Dosen dan Mahasiswa

PROPOSAL

PENELITIAN

ASESMEN TATA KELOLA KEAMANAN TEKNOLOGI INFORMASI STMIK PALANGKARAYA MENGGUNAKAN INDEKS KEAMANAN INFORMASI

TIM PENGUSUL

Amaya Andri Damaini, S.Kom., M.T	NIK. 199309042018001
Abdul Hadi. ST., M.Kom	NIK. 198505102021101
Elia Zakharia, M.T..	NIK. 199205262016104
Herkules, S.Kom., M.Cs	NIK. 198510042010106
Yoantri Et Devitsu	NIM. C2155201035

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER (STMIK) PALANGKARAYA
2024

HALAMAN PENGESAHAN
PROPOSAL

Judul Penelitian	:Asesmen Tata Kelola Keamanan Teknologi Informasi STMIK Palangkaraya Menggunakan Indeks Keamanan Informasi
Kode / Rumpun Ilmu	:123 / Ilmu Komputer
Peneliti:	
a. Nama Lengkap	: Amaya Andri Damaini, S.Kom., M.T
b. NIDN	: 1104099301
c. Jabatan Fungsional	: Asisten Ahli
d. Program Studi	: Teknik Informatika
e. Nomor HP	: 0852-4836-7262
f. Alamat surel (e-mail)	: amayaandridamaini@gmail.com
Anggota Peneliti (1)	
a. Nama Lengkap	: Abdul Hadi, ST. M.Kom
b. NIDN	: 1110058501
c. Jabatan Fungsional	: Asisten Ahli
d. Program Studi	: Teknik Informatika
e. Nomor HP	: 085280005003
f. Alamat surel (e-mail)	: abdulhadi@stmikplk.ac.id
Anggota Peneliti (2)	
a. Nama Lengkap	: Elia Zakharia, M.T..
b. NIDN	: 1126059201
c. Jabatan Fungsional	: Asisten Ahli
d. Program Studi	: Teknik Informatika
e. Nomor HP	: 085752443600
f. Alamat surel (e-mail)	: eliazakharia@gmail.com
Anggota Peneliti (3)	
a. Nama Lengkap	: Herkules, S.Kom.,M.Kom.
b. NIDK	: 1104108502
c. Jabatan Fungsional	: Lektor

d.	Program Studi	: Teknik Informatika
e.	Nomor HP	: 085228043555
Anggota Peneliti (4)		
a.	Nama Lengkap	: Yoantri Et Devitsu
b.	NIM	: C2155201035
c.	Program Studi	: Teknik Informatika
d.	Nomor HP	: 082255774987
e.	Alamat surel (e-mail)	: an9820556@gmail.com
Jangka Waktu Kegiatan		: 1 Semester
Biaya Penelitian		: Rp. 3.000.000,-

Palangka Raya, 9 September 2024

Menyetujui,
Kepala UP3M

Rosmiati, M.Kom
NIK. 197810102005003

Ketua Peneliti

Amaya Andri Damaini, S.Kom., M.T
199309042018001

Mengetahui
Ketua STMIK Palangkaraya

Suparno ,M.Kom
NIK. 196901041995105

IDENTITAS DAN URAIAN UMUM

Judul Penelitian : Asesmen Tata Kelola Keamanan Teknologi Informasi STMIK Palangkaraya Menggunakan Indeks Keamanan Informasi Peneliti

No	Nama	Jabatan	Bidang keahlian	Instansi Asal	Alokasi Waktu (jam/Minggu)
1.	Amaya Andri Damaini, S.Kom., M.T	Ketua	Ilmu Komputer	STMIK Palangkaraya	5.0
2.	Abdul Hadi, ST. M.Kom	Anggota	Ilmu Komputer	STMIK Palangkaraya	5.0
3.	Elia Zakharia, M.T..	Anggota	Ilmu Komputer	STMIK Palangkaraya	5.0
4.	Herkules, S.Kom., M.Cs	Anggota	Ilmu Komputer	STMIK Palangkaraya	5.0
5.	Yoantri Et Devitsu	Anggota	Ilmu Komputer	STMIK Palangkaraya	5.0

1. Objek Penelitian

   Objek penelitian dari judul "Asesmen Tata Kelola Keamanan Teknologi Informasi STMIK Palangkaraya Menggunakan Indeks Keamanan Informasi (KAMI)" adalah tata kelola keamanan teknologi informasi di STMIK Palangkaraya. Penelitian ini berfokus pada analisis dan evaluasi kebijakan, prosedur, serta praktik keamanan teknologi informasi yang diterapkan di institusi tersebut.
2. Masa pelaksanaan

   Mulai : Juli 2024

   Berakhir : Januari 2025
3. Kebutuhan Biaya : Rp. 3.000.000,-
4. Lokasi penelitian :

   Lokasi penelitian di STMIK Palangkaraya.
5. Instansi lain yang terlibat:

   Tidak ada.

6. Temuan yang ditargetkan

   Hasil asesmen berupa tingkat kematangan keamanan TI di STMIK Palangkaraya dan memberikan rekomendasi yang jelas untuk perbaikan tata kelola keamanan TI, termasuk pengembangan kebijakan yang lebih komprehensif, peningkatan pelatihan dan kesadaran pengguna, serta pemantauan dan evaluasi yang lebih rutin terhadap sistem keamanan yang ada.

7. Kontribusi mendasar pada suatu bidang ilmu

   Penelitian ini memberikan kontribusi terhadap keilmuan dibidang keamanan informasi dan manajemen teknologi informasi.

8. Jurnal ilmiah yang menjadi sasaran

   Jurnal Saintekom : Sains, Teknologi, Komputer dan Manajemen

9. Rencana luaran HKI, buku, purwarupa atau luaran lainya yang ditargetkan, tahun rencana perolehan atau penyelesaiannya

   - Publikasi Ilmiah Jurnal Nasional Terakreditasi, Tahun ke-1 Target : submitted
   - Buku Ajar (ISBN), tahun ke-1 Target : Draft
   - Tingkat kesiapan Teknologi (TKT), tahun ke-1 Target skala 2

DAFTAR ISI

Halaman Judul i
Halaman Pengesahan ii
Identitas Dan Uraian Umum iv
Daftar Isi vi
Ringkasan Proposal vii
Daftar Gambar ix
Daftar Tabel x
BAB 1 PENDAHULUAN 1
1.1 Latar Belakang Masalah 1
1.2 Rumusan Masalah 3
1.3 Tujuan Penelitian 3
1.4 Manfaat penelitian 4
1.5 Target Luaran Penelitian 4
BAB 2 TINJAUAN PUSTAKA 5
2.1 Keamanan Informasi 5
2.2 Indeks Keamanan Informasi (KAMI) 8
BAB 3 METODE PENELITIAN 12
3.1 Waktu dan Tempat Penelitian 12
3.2 Alat dan Bahan Penelitian 13
3.3 Metode Penelitian 13
BAB 4 BIAYA DAN JADWAL PENELITIAN 15
4.1 Anggaran Biaya 15
4.2 Jadwal Penelitian 16
DAFTAR PUSTAKA 17

RINGKASAN PROPOSAL

Keamanan teknologi informasi (TI) merupakan isu krusial bagi institusi pendidikan tinggi, termasuk STMIK Palangkaraya, mengingat meningkatnya ancaman siber yang dapat mengganggu operasional dan merusak reputasi institusi. Penelitian ini bertujuan untuk melakukan asesmen tata kelola keamanan TI di STMIK Palangkaraya menggunakan Indeks Keamanan Informasi (KAMI). Dengan melakukan evaluasi terhadap kebijakan dan prosedur keamanan yang diterapkan, penelitian ini diharapkan dapat memberikan gambaran yang jelas mengenai kondisi keamanan saat ini dan mengidentifikasi area yang memerlukan perbaikan.

Metodologi penelitian yang digunakan adalah pendekatan deskriptif kualitatif dengan pengumpulan data melalui survei dan wawancara yang melibatkan pihak-pihak pengelola TIK di STMIK Palangkaraya. Indeks KAMI digunakan sebagai alat asesmen untuk mengevaluasi tingkat kematangan tata kelola keamanan TI, yang mencakup berbagai aspek seperti kebijakan, prosedur, pelatihan pengguna, dan infrastruktur TI. Data yang diperoleh kemudian dianalisis untuk mengidentifikasi kekuatan dan kelemahan dalam sistem keamanan yang ada.

Hasil penelitian diharapkan menunjukkan bahwa tingkat kematangan tata kelola keamanan TI di STMIK Palangkaraya. Penelitian ini juga diharapkan mengungkapkan kelemahan yang ada serta memberikan rekomendasi konkret untuk perbaikan, sehingga institusi dapat meningkatkan keamanan informasi dan melindungi aset-aset pentingnya dari ancaman yang semakin kompleks. Temuan ini diharapkan dapat menjadi acuan bagi institusi lain dalam mengembangkan strategi keamanan TI yang lebih efektif.

