikasi secara tepat
 - (c) Pengaturan keamanan database secara tepat
 - (2) Untuk pengamanan dari sisi infrastruktur teknologi dapat diimplementasikan komponen standar sebagai berikut:
 - (a) Hardening dari sisi sistem operasi
 - (b) Firewall, sebagai pagar untuk menghadang ancaman dari luar sistem
 - (c) Intrusion Detection System/ Intrusion-Prevention Systems (IDS/IPS), sebagai pendeteksi atau pencegah aktivitas ancaman terhadap sistem
 - (d) Network monitoring tool, sebagai usaha untuk melakukan monitoring atas aktivitas di dalam jaringan
 - (e) Log processor dan analysis, untuk melakukan pendeteksian dan analisis kegiatan yang terjadi di sistem.
 - (3) Untuk sistem kritis dengan SLA yang ketat, dapat ditempuh penyediaan sistem cadangan yang dapat secara cepat mengambil alih sistem utama jika terjadi gangguan ketersediaan (*availability*) pada sistem utama.
 - (4) Assessment kerentanan keamanan sistem (*security vulnerability system*) secara teratur sesuai dengan kebutuhan.
 - (5) Penyusunan *IT Contingency Plan* khususnya untuk proses bisnis kritis, yang diuji validitasnya secara teratur sesuai dengan kebutuhan.
- 3. Manajemen software aplikasi.
 - a. Setiap software aplikasi harus selalu menyertakan prosedur backup dan restore, dan juga mengimplementasikan fungsionalitasnya di dalam software aplikasi.
 - b. Setiap pengoperasian software aplikasi harus disertai oleh dokumentasi berikut ini:
 - (1) Dokumentasi hasil aktivitas tahapan-tahapan dalam SDLC
 - (2) Manual Pengguna, Operasi, Dukungan Teknis dan Administrasi
 - (3) Materi transfer pengetahuan dan materi Training

4. Manajemen infrastruktur. Setiap pengoperasian infrastruktur teknologi selalu memperhatikan kontrol yang terkait dengan faktor keamanan dan auditability (memungkinkan audit atas kinerja dan sejarah transaksi yang terjadi).
5. Manajemen data.
 - a. Data dari setiap software aplikasi secara kumulatif dibackup secara terpusat dalam media penyimpanan data (data storage), terutama software aplikasi kritikal.
 - b. Backup data dilakukan secara reguler, dengan frekuensi dan jenis backup disesuaikan dengan tingkat kritikal sistem.
 - c. Dilakukan pengujian secara teratur mekanisme backup dan restore data, untuk memastikan integritas dan validitas prosedur.
 - d. Implementasi mekanisme inventori atas media penyimpanan data, terutama media off-line.
6. Manajemen layanan pihak ketiga.
 - a. Layanan TIK dapat diselenggarakan sebagian atau seluruhnya oleh pihak ketiga, dengan mempertimbangkan faktor berikut:
 - (1) Sumber daya internal yang dimiliki tidak cukup untuk mencapai tingkat layanan minimal yang diperlukan/dipersyaratkan.
 - (2) Seluruh data yang diolah melalui layanan pihak ketiga adalah data milik Universitas, dan pihak ketiga harus menjaga kerahasiaannya dan tidak berhak menggunakannya untuk hal-hal di luar kerjasama.
 - b. Seluruh layanan TIK yang diselenggarakan oleh pihak ketiga harus mematuhi ketentuan operasi sistem yang telah dijelaskan di atas, terkait:
 - (1) Manajemen tingkat layanan
 - (2) Keamanan dan keberlangsungan sistem
 - (3) Manajemen software aplikasi
 - (4) Manajemen infrastruktur
 - (5) Manajemen data
 - c. Secara reguler pihak ketiga penyelenggara layanan TI harus memberikan laporan atas tingkat kepatuhan terhadap ketentuan operasi sistem di atas.
 - d. Pengelola TI Universitas secara reguler dan insidental dapat melakukan audit atas laporan yang disampaikan oleh pihak ketiga untuk memastikan validitasnya.
7. Indikator keberhasilan dalam pengoperasian sistem adalah sebagai berikut:
 - a. Persentase jumlah sistem kritikal yang memiliki SLA dibanding jumlah keseluruhan
 - b. Persentase layanan TI yang memenuhi SLA
 - c. Tingkat kepatuhan sistem terhadap kriteria keamanan
 - d. Jumlah insiden yang menyebabkan downtime