DAFTAR GAMBAR

Hal

Gambar 2.1 Contoh Hasil Indek KAMI.....11
Gambar 3.1 Flowchart Alur Penelitian 12

DAFTAR TABEL

Hal

Tabel 1.1. Rencana target Luaran 4
Tabel 3.1. Perangkat Jaringan 20
Tabel 4.1. Rincian Anggaran Biaya yang Direncanakan 15
Tabel 4.2. Jadwal Kegiatan Penelitian 16

BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Keamanan teknologi informasi (TI) telah menjadi salah satu pilar utama dalam menjaga kelangsungan dan kehandalan operasional berbagai organisasi, termasuk institusi pendidikan tinggi seperti Sekolah Tinggi Manajemen Informatika dan Komputer (STMIK) Palangkaraya. Dalam beberapa dekade terakhir, peran teknologi informasi dalam menunjang aktivitas akademik, administrasi, dan penelitian semakin meningkat secara eksponensial. STMIK Palangkaraya, sebagai lembaga yang berfokus pada bidang informatika dan komputer, memiliki ketergantungan yang sangat tinggi terhadap infrastruktur TI untuk mendukung proses pembelajaran, penyimpanan data akademik, serta pengelolaan informasi strategis. Infrastruktur ini mencakup jaringan komunikasi, server penyimpanan data, sistem manajemen basis data, hingga berbagai perangkat lunak yang digunakan dalam operasional sehari-hari.

Namun, dengan kemajuan teknologi yang pesat, muncul tantangan baru berupa ancaman-ancaman keamanan yang semakin canggih dan kompleks. Serangan siber, seperti peretasan, malware, ransomware, dan phishing, telah berkembang menjadi ancaman serius yang dapat merusak integritas, kerahasiaan, dan ketersediaan data (Paramita et al., 2022). Salah satu contoh insiden terjadinya pemalsuan akun whatsApp yang terjadi dilingkung STMIK Palangkaraya, sipelaku kejahatan mengganti foto profil yang menyerupai orang yang dikenal oleh korban dan mengirim pesan palsu kepada rekan kerja dengan menyebutkan nama lengkap si korban. Tujuannya adalah untuk menipu korban agar percaya bahwa mereka sedang berkomunikasi dengan orang yang sebenarnya, padahal akun tersebut dikendalikan oleh pelaku, berdasar insiden ini dapat diidentifikasi adanya kebocoran data identitas korban.

Dalam konteks pendidikan tinggi, insiden keamanan ini tidak hanya dapat menyebabkan kerugian finansial yang signifikan, tetapi juga dapat mengancam privasi data mahasiswa, merusak reputasi institusi, serta menghambat kelancaran proses akademik dan administratif (Aji, 2023). Selain itu, kebijakan keamanan yang tidak memadai, kurangnya kesadaran pengguna terhadap risiko keamanan, serta kelemahan dalam implementasi prosedur keamanan, sering kali menjadi celah yang dapat dimanfaatkan oleh pihak-pihak yang tidak bertanggung jawab (Evan Alfian Syahnur et al., 2022).

Di sisi lain, pentingnya tata kelola keamanan TI yang baik merupakan prasyarat utama untuk memastikan bahwa STMIK Palangkaraya dapat beroperasi secara efektif dan aman. Tata kelola ini mencakup berbagai aspek, mulai dari pengelolaan risiko, kepatuhan terhadap regulasi dan standar keamanan, hingga pemantauan dan evaluasi berkala terhadap sistem keamanan yang diterapkan (Khusna & Sugiantoro, 2023). Namun, untuk mencapai tata kelola yang efektif, diperlukan pemahaman yang mendalam mengenai kondisi keamanan saat ini dan identifikasi terhadap potensi risiko yang ada (Jauhary et al., 2022). Dalam hal ini, metode penilaian atau asesmen yang komprehensif sangat diperlukan untuk mengukur sejauh mana kebijakan dan prosedur keamanan yang ada mampu menghadapi ancaman yang ada (Khusna & Sugiantoro, 2023).

Indeks Keamanan Informasi (KAMI) merupakan salah satu alat yang dapat digunakan untuk melakukan asesmen ini. Indeks ini menyediakan kerangka kerja yang sistematis dan terstruktur untuk menilai tingkat kematangan tata kelola keamanan informasi dalam suatu organisasi (Savitri et al., 2024; Tawar et al., 2022). Alasan Penulis menggunakan Indeks Keamanan Informasi, STMIK Palangkaraya karena adaptif terhadap kebutuhan institusi termasuk institusi pendidikan, pemerintahan atau perusahaan skala nasional sehingga mengidentifikasi kelemahan-kelemahan dalam sistem keamanan secara komprehensif, penilian standar yang terukur, meningkatkan efektivitas tata kelola TI, serta menentukan langkah-langkah

perbaikan yang diperlukan untuk meningkatkan keamanan informasi secara menyeluruh. Penelitian ini bertujuan untuk melakukan asesmen terhadap tata kelola keamanan TI di STMIK Palangkaraya dengan menggunakan Indeks Keamanan Informasi versi 5, yang diharapkan dapat memberikan panduan bagi institusi dalam mengembangkan strategi keamanan yang lebih tangguh dan berkelanjutan di masa depan.

Melalui penelitian ini, diharapkan tidak hanya memberikan gambaran mengenai kondisi tata kelola keamanan TI saat ini, tetapi juga menghasilkan rekomendasi praktis yang dapat diimplementasikan untuk memperkuat sistem keamanan informasi di STMIK Palangkaraya. Mengingat pentingnya keamanan informasi dalam menjaga kelangsungan operasional dan reputasi lembaga, hasil penelitian ini diharapkan dapat menjadi dasar bagi pengambilan keputusan strategis dalam bidang keamanan TI, serta berkontribusi terhadap pengembangan kebijakan keamanan yang lebih baik di lingkungan pendidikan tinggi.

1.2 Rumusan Masalah

Berdasarkan penjabaran dalam latar belakang, maka Penulis merumuskan masalah yaitu bagaimana asesmen kondisi tata kelola keamanan teknologi informasi di STMIK Palangkaraya dengan menggunakan Indeks KAMI dengan tujuh parameter penilian yaitu aspek tata kelola, aspek pengelolaan risiko, aspek kerangka kerja keamanan informasi, aspek pengelolaan aset, aspek teknologi dan keanaman informasi, aspek perlindungan data pribadi dan aspek pengamanan keterlibatan pihak ketiga.

1.3 Tujuan Penelitian

Penelitian ini bertujuan untuk mengidentifikasi dan mengevaluasi efektivitas tata kelola keamanan teknologi informasi di STMIK Palangkaraya dengan menggunakan Indeks KAMI. Penelitian ini berfokus pada bagaimana tata kelola saat ini menghadapi ancaman keamanan, serta mengidentifikasi kelemahan dan kekuatan yang ada. Hasil asesmen ini diharapkan dapat memberikan rekomendasi tingkat kesiapan seperti pada Gambar 2.1 sehingga

dapat mengevaluasi dan meningkatkan keamanan informasi di institusi tersebut.

1.4 Manfaat penelitian

Penelitian ini memiliki manfaat penting dalam memberikan pemahaman yang mendalam mengenai kondisi aktual tata kelola keamanan teknologi informasi di STMIK Palangkaraya. Dengan menggunakan indek KAMI, penelitian ini akan membantu institusi dalam mengidentifikasi area-area yang memerlukan perbaikan dan meningkatkan kesadaran terhadap potensi risiko keamanan yang mungkin belum sepenuhnya diantisipasi. Selain itu, hasil asesmen ini dapat digunakan sebagai dasar untuk merumuskan kebijakan dan strategi keamanan yang lebih efektif, sehingga dapat memperkuat perlindungan terhadap data dan infrastruktur teknologi informasi yang krusial bagi operasional akademik dan administratif.

Manfaat lainnya adalah bahwa hasil penelitian ini dapat digunakan sebagai acuan oleh institusi pendidikan lain yang memiliki karakteristik serupa dalam upaya mereka meningkatkan tata kelola keamanan teknologi informasi. Dengan demikian, penelitian ini tidak hanya memberikan nilai bagi STMIK Palangkaraya, tetapi juga dapat berkontribusi secara lebih luas dalam pengembangan praktik keamanan informasi di lingkungan pendidikan tinggi.

1.5 Target Luaran Penelitian

Rencana target luaran yang akan dicapai dalam penelitian ini terdiri dari beberapa jenis, sebagaimana Tabel 1.1.

Tabel 1.1. Rencana target Luaran

No	Jenis Luaran		Indikator Capaian
1	Publikasi Ilmiah di Jurnal Nasional (ber ISSN)		Accepted
2	Pemakalah dalam temu ilmiah	Nasional	Draf
		Lokal	Tidak ada
3	Bahan Ajar		Proses Penulisan
4	Luaran Lainya jika ada (teknologi Tepat Guna , model/Desain/karya Seni/ Rekayasa Sosial)		Tidak ada
5	Tingkat Kesiapan Teknologi (TKT)		2

BAB 2
TINJAUAN PUSTAKA

2.1 Keamanan Informasi

Keamanan informasi adalah bidang yang berkembang pesat dan sangat penting di era digital ini. Konsep keamanan informasi mencakup berbagai prinsip, praktik, dan teori yang dirancang untuk melindungi informasi dari ancaman yang bisa merusak, mencuri, atau mengungkapkan data tanpa izin. Karena informasi menjadi salah satu aset paling berharga bagi individu, perusahaan, dan pemerintah, keamanan informasi menjadi sangat krusial.

Pada dasarnya, keamanan informasi berfokus pada tiga prinsip utama yang dikenal sebagai CIA Triad: kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) (Vansuri et al., 2023). Kerahasiaan memastikan bahwa informasi hanya dapat diakses oleh orang-orang yang memiliki otorisasi. Ini berarti data yang sensitif, seperti informasi keuangan atau data pribadi, harus dilindungi agar tidak jatuh ke tangan yang salah. Teknik yang umum digunakan untuk menjaga kerahasiaan termasuk enkripsi, yang mengubah informasi menjadi bentuk kode yang hanya bisa dibaca oleh orang yang memiliki kunci dekripsi, serta kontrol akses yang membatasi siapa saja yang bisa melihat atau mengubah data.

Integritas adalah aspek yang memastikan bahwa informasi tetap akurat dan tidak diubah oleh pihak yang tidak berwenang. Ini sangat penting untuk menjaga kepercayaan terhadap data yang digunakan dalam berbagai keputusan bisnis atau pribadi. Tanpa integritas, informasi yang salah bisa menyebabkan kerugian besar. Teknik yang digunakan untuk menjaga integritas termasuk hash functions, yang memeriksa apakah data telah diubah, dan tanda tangan digital, yang memastikan keaslian dan keutuhan data.

Ketersediaan adalah prinsip yang memastikan bahwa informasi dapat diakses oleh pihak yang berwenang saat dibutuhkan. Tanpa ketersediaan, bahkan informasi yang paling aman pun tidak akan berguna. Serangan siber

seperti Denial of Service (DoS), yang membuat sistem tidak dapat diakses oleh pengguna sah, adalah ancaman utama terhadap ketersediaan. Oleh karena itu, sistem yang dirancang dengan baik harus mencakup mekanisme pemulihan bencana dan backup data untuk memastikan ketersediaan informasi bahkan dalam situasi darurat.

Ancaman terhadap keamanan informasi dapat datang dari berbagai sumber, baik dari dalam maupun luar organisasi. Ancaman internal sering kali melibatkan orang dalam organisasi, seperti karyawan atau kontraktor, yang memiliki akses ke sistem informasi. Mereka bisa saja secara sengaja atau tidak sengaja menyebabkan kebocoran atau kerusakan data. Ancaman eksternal, di sisi lain, biasanya datang dari hacker, malware, atau penyerang lainnya yang mencoba mengakses informasi secara ilegal. Misalnya, serangan phishing sering digunakan oleh penyerang untuk menipu pengguna agar membocorkan informasi sensitif seperti kata sandi atau detail kartu kredit.

Selain ancaman teknis, serangan sosial atau social engineering adalah metode yang digunakan penyerang untuk memanipulasi orang agar membocorkan informasi rahasia. Ini bisa melibatkan penyerang yang berpura-pura menjadi petugas dukungan teknis atau pihak berwenang lainnya untuk mendapatkan akses ke informasi yang dilindungi. Oleh karena itu, pendidikan dan pelatihan keamanan bagi karyawan menjadi salah satu langkah penting dalam menjaga keamanan informasi.

Untuk membantu dalam implementasi keamanan informasi, berbagai model keamanan telah dikembangkan. Salah satu model dasar yang sering digunakan adalah model CIA Triad yang sudah dibahas sebelumnya. Model lain yang dikenal adalah Bell-LaPadula yang fokus pada menjaga kerahasiaan informasi, terutama dalam konteks militer. Model ini menggunakan hierarki keamanan untuk mengatur siapa saja yang bisa mengakses data berdasarkan tingkat sensitivitasnya. Ada juga model Biba, yang lebih fokus pada integritas informasi. Model ini memastikan bahwa informasi dengan tingkat integritas yang lebih tinggi tidak bisa diubah oleh entitas dengan tingkat yang lebih rendah. Sementara itu, model Clark-Wilson adalah model yang dirancang

untuk menjaga integritas dalam lingkungan bisnis dengan menggunakan konsep seperti well-formed transactions dan separation of duties untuk mencegah manipulasi data yang tidak sah.

Selain model-model tersebut, ada juga berbagai standar dan kerangka kerja yang digunakan oleh organisasi untuk mengelola keamanan informasi. Salah satu standar internasional yang paling terkenal adalah ISO/IEC 27001, yang menyediakan pedoman untuk membangun, mengimplementasikan, memelihara, dan terus meningkatkan Sistem Manajemen Keamanan Informasi (ISMS) (Al Faruq, 2020; Jauhary et al., 2022). Standar ini menggunakan pendekatan berbasis risiko untuk mengelola dan melindungi informasi, dan merupakan acuan penting bagi banyak organisasi di seluruh dunia.

Di Amerika Serikat, NIST Cybersecurity Framework yang dikembangkan oleh National Institute of Standards and Technology (NIST) juga merupakan alat penting bagi organisasi dalam mengelola dan mengurangi risiko keamanan informasi. Kerangka kerja ini dibagi menjadi lima fungsi utama: Identify, Protect, Detect, Respond, dan Recover, yang memberikan panduan komprehensif untuk keamanan informasi (Mahendra & Soewito, 2023). Kerangka kerja lain yang juga digunakan adalah COBIT (Control Objectives for Information and Related Technologies), yang berfokus pada tata kelola dan pengelolaan risiko TI, termasuk keamanan informasi (Ardi Prasetyo & Melkior N.N. Sitokdana, 2021; Wawondatu, 2020).

Namun, keamanan informasi bukanlah sesuatu yang statis; tantangan baru terus bermunculan seiring dengan perkembangan teknologi. Munculnya teknologi baru seperti cloud computing, Internet of Things (IoT), dan kecerdasan buatan (AI) membawa ancaman baru yang harus diantisipasi. Misalnya, perangkat IoT sering kali kurang aman dan dapat menjadi pintu masuk bagi penyerang untuk mengakses jaringan yang lebih luas. Oleh karena itu, pendekatan keamanan harus terus berkembang untuk mengatasi ancaman-ancaman ini.

Selain itu, banyak negara dan industri memiliki regulasi yang ketat terkait keamanan informasi, seperti General Data Protection Regulation (GDPR) di Uni Eropa, yang mengatur bagaimana data pribadi harus dilindungi dan dikelola. Organisasi harus memastikan bahwa mereka tidak hanya melindungi informasi mereka, tetapi juga mematuhi berbagai regulasi ini, yang bisa menjadi tantangan tersendiri.

Dalam menghadapi semua tantangan ini, organisasi harus menerapkan praktik terbaik dalam keamanan informasi, seperti melakukan audit keamanan secara berkala, mengedukasi karyawan tentang ancaman keamanan, dan mengadopsi teknologi keamanan terbaru. Dengan demikian, mereka dapat mengurangi risiko yang terkait dengan keamanan informasi dan melindungi aset informasi mereka dengan lebih baik.

2.2 Indeks Keamanan Informasi (KAMI)

Indeks KAMI adalah alat evaluasi untuk menganalisa tingkat kesiapan pengamanan informasi di suatu organisasi. Alat evaluasi ini tidak ditujukan untuk menganalisa kelayakan atau efektifitas bentuk pengamanan yang ada, melainkan sebagai perangkat untuk memberikan gambaran kondisi kesiapan (kelengkapan dan kematangan) kerangka kerja keamanan informasi kepada pimpinan Instansi/Perusahaan (Savitri et al., 2024). Evaluasi dilakukan terhadap berbagai area yang menjadi target penerapan keamanan informasi dengan ruang lingkup pembahasan yang juga memenuhi semua aspek keamanan yang didefinisikan oleh standar ISO/IEC 27001:2013.

Bentuk evaluasi yang diterapkan dalam indeks KAMI dirancang untuk dapat digunakan oleh suatu organisasi dari berbagai tingkatan, ukuran, maupun tingkat kepentingan penggunaan TIK dalam mendukung terlaksananya proses yang ada. Data yang digunakan dalam evaluasi ini nantinya akan memberikan snapshot indeks kesiapan - dari aspek kelengkapan maupun kematangan - kerangka kerja keamanan informasi yang diterapkan dan dapat digunakan sebagai pembanding dalam rangka menyusun langkah perbaikan dan penetapan prioritasnya.