- e. Jumlah kumulatif waktu downtime per durasi waktu
- f. Jumlah insiden terkait permasalahan integritas data
- g. Jumlah kegagalan *restore* data kritikal

Bab 9. Kebijakan Pemeliharaan Teknologi Informasi

1. Tujuan

Memastikan seluruh sumber daya TI dapat berfungsi sebagaimana mestinya dalam durasi siklus hidup yang seharusnya, dalam rangka mendukung operasional sistem secara maksimal.

2. Ruang Lingkup

Ruang lingkup kebijakan ini meliputi:

1. Pemeliharaan software aplikasi
2. Pemeliharaan infrastruktur teknologi
3. Pemeliharaan data
4. Siklus hidup dan likuidasi sumber daya infrastruktur teknologi

3. Kebijakan

1. Pemeliharaan software aplikasi
 - a. Pengelola TI menerapkan mekanisme *patching* software aplikasi atas software aplikasi yang dikembangkan secara mandiri atau kerjasama dengan pihak ketiga.
 - b. Upgrade yang bersifat kecil (minor) atas software aplikasi minimal harus melalui *regression test* dan harus disertai dengan update dokumentasi yang terkait langsung dengan modul yang diupgrade.
 - c. Backup aplikasi dari sisi source code dan asset digital.
2. Pemeliharaan infrastruktur teknologi
 - a. Pengelola TI menerapkan mekanisme *patching* infrastruktur teknologi (yaitu update *patch* atas infrastruktur teknologi untuk menutup lobang kerentanan) atas seluruh infrastruktur teknologinya. Mekanisme *patching* ini jika memungkinkan dapat difasilitasi secara otomatis dengan software tool, sehingga meningkatkan efisiensi di sisi administrator dan pengguna akhir. Mekanisme *patching* ini minimal dilakukan atas:
 - (1) System software di perangkat jaringan
 - (2) System software di server
 - (3) Database server
 - b. Secara reguler Pengelola TI melakukan penilaian pertumbuhan kapasitas dan membandingkannya dengan estimasi pertumbuhan. Berdasarkan analisis
 - c. perbandingan tersebut, Pengelola TI menyusun langkah untuk pengelolaan kapasitas dalam jangka menengah dan pendek.
3. Pemeliharaan data
 - a. Pemeliharaan data difokuskan pada keaslian, keutuhan, dan ketersediaan data. Semua pihak di Universitas secara bersama bertanggung jawab dalam melakukan pemeliharaan

data sesuai tanggung jawab pekerjaan masing-masing dan harus menaati prosedur pemeliharaan data yang telah ditetapkan.

- b. Data Center dikelola sesuai dengan prosedur baku yang ada.
 - c. Data harus dilindungi dari pihak-pihak yang tidak memiliki hak akses.
 - d. Backup database harus dilakukan dengan menerapkan minimal dua lokasi backup yang salah satunya di luar daerah kampus.
4. Likuidasi sumber daya infrastruktur teknologi
- a. Likuidasi sumber daya yang masuk kategori *sunset technology* (mulai usang) dilakukan jika tidak dinilai sudah tidak layak, tidak ada lagi *technical support*, dan sudah ada teknologi pengganti yang lebih handal dan terjangkau
 - b. Umur ideal dari perangkat infrastruktur server adalah kurang dari 7 tahun, dan perangkat jaringan adalah kurang dari 5 tahun.
 - c. Perlu dilakukan review tahunan terkait penggantian perangkat jika umur perangkat telah mencapai umur ideal kurang dua tahun
 - d. Likuidasi perlu mendapat persetujuan pimpinan Universitas
5. Indikator keberhasilan
- a. Jumlah permasalahan software aplikasi akibat kesalahan patching
 - b. Jumlah permasalahan infrastruktur teknologi akibat kesalahan patching
 - c. Jumlah permasalahan terkait integritas, kerahasiaan dan ketersediaan data.