Alat evaluasi ini kemudian bisa digunakan secara berkala untuk mendapatkan gambaran perubahan kondisi keamanan informasi sebagai hasil dari program kerja yang dijalankan, sekaligus sebagai sarana untuk menyampaikan peningkatan kesiapan kepada pihak yang terkait (*stakeholders*)(Tawar et al., 2022).

Khusus untuk Instansi Pemerintah, penggunaan dan publikasi hasil evaluasi Indeks KAMI merupakan bentuk tanggungjawab penggunaan dana publik sekaligus menjadi sarana untuk meningkatkan kesadaran mengenai kebutuhan keamanan informasi. Pertukaran informasi dan diskusi dengan Instansi pemerintah lainnya sebagai bagian dari penggunaan alat evaluasi Indeks KAMI ini juga menciptakan alur komunikasi antar pengelola keamanan informasi di sektor pemerintah sehingga semua pihak dapat mengambil manfaat dari lesson learned yang sudah dilalui.

Alat evaluasi Indeks KAMI ini dapat digunakan oleh organisasi dengan skala nasional, maupun yang berukuran kecil. Penggunaan di Instansi pemerintah dapat dilakukan di tingkat pusat maupun satuan kerja yang ada di tingkatan Direktorat Jenderal, Badan, Pusat atau Direktorat untuk mendapatkan gambaran mengenai kematangan program kerja keamanan informasi yang dijalankannya. Evaluasi ini dianjurkan untuk dilakukan oleh pejabat yang secara langsung bertanggungjawab dan berwenang untuk mengelola keamanan informasi di seluruh cakupan instansinya.

Proses evaluasi dilakukan melalui sejumlah pertanyaan di masing-masing area di bawah ini:

- Kategori Sistem Elektronik yang digunakan Instansi
- Tata Kelola Keamanan Informasi
- Pengelolaan Risiko Keamanan Informasi
- Kerangka Kerja Keamanan Informasi
- Pengelolaan Aset Informasi, dan

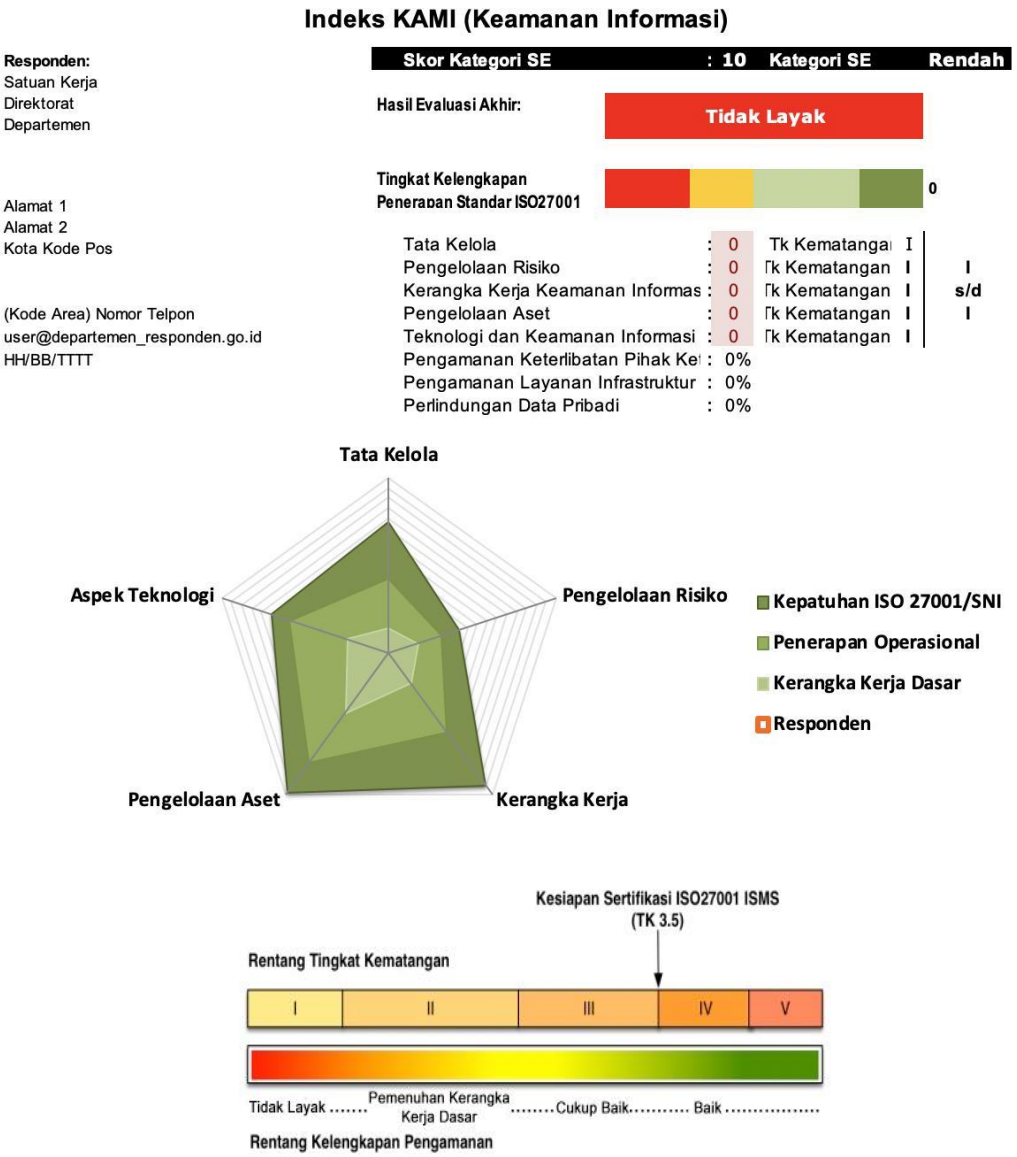
- Teknologi dan Keamanan Informasi

- Suplemen: area evaluasi untuk aspek pengamanan keterlibatan pihak ketiga penyedia layanan, pengamanan layanan infrastruktur awan (*cloud service*) dan perlindungan data pribadi.

Pertanyaan yang ada belum tentu dapat dijawab semuanya, akan tetapi yang harus diperhatikan adalah jawaban yang diberikan harus merefleksikan kondisi penerapan keamanan informasi sesungguhnya. Alat evaluasi ini hanya akan memberikan nilai tambah bagi semua pihak apabila pengisiannya menggunakan asas keterbukaan dan kejujuran.

Sebelum mulai menjawab pertanyaan terkait kesiapan pengamanan informasi, responden diminta untuk mendefinisikan Kategori Sistem Elektronik di Instansinya. Definisi ini bisa dijabarkan untuk tingkat Satuan Kerja baik di tingkat Kementerian/Lembaga, ataupun untuk satuan kerja yang lebih kecil, sampai ke Unit Eselon III. Responden juga diminta untuk mendeskripsikan infrastruktur TIK yang ada dalam satuan kerjanya secara singkat. Tujuan dari proses ini adalah untuk mengelompokkan Sistem Elektronik yang digunakan instansi ke "tingkat" tertentu: Rendah, Tinggi dan Strategis. Dengan pengelompokan ini nantinya bisa dilakukan pemetaan terhadap instansi yang mempunyai karakteristik Sistem Elektornik yang sama.

Pertanyaan dikelompokkan untuk 2 keperluan. Pertama, pertanyaan dikategorikan berdasarkan tingkat kesiapan penerapan pengamanan sesuai dengan kelengkapan kontrol yang diminta oleh standar ISO/IEC 27001:2013. Dalam pengelompokan ini responden diminta untuk memberi tanggapan mulai dari area yang terkait dengan bentuk kerangka kerja dasar keamanan informasi (pertanyaan diberi label "1"), efektifitas dan konsistensi penerapannya (label "2"), sampai dengan kemampuan untuk selalu meningkatkan kinerja keamanan informasi (label "3"). Tingkat terakhir ini sesuai dengan kesiapan minimum yang diprasyaratkan oleh proses sertifikasi standar ISO/IEC 27001:2013. Berikut Gambar 1 contoh hasil indek KAMI.



Gambar 2.1 Contoh hasil indek KAMI

Tingkat kematangan pada Gambar 2.1 didefinisikan sebagai:

a. Tingkat I - Kondisi Awal
b. Tingkat II - Penerapan Kerangka Kerja Dasar
c. Tingkat III - Terdefinisi dan Konsisten
d. Tingkat IV - Terkelola dan Terukur
e. Tingkat V - Optimal

BAB 3
METODOLOGI

Metodologi yang digunakan dalam penelitian ini adalah metode deskriptif kualitatif yang berfokus pada penerapan Indeks Keamanan Informasi (KAMI). Pendekatan ini bertujuan untuk menggambarkan dan menganalisis tingkat kesiapan dan keamanan informasi dalam sebuah organisasi secara mendalam, tanpa mengandalkan data numerik atau statistik semata. Melalui analisis deskriptif kualitatif ini, penelitian dapat menghasilkan pemahaman yang komprehensif tentang kondisi keamanan informasi dalam organisasi yang diteliti, serta memberikan rekomendasi yang lebih relevan dan kontekstual untuk meningkatkan keamanan informasi di masa mendatang.

Dengan menggunakan metode deskriptif kualitatif, penelitian ini tidak hanya mengukur atau menilai aspek-aspek keamanan informasi berdasarkan parameter yang sudah ditetapkan dalam Indeks KAMI, tetapi juga berusaha memahami konteks dan dinamika yang mempengaruhi hasil tersebut. Ini mencakup eksplorasi terhadap kebijakan, praktik, dan budaya keamanan informasi di dalam organisasi, serta bagaimana berbagai faktor internal dan eksternal mempengaruhi penerapan keamanan informasi.

Data yang dikumpulkan dalam penelitian ini mungkin mencakup wawancara dengan personel yang bertanggung jawab atas keamanan informasi, analisis dokumen kebijakan dan prosedur, serta observasi terhadap implementasi kontrol keamanan di lapangan. Pendekatan kualitatif memungkinkan peneliti untuk mendapatkan wawasan yang lebih kaya dan mendalam mengenai tantangan, hambatan, dan peluang yang ada dalam upaya pengelolaan keamanan informasi.

3.1 Waktu dan Tempat Penelitian

Penelitian dilaksanakan mulai dari bulan September 2024 sampai dengan Januari 2025 dengan melibatkan Dosen, Mahasiswa dan stakeholder STMIK Palangkaraya. Lokasi penelitian berada di Jl. G. Obos No.114, Menteng, Kec. Jekan Raya, Kota Palangka Raya, Kalimantan Tengah 74874

3.2 Alat dan Bahan Penelitian

Alat dan bahan yang diperlukan mencakup beberapa komponen penting untuk mendukung proses pengumpulan data, analisis, dan evaluasi keamanan teknologi informasi di institusi tersebut. Alat penelitian yang digunakan berupa aplikasi excel yang didalamnya sudah terintegrasi perhitungan indek KAMI.

Sedangkan bahan penelitian berupa data primer yang diambil dari dari sumber utama melalui kuesioner, wawancara, dan observasi. Data ini mencakup tanggapan dari staf TI, manajemen, dan pihak lain yang terlibat dalam tata kelola keamanan informasi di STMIK Palangkaraya. Data sekunder diperoleh dari sumber yang sudah ada, seperti laporan tahunan, audit keamanan, publikasi penelitian sebelumnya, dan dokumentasi kebijakan. Data ini akan digunakan untuk melengkapi dan memperkuat analisis yang dilakukan.

3.3 Metode Penelitian

Tahapan penelitian dimulai dari persiapan, desain penelitian, analisis data, dan penyusunan laporan. Seperti alur penelitian pada Gambar 3.1.



Gambar 3.1 Alur Penelitian

Tahapan persiapan, peneliti melakukan telaah dokumen bisnis dan studi literatur yaitu dokumen TIK STMIK Palangkaraya dan dokumen hasil audit sistem informasi juga melakukan pencarian dasar-dasar teori dan penemuan dari penelitian yang telah dilakukan sebelumnya. Keluaran yang didapatkan

dari tahap persiapan yaitu identifikasi permasalahan TIK yang ada di STMIK Palangkaraya.

Pada tahapan desain penelitian, peneliti melakukan identifikasi organisasi dan penilaian INDEKS KAMI. Identifikasi organisasi berisi tentang visi, misi, struktur organisasi, rencana strategis STMIK Palangkaraya tentang TIK Dan laporan hasil audit. Indeks KAMI dapat mengevaluasi penerapan tata kelola keamanan informasi yang dilakukan secara berkelanjutan, dan digunakan untuk memberikan gambaran kemajuan hasil penerapan secara berkala. Keluaran yang di dapatkan dari tahap desain penelitian yaitu hasil kuisioner, wawancara dan batasan masalah.

Pada tahapan pengumpulan dan analisa data, peneliti menentukan sampel dan teknik analisis data yang diperlukan seperti kategori sistem elektronik yang digunakan instansi, tata kelola keamanan informasi, pengelolaan risiko keamanan informasi, kerangka kerja keamanan informasi, pengelolaan aset informasi, teknologi dan keamanan informasi, dan suplemen yaitu area evaluasi untuk aspek pengamanan keterlibatan pihak ketiga penyedia layanan, pengamanan layanan infrastruktur awan (*cloud service*) dan perlindungan data pribadi. Populasi dalam penelitian ini adalah pengelola TIK STMIK Palangkaraya. Keluaran dari tahap ini adalah nilai tingkat kematangan dan saran rekomendasi untuk tingkat kelengkapan pengamanan dan tingkat kematangan pengamanan. Adapun isi assesmen tertuang pada Indeks KAMI pada url berikut https://cloud.bssn.go.id/s/r8Sgwqb4JF8442Z

Pada tahap yang terakhir yaitu penyusunan laporan, peneliti memasukan *draft* hasil penelitian kedalam laporan. Keluaran dari tahapan ini yaitu laporan hasil penelitian, jurnal ilmiah, poster penelitian, dan presentasi hasil penelitian.

Berdasar penggunaan pada panduan Indeks Kami, institusi sebaiknya melakukan sebanyak dua kali dalam setahun untuk melakukan tinjauan ulang kesiapan keamanan informasi sekaligus untuk mengukur keberhasilan inisiatif perbaikan yang diterapkan, dengan pencapaian tingkat kelengkapan atau kematangan tertentu.

BAB 4
BIAYA DAN JADWAL PENELITIAN

4.1 Anggaran Biaya

Justifikasi anggaran biaya yang digunakan dalam penelitian ini dirincikan pada Tabel 4.1.

Tabel 4.1. Rincian Anggaran Biaya yang Direncanakan

1. Honorarium				
Honor	Honor/ Jam (Rp)	Waktu (jam/minggu)	Minggu	Honor Per Tahun (RP)
Pengumpul data	Rp 6.000	5	24	Rp 720.000
Pengolah data	Rp 9.000	5	24	Rp 1.080.000
Peyusunan laporan	Rp 8.000	5	24	Rp 960.000
			Subtotal (Rp)	Rp 2.760.000
2. Penggandaan				
Penggandaan	Justifikasi Penggandaan	Kuantitas	Harga Satuan (Rp)	Harga peralatan penunjang (Rp)
Print proposal dan laporan	100 Lembar	100	Rp 1.000	Rp 100.000
Foto copy	100 lbr x 5 eksemplar	100	Rp 200	Rp 100.000
Jilid proposal dan laporan	5 Eksemplar	5	Rp 6.000	Rp 30.000
			Subtotal (Rp)	Rp 240.000
3. Lain-lain				
Material	Justifikasi	Kuantitas	Harga Satuan (Rp)	Biaya per Tahun (Rp)
Materai	1	1	Rp 10.000	Rp 10.000
			Subtotal (Rp)	Rp 10.000
			Total Anggaran Yang Diperlukan (Rp)	Rp 3.000.000

4.2 Jadwal Penelitian

Kegiatan Penelitian hingga penyusunan laporan direncanakan selama dua bulan dimulai dari bulan September pada tahun 2024 dengan tahapan kegiatan dan jadwal pelaksanaan penelitian diuraikan pada Tabel 4.2.

Tabel 4.2. Jadwal Kegiatan Penelitian

No	Kegiatan	**Bulan ke-Tahun 2024**					**Bulan ke-Tahun 2025**
		8	**9**	**10**	**11**	**12**	**1**
1	Persiapan						
2	Desain penelitian						
3	Pengumpulan Data						
4	Analisis Data						
5	Penyusunan Laporan						

DAFTAR PUSTAKA

Aji, M. P. (2023). Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi) [Cyber Security System and Data Sovereignty in Indonesia in Political Economic Perspective]. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional*, *13*(2), 222–238. https://doi.org/10.22212/jp.v13i2.3299

Al Faruq, B. (2020). Integration of ITIL V3, ISO 20000 & ISO 27001:2013forIT Services and Security Management System. *International Journal of Advanced Trends in Computer Science and Engineering*, *9*(3), 3514–3531. https://doi.org/10.30534/ijatcse/2020/157932020

Ardi Prasetyo, T. M. & Melkior N.N. Sitokdana. (2021). Analisis Tata Kelola Pusat Data dan Informasi Kementerian XYZ Menggunakan COBIT 2019. *Journal of Applied Computer Science and Technology*, *2*(2), 95–107. https://doi.org/10.52158/jacost.v2i2.265

Evan Alfian Syahnur, Hibrizi, M. N. F., Lesmana, R. K., & Irawan, M. D. (2022). Analisis Manajemen Risiko Keamanan Informasi di PT. Adhi Commuter Properti Medan Menggunakan Standart ISO 31000:2018 (Studi Kasus Hotel Grandhika Medan). *Balance : Jurnal Akuntansi dan Manajemen*, *1*(3), 330–338. https://doi.org/10.59086/jam.v1i3.219

Jauhary, H., Pratiwi2, G. E., Salim, A. Z., & Fitroh, F. (2022). Penerapan ISO27001 dalam Menjaga dan Meminimalisir Risiko Keamanan Informasi: Literatur Review. *Media Jurnal Informatika*, *14*(1), 43. https://doi.org/10.35194/mji.v14i1.1581

Khusna, T. N., & Sugiantoro, B. (2023). PENGUKURAN TINGKAT KEAMANAN INFORMASI PADA UPT-PSI UNIVERSITAS MURIA KUDUS BERDASARKAN INDEKS KEAMANAN INFORMASI (KAMI) VERSI 4.2. *JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)*, *8*(3), 847–856. https://doi.org/10.29100/jipi.v8i3.3720

Mahendra, V., & Soewito, B. (2023). Penerapan Kerangka Kerja NIST Cybersecurity dan CIS Controls sebagai Manajemen Risiko Keamanan Siber. *Techno.Com*, *22*(3), 527–538. https://doi.org/10.33633/tc.v22i3.8491

Paramita, S., Siregar, S. A., Damanik, R. A., & Dedi Irawan, M. (2022). Analisis Manejemen Resiko Keamanan Data Sistem Informasi Berdasarkan Indeks Keamanan Informasi (KAMI) ISO 27001:2013. *Bulletin of Information Technology (BIT)*, *3*(4), 374–379. https://doi.org/10.47065/bit.v3i4.421

Savitri, R., Firmansyah, Dworo, & Said Hasibuan, M. (2024). Information Security Measurement using INDEX KAMI at Metro City. *Journal of Applied Data Sciences*, *5*(1), 33–45. https://doi.org/10.47738/jads.v5i1.152

Tawar, Imam Riadi, Adiniah Gustika Pratiwi, & Ariqah Adliana Siregar. (2022). Assessment and Mitigation of Information Security Policy in Budgeting System using KAMI Index 4.1. *Journal of Novel Engineering Science and Technology*, *1*(01), 24–29. https://doi.org/10.56741/jnest.v1i01.57

Vansuri, R., Fauzi, A., Prasetyo, E. T., Negara, R., Restu, A. M., & Firmansyah, R. R. (2023). *Peran CIA (Confidentiality, Integrity, Availability) Terhadap Manajemen Keamanan Informasi*. *2*(1).

Wawondatu, A. R. S. (2020). *Penggabungan Klausul dari Framework ISO/IEC 20000 dan COBIT 5.0 DSS06 dalam Analisis Layanan Teknologi Informasi di Universitas X*. *2*.

Lampiran 1. Susunan organisasi tim peneliti dan pembagian tugas

No	Nama	Bidang keahlian	Instansi Asal	Alokasi Waktu (jam/Minggu)	Uraian Tugas
1.	Amaya Andri Damaini, S.Kom., M.T	Ketua	Ilmu Komputer	5.0	Menyiapkan Kuesioner/wawancara, saran dan rekomendasi
2.	Abdul Hadi, ST. M.Kom	Anggota	Ilmu Komputer	5.0	Penyusunan Laporan, saran dan rekomendasi
3.	Elia Zakharia, M.T..	Anggota	Ilmu Komputer	5.0	Pengumpulan data, Penlialain indek kami
4.	Herkules, S.Kom., M.Cs	Anggota	Ilmu Komputer	5.0	Penilaian indek kami, analisis data
5.	Yoantri Et Devitsu	Anggota	Ilmu Komputer	5.0	Pengumpulan data

Lampiran 2. Biodata ketua dan anggota tim peneliti

A. Identitas Diri Ketua Pelaksana

1	Nama Lengkap	Amaya Andri Damaini, S.Kom., M.T
2	Jenis Kelamin	Perempuan
3	Jabatan Fungsional	Asisten Ahli
4	NIK	199309042018001
5	NIDN	1104099301
6	Tempat dan Tanggal Lahir	Palangka Raya, 04 September 1993
7	E-mail	amayaandridamaini@gmail.com
8	Nomor Telepon/HP	0852-4836-7262
9	Alamat Kantor	Jl. G. Obos No. 114
10	Nomor Telepon / Faks	0536-3224593
11	Lulusan yang Telah Dihasilkan	S1 =12 orang
12	Mata Kuliah yang diampu	1. Multimedia
		2. Sistem Operasi
		3. Arsitektur dan Organisasi Komputer

B. Riwayat Pendidikan

	S-1	S-2
Nama Perguruan Tinggi	STMIK Palangkaraya	Universitas Atma Jaya Yogyakarta
Bidang Ilmu	Teknik Informatika	Big data & Machine Learning
Tahun Masuk-Lulus	2011-2015	2016-2018
Judul Skripsi/Tesis/ Disertasi	Aplikasi Penentu Kebutuhan Gizi Harian berbasis *Mobile Android*	Transliterasi Aksara Jawa kedalam Huruf Latin menggunakan *Pseudo Zernike Moment* dan *Multi-Class Support Vector Machine*
Nama Pembimbing	1. Herkules, S.Kom., M.Cs 2. Drs. Sartana, M. Si	1. Dr. Pranowo ST., MT. 2. Ir. A. Djoko Budiyanto SHR, M.Eng., Ph.D

C. Pengalaman Penelitian Dalam 5 Tahun Terakhir

No	Tahun	Judul Penelitian	Pendanaan	
			Sumber	Jumlah (Rp)
1	2020	Penggunaan Rapid Application Development Pada Perancangan Informasi Akademik Program Studi Teknik Informatika STMIK Palangkaraya	STMIK Palangkaraya	Rp 3.000.000

2	2020	Rancang Bangun Sistem Informasi Kerajinan Tangan Khas Kalimantan Tengah	STMIK Palangkaraya	Rp 6.985.000

D. Pengalaman Pengabdian Kepada Masyarakat dalam 5 Tahun Terakhir

No	Tahun	Judul Pengabdian Kepada Masyarakat	Pendanaan	
			Sumber	Jumlah (Rp)
1	2019	Analisi Penerapan SIKD pada Dinas Pemuda dan Olahraga (DISPORA) Provinsi Kalimantan Tengah	STMIK Palangkaraya	Rp 3.000.000
2	2023	Penerapan Penggunaan Aplikasi Try Out Berbasis Android Di MI Nur Syafa'at Desa Pundu Kecamatan Cempaga Hulu Kabupaten Kotawaringin Timur.	STMIK Palangkaraya	Rp 3.000.000
3	2023	Sosialisasi Dampak Bahaya Penggunaan Smartphone Terhadap Anak-Anak TK Risten Rehobot Palangka Raya	STMIK Palangkaraya	Rp 1.500.000

E. Publikasi Artikel Ilmiah Dalam Jurnal dalam 5 Tahun Terakhir

No	Judul Artikel Ilmiah	Nama Jurnal	Volume/ Nomor/Tahun
1	Penggunaan Rapid Application Development Pada Perancangan Informasi Akademik Program Studi Teknik Informatika STMIK Palangkaraya	Jurnal Prodi Teknik Informatika UNW "Multimatrix"	Vol II/No. 2/2020
2	Penerapan Aplikasi Try Out Berbasis Android di MI Nur Syafa'at Desa Pundu Kecamatan Cempaga Hulu Kabupaten Kotawaringin Timur.	Jurnal Pengabdian Masyarakat Mitra Kreasi Cendekia (MKC)	Vol 1/No. 2/2023
3.	Evaluasi Antarmuka Web Badan Pengelola Pajak dan Retribusi Daerah Kota Palangka Raya	Jurnal Sains Komputer dan Teknologi Informasi	Vol. 6/No. 1/2023

Semua data yang saya isikan dan tercantum dalam biodata ini adalah benar dan dapat dipertanggung jawabkan secara hukum. Apabila di kemudian hari ternyata dijumpai ketidak-sesuaian dengan kenyataan, saya sanggup menerima sanksi.

Demikian biodata ini saya buat dengan sebenarnya untuk memenuhi salah satu persyaratan dalam pengajuan Penugasan penelitian.

Palangka Raya, 9 September 2024
K e t u a,

Amaya Andri Damaini, S.Kom., M.T
NIK. 199309042018001

A. Identitas Diri Anggota Pelaksana

1	Nama Lengkap	Abdul Hadi, S.T., M.Kom
2	Jenis Kelamin	Laki-laki
3	Jabatan Fungsional	Asisten Ahli
4	NIK	198505102021101
5	NIDN	1110058501
6	Tempat dan Tanggal Lahir	Palangka Raya, 10 Mei 1985
7	E-mail	abdulhadi@stmikplk.ac.id
8	Nomor Telepon/HP	085280005003
9	Alamat Kantor	Jl. G.Obos No.114 Palangkaraya, Kalimantan Tengah
10	Nomor Telepon / Faks	0536-3225515 / 0536-3236933
11	Lulusan yang Telah Dihasilkan	D-3 = 0 Orang ; S-1 = 4 Orang;
12	Mata Kuliah yang diampu	1. Computer Network
		2. Network Security
		3. Digital Forensics
		4. Multimedia Pembelajaran
		5. Sistem Keamanan

B. Riwayat Pendidikan

Tahun Lulus	Jenjang	Perguruan Tinggi	Jurusan/ Bidang Studi
2011	S1	Universitas Ahmad Dahlan, Yogyakarta	Teknik Informatika
2020	S2	Universitas Ahmad Dahlan, Yogyakarta	Magister Teknik Informatika / Digital Forensics

C. Pengalaman Penelitian Dalam 5 Tahun Terakhir

No	Tahun	Judul Penelitian	Pendanaan	
			Sumber	Jumlah
1	2021	Perencanaan Kebutuhan Dan Layout Data Center Dinas Komunikasi, Informatika, Persandian Dan Statistik Provinsi Kalimantan Tengah	STMIK Palangkaraya	Rp 3.000.000
2	2022	Standar Tata Kelola Pusat Data Berbasis Iso 27001	STMIK Palangkaraya	Rp 3.000.000

		Dan Iso 20000 Pada Dinas Komunikasi, Informatika, Persandian Dan Statistik Provinsi Kalimantan Tengah		

D. Pengalaman Pengabdian Kepada Masyarakat dalam 5 Tahun Terakhir

No	Tahun	Judul Pengabdian Kepada Masyarakat	Pendanaan	
			Sumber	Jumlah
1	2021	Implementasi Pembelajaran VLAN Menggunakan *Model Small Office Home Office* untuk Meningkatkan Kompetensi Guru dan Siswa pada SMK Al Ishlah Palangka Raya	STMIK Palangka Raya	Rp 2.000.000
2	2021	Implementasi Skema Junior Web Developer Untuk Meningkatkan Kompetensi Siswa Jurusan Rpl Di Smk Negeri 1 Palangka Raya	STMIK Palangka Raya	Rp 2.000.000
3	2022	Optimalisasi Multimedia Pembelajaran Interaktif Menggunakan Microsoft Power Point Bagi Guru MI Muslimat NU Palangka Raya	STMIK Palangka Raya	Rp 2.000.000
4	2023	Implementasi Multimedia Pembelajaran Interaktif Menggunakan Classpoint	STMIK Palangka Raya	Rp 2.000.000

No	Tahun	Judul Pengabdian Kepada Masyarakat	Pendanaan	
			Sumber	Jumlah
		bagi Guru MIS NU Palangka Raya		

E. Publikasi Artikel Ilmiah Dalam Jurnal dalam 5 Tahun Terakhir

Tahun	Judul	Penerbit/Jurnal
2023	Optimalisasi Multimedia Pembelajaran Interaktif Menggunakan Microsoft Power Point Bagi Guru Mi Muslimat NU Palangka Raya	Abdimas Galuh Volume 5, Nomor 1, Maret 2023
2022	Komparasi Analisis Bukti Digital Tiktok Lite Menggunakan Metode National Institute of Justice	J-Sakti Vol 6, No. 2 2022
2022	Implementasi Skema Junior Web Developer untuk Meningkatkan Kompetensi Siswa di SMK Negeri 1 Palangka Raya	PengabdianMu: Jurnal Ilmiah Pengabdian kepada Masyarakat Vol 7 No. 5 2022
2021	Perencanaan Layout Data Center Dinas Komunikasi Informatika Persandian dan Statistik Provinsi Kalimantan Tengah	Jurnal Sains Komputer Dan Teknologi Informasi 4 (1), 9-16
2021	Implementasi Pembelajaran VLAN Menggunakan Model Small Office Home Office untuk Meningkatkan Kompetensi Guru dan Siswa	JPMB: Jurnal Pemberdayaan Masyarakat Berkarakter 4 (2), 169-178
2020	Analisis Bukti Digital Trim Enable SSD NVMe menggunakan Statics Forensics	Informatics Engineering Study Program, Universitas Muhammadiyah Purwokerto (JUITA), Sinta 2, Vol. 8 No. 1/ http://jurnalnasional.ump.ac.id/index.php/JUITA/article/download/6584/3130

Tahun	Judul	Penerbit/Jurnal
2019	Analisis Bukti Digital SSD NVMe pada Sistem Operasi Proprietary Menggunakan Metode Static Forensics	Informatics Engineering Department – Universitas Islam Negeri Sultan Syarif Kasim Riau (CoreIT),Sinta 4, VOL 5, No. 2/ http://ejournal.uin-suska.ac.id/index.php/coreit/article/download/8217/pdf
2019	Perancangan Database Point of Sales Apotek Dengan Menerapkan Model Data Relasional	Faculty of Science and Technology State Islamic University Medan (QUERY), VOL 3, No. 2/ http://jurnal.uinsu.ac.id/index.php/query/article/view/6394/2765
2019	Forensik Bukti Digital Pada Solid State Drive (SSD) Nvme Menggunakan Metode National Institute Of Standards And Technology (NIST)	Prosiding SEMNASTEK 2019

F. Pemakalah Seminar Ilmiah (*Oral Presentation*) dalam 5 Tahun Terakhir

No	Nama Temu Ilmiah / Seminar	Judul Artikel Ilmiah	Waktu dan Tempat
1	2	3	4
1	Prosiding SEMNASTEK 2019	Forensik Bukti Digital Pada Solid State Drive (SSD) Nvme Menggunakan Metode National Institute Of	Jakarta 17 Juli 2019, Teknologi Fakultas Teknik

No	Nama Temu Ilmiah / Seminar	Judul Artikel Ilmiah	Waktu dan Tempat
		Standards And Technology (NIST)	Universitas Krisnadwipa yana,

Semua data yang saya isikan dan tercantum dalam biodata ini adalah benar dan dapat dipertanggungjawabkan secara hukum. Apabila di kemudian hari ternyata dijumpai ketidak-sesuaian dengan kenyataan, saya sanggup menerima sanksi.

Demikian biodata ini saya buat dengan sebenarnya untuk memenuhi salah satu persyaratan dalam pengajuan penelitian.

Palangka Raya, 9 September 2024

Anggota Pelaksana,

Abdul Hadi, S.T., M.Kom

A. Identitas Diri Anggota

1	Nama Lengkap	Elia Zakharia, M.T.
2	Jenis Kelamin	Laki-Laki
3	Jabatan Fungsional	Lektor (300)
4	NIK	199205262016104
5	NIDN	1126059201
6	Tempat dan Tanggal Lahir	Palangka Raya, 26 Mei 1992
7	E-mail	eliazakharia@gmail.com
8	Nomor Telepon/HP	085752443600
9	Alamat Kantor	Jl. G.Obos No.114 Palangkaraya, Kalimantan Tengah
10	Nomor Telepon / Faks	0536-3225515 / 0536-3236933
11	Lulusan yang Telah Dihasilkan	S-1 = 67 Orang
12	Mata Kuliah yang diampu	1. Multimedia
		2. Network computing
		3. Rekayasa perangkat lunak

B. Riwayat Pendidikan

Tahun Lulus	Jenjang	Perguruan Tinggi	Jurusan/ Bidang Studi
2014	S1	UNIVERSITAS PALANGKA RAYA	TEKNIK INFORMATIKA
2016	S2	UNIVERSITAS ATMA JAYA YOGYAKARTA	TEKNIK INFORMATIKA

C. Pengalaman Penelitian Dalam 5 Tahun Terakhir

No	Tahun	Judul Penelitian	Pendanaan	
			Sumber	Jumlah

D. Pengalaman Pengabdian Kepada Masyarakat dalam 5 Tahun Terakhir

No	Tahun	Judul Pengabdian Kepada Masyarakat	Pendanaan	
			Sumber	Jumlah
1	2022	Optimalisasi Multimedia Pembelajaran Interaktif Menggunakan Microsoft Power Point Bagi Guru MI Muslimat NU Palangka Raya	STMIK Palangka Raya	Rp 2.000.000
2	2023	Implementasi Multimedia Pembelajaran Interaktif Menggunakan Classpoint bagi Guru MIS NU Palangka Raya	STMIK Palangka Raya	Rp 2.000.000

E. Publikasi Artikel Ilmiah Dalam Jurnal dalam 5 Tahun Terakhir

No	Judul Artikel Ilmiah	Nama Jurnal	Volume/ Nomor / Tahun

Semua data yang saya isikan dan tercantum dalam biodata ini adalah benar dan dapat dipertanggung jawabkan secara hukum. Apabila di kemudian hari ternyata dijumpai ketidak-sesuaian dengan kenyataan, saya sanggup menerima sanksi.

Demikian biodata ini saya buat dengan sebenarnya untuk memenuhi salah satu persyaratan dalam pengajuan Penugasan penelitian

Palangka Raya, 24 Agustus 2024

Anggota,

Elia Zakharia, M.T

A. **Identitas Diri Anggota**

1	Nama Lengkap	Herkules, S.Kom.,M.Cs.
2	Jenis Kelamin	Laki-Laki
3	Jabatan Fungsional	Lektor (300)
4	NIK	198510042010106
5	NIDN	1104108502
6	Tempat dan Tanggal Lahir	Palangka Raya, 04-10-1985
7	E-mail	Herkules11282@gmail.com
8	Nomor Telepon/HP	085228043555
9	Alamat Kantor	Jl. G.Obos No.114 Palangkaraya, Kalimantan Tengah
10	Nomor Telepon / Faks	0536-3225515 / 0536-3236933
11	Lulusan yang Telah Dihasilkan	S-1 = 85 Orang
12	Mata Kuliah yang diampu	4. Sistem Basis Data
		5. Rekayasa Perangkat Lunak
		6. Pemrograman Berorientasi Objek
		7. Pemrograman Web
		8. Sistem Terdistribusi
		6. IoT
		7. Praktikum Sistem Basis Data

F. Riwayat Pendidikan

	S-1	**S-2**
Perguruan Tinggi	STMIK AMIKOM Yogyakarta	Universitas Gadjah Mada
Bidang Ilmu	Sistem Informasi	Ilmu Komputer
Tahun Masuk-Lulus	2003-2007	2007-2010
Judul Skripsi/tesis	Rancang Bangun Website pada PT Aseli Dagadu Djokja sebagai sarana promosi dan penjualan Online produk	Sistem Pendukung Keputusan Penentuan Penerima Bantuan Langsung Masyarakat (PNPM) Mandiri Perdesaan

G. Pengalaman Penelitian Dalam 5 Tahun Terakhir

No	**Tahun**	**Judul Penelitian**	**Pendanaan**	
			Sumber	**Jumlah**
1	2020	Perencanaan Kebutuhan Dan Layout Data Center Dinas Komunikasi, Informatika, Persandian Dan Statistik	STMIK Palangkaraya	Rp 3.000.000

No	Tahun	Judul Penelitian	Pendanaan	
			Sumber	Jumlah
		Provinsi Kalimantan Tengah		
2	2020	Aplikasi Pengelolaan Mata Kuliah Teknik Informatika Berbasis Client Server Pada Stmik Palangka Raya	STMIK Palangkaraya	Rp 3.000.000
3	2017	Aplikasi Web Pengelolaan Tugas Akhir Pada Teknik Informatika STMIK Palangka Raya	STMIK Palangkaraya	Rp 3.000.000

H. Pengalaman Pengabdian Kepada Masyarakat dalam 5 Tahun Terakhir

No	Tahun	Judul Pengabdian Kepada Masyarakat	Pendanaan	
			Sumber	Jumlah
1	2021	Implementasi Skema Junior Web Developer Untuk Meningkatkan Kompetensi Siswa Jurusan RPL Di SMK Negeri 1 Palangka Raya	STMIK Palangkaraya	Rp 2.000.000
2	2020	Penerapan, Pelatihan, Dan Pendampingan Pemanfaatan Sistem Informasi Desa Berbasis Open Source Menggunakan Opensid Pada Kantor Desa Tuwung	STMIK Palangkaraya	Rp 2.000.000
3	2019	Implementasi Sistem Informasi Desa Menggunakan Opensid Pada Desa Lawang Uru Kec. Banama Tingang Kab. Pulang Pisau Kalimantan Tengah	STMIK Palangkaraya	Rp 2.000.000
4	2018	Pelatihan Penggunaan SLIMS8 Pada Perpustakaan Penjaminan Mutu Pendidikan (LPMP) Kalimantan Tengah	STMIK Palangkaraya	Rp 2.000.000

I. Publikasi Artikel Ilmiah Dalam Jurnal dalam 5 Tahun Terakhir

No	Judul Artikel Ilmiah	Nama Jurnal	Volume/ Nomor / Tahun
1	Perencanaan Layout Data Center Dinas Komunikasi Informatika Persandian dan Statistik Provinsi Kalimantan Tengah	J-SAKTI	Vol 4 /1/November 2021
2	Aplikasi Pengelolaan Mata Kuliah Teknik Informatika Berbasis Client Server Pada Stmik Palangka Raya	Saintekkom	Vol 10/2/September 2020
3	Aplikasi Web Pengelolaan Tugas Akhir Pada Teknik Informatika STMIK Palangka Raya	Saintekkom	Vol 8/1/Maret/2018
4	Determinants of CAATT acceptance Insights from public accounting firms in Indonesia terindeks Scopus	Procedia Computer	Volume : 124,Edisi (Bulan/Tahun): Desember 2017,ISSN 1877-0509 (Versi Online),Penerbit : Elsevier B.V
5	Critical Success Factors Of E-Government Implementation	IIOAB Journal	suppl 1/7,Desember 2016,ISSN 0976-3104 (Versi Online)

Semua data yang saya isikan dan tercantum dalam biodata ini adalah benar dan dapat dipertanggung jawabkan secara hukum. Apabila di kemudian hari ternyata dijumpai ketidak-sesuaian dengan kenyataan, saya sanggup menerima sanksi.

Demikian biodata ini saya buat dengan sebenarnya untuk memenuhi salah satu persyaratan dalam pengajuan Penugasan penelitian

Palangka Raya, 11 September 2023

Anggota,

Herkules, S.Kom., M.Cs

A. Identitas Diri

1	Nama Lengkap	Yoantri Et Devitsu
2	Jenis Kelamin	Laki - Laki
3	NIM	C2155201035
4	Tempat dan Tanggal Lahir	Gunung Mas, 23 Juli 2003
5	E-mail	yoantri90@gmail.com
6	Nomor Telepon/HP	082255774987
7	Alamat Kampus	Jl. G. Obos No.114, Menteng, Kec. Jekan Raya, Kota Palangka Raya, Kalimantan Tengah 74874
8	Nomor Telepon / Faks	-
9	Mata Kuliah Yang Relevan Dengan Penelitian	1. Sistem Keamanan
		2. Keamanan jaringan
		3. Desain dan Manajemen Jaringan

B. Riwayat Pendidikan

Tahun Lulus	Jenjang	Instansi	Jurusan/ Bidang Studi
2021	SMA	SMAN 5 Palangka Raya	IPA
2018	SMP	SMPN 2 Katingan Hilir	

C. Pengalaman Penelitian Dalam 5 Tahun Terakhir

No	Tahun	Judul Penelitian	Pendanaan	
			Sumber	Jumlah

D. Pengalaman Pengabdian Kepada Masyarakat dalam 5 Tahun Terakhir

No	Tahun	Judul Pengabdian Kepada Masyarakat	Pendanaan	
			Sumber	Jumlah

E. Publikasi Artikel Ilmiah Dalam Jurnal dalam 5 Tahun Terakhir

No	Judul Artikel Ilmiah	Nama Jurnal	Volume/ Nomor / Tahun

F. Pelatihan Profesional

Tahun	Pelatihan	Penyelenggara
2022	Junior Network Administrator	KOMINFO

G. Penghargaan/Piagam

Tahun	Bentuk Penghargaan	Pemberi

H. Organisasi

Tahun	Organisasi	Jabatan

Semua data yang saya isikan dan tercantum dalam biodata ini adalah benar dan dapat dipertanggung jawabkan secara hukum. Apabila di kemudian hari ternyata dijumpai ketidak-sesuaian dengan kenyataan, saya sanggup menerima sanksi.

Demikian biodata ini saya buat dengan sebenarnya untuk memenuhi salah satu persyaratan dalam pengajuan Penugasan penelitian

Palangka Raya, 24 Agustus 2024
Anggota,

Yoantri Et Devitsu

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
(STMIK) PALANGKARAYA
Jl. G. Obos No.114 Telp.0536-3224593, 3225515 Fax.0536-3225515 Palangka Raya
email : humas@stmikplk.ac.id - website : www.stmikplk.ac.id

SURAT PERNYATAAN
KETUA PENGUSUL

Nama : Amaya Andri Damaini, S.Kom., M.T
NIDN : 1104099301
Pangkat / Golongan : Penata Muda Tk. 1/ Ruang III/b
Jabatan Fungsional : Asisten Ahli

Dengan ini menyatakan bahwa proposal saya dengan judul:

Asesmen Tata Kelola Keamanan Teknologi Informasi STMIK Palangkaraya Menggunakan Indeks Keamanan Informasi

yang diusulkan dalam skema penelitian untuk tahun anggaran 2024 bersifat original dan belum pernah dibiayai oleh lembaga/sumber dana lain.

Bilamana di kemudian hari ditemukan ketidak sesuaian dengan pernyataan ini, maka saya bersedia dituntut dan diproses sesuai dengan ketentuan yang berlaku dan mengembalikan seluruh biaya penugasan yang sudah diterima ke Kas STMIK Palangkaraya

Demikian pernyataan ini dibuat dengan sesungguhnya dan dengan sebenar-benarnya.

Palangka Raya, 9 September 2024

Mengetahui :
Kepala UP3M,



Rosmiati, M.Kom
NIK. 197810102005003

Yang Menyatakan,

Amaya Andri Damaini, S.Kom., M.T
NIK. 199309042018001