BAB I

PENDAHULUAN

1.1 Gambaran Umum Objek Penelitian

Institusi XYZ adalah institusi yang mempunyai tugas menyelenggarakan urusan di bidang pemerintahan untuk membantu Presiden dalam menyelenggarakan pemerintahan negara. Institusi XYZ berada di bawah dan bertanggung jawab kepada Presiden.

Institusi memiliki pusat data dan informasi (PUSDATIN). Pusat Data dan Informasi (PUSDATIN) mengelola tentang layanan informasi kepada mayarakat maupun operasional sehari-hari di lingkungan institusi tesebut.

Setiap data yang dikelola harus dilakukan secara terintegrasi mulai dari Sistem Informasi dan Manajemen Pertanahan Nasional (SIMTANAS) yang mengalirkan informasi antar seluruh unit organisasi baik di tingkat kantor Pusat, Kantor Wilayah dan Kantor Pertanahan.

Data dan informasi pertanahan dikelola secara elektronik untuk mewujudkan *good governance* , dimana terdapat keterbukaan informasi bagi masyarakat dan pertukaran informasi antar instansi pemerintah.

Data – data pertanahan yang diolah menggunakan teknologi informasi diantaranya data spasial (objek hak), data Yuridis (*data textual*) beserta riwayat tanahnya, penilaian tanah, dan penggunaan dan pemanfaatan bidang-bidang tanahnya.

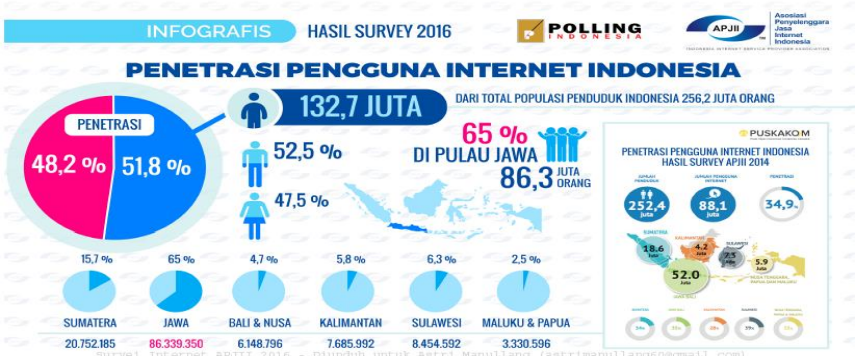
1.2 Latar Belakang Penelitian

Perkembangan teknologi informasi pada era digital saat ini semakin pesat. Seiring dengan perkembangan teknologi informasi tersebut institusi – institusi di indonesia menerapkan teknologi informasi dalam institusi mereka.

Teknologi informasi dimanfaatkan untuk mengolah data, termasuk memproses, mendapatkan, menyusun, menyimpan, memanipulasi data dalam berbagai cara untuk menghasilkan informasi yang berkualitas, yaitu informasi yang relevan, akurat dan tepat waktu, yang digunakan untuk keperluan pribadi, bisnis, dan pemerintahan dan merupakan informasi yang strategis untuk mengambil keputusan.

Dengan perkembangan teknologi saat ini telah memudahkan orang dalam memperoleh informasi. Terlihat dari peningkatan jumlah pengunjung internet dari tahun ke tahun. Hal ini mengindikasikan kenaikan 51,8 persen dari tahun 2014 sampai tahun 2016.

Survei yang dilakukan APJII pada 2014 hanya ada 88 juta pengguna internet sedangkan pada tahun 2016 terdapat 132,7 juta pengguna. Hal ini tampak pada gambar 1.1 pengunjung internet pada tahun 2016 yang bersumber dari Assosiasi Penyelenggara Jasa Internet Indonesia (APJII) dibawah ini.



Gambar 1.1 Pengunjung Internet pada tahun 2016

Sumber : https://www.apjii.or.id/

Dalam institusi menghasilkan banyak data dan informasi. Data dan informasi tersebut merupakan bagian yang sangat penting karena berguna untuk menjalankan sistem dalam institusi tersebut.

Data dan informasi tersebut ada yang disimpan dalam bentuk elektronik dan dikelola oleh institusi agar berjalan sesuai dengan kebutuhan dan sistem dalam institusi tersebut, tetapi ada institusi yang tidak menjaga data dan informasi.

Institusi ada yang tidak menyadari kebutuhan dan keamanan akan data dan informasi tersebut dimasa yang akan datang, data – data tersebut rentan terhadap berbagai jenis ancaman yang berasal dari faktor teknis, organisasi, dan lingkungan yang ada.

Bagi institusi didalam menyimpan data-data penting yang menyangkut privasi atau kerahasiaan institusi, apalagi institusi yang menggunakan web, sangat rentan terhadap penyalahgunaan, karena pada dasarnya web mempunyai akses yang sangat luas dan dapat diakses oleh semua orang, membuat sistem institusi dengan mudah mendapat serangan yang pada umumnya berasal dari pihak luar, seperti *hacker*, dan hal itu sangat merugikan institusi atau institusi.

Menurut Symantec Corporation dalam *Internet Security Threat Report 2017 Trends* terdapat 10 besar yang menjadi target kejahatan terhadap situs web yang paling sering di terjadi adalah :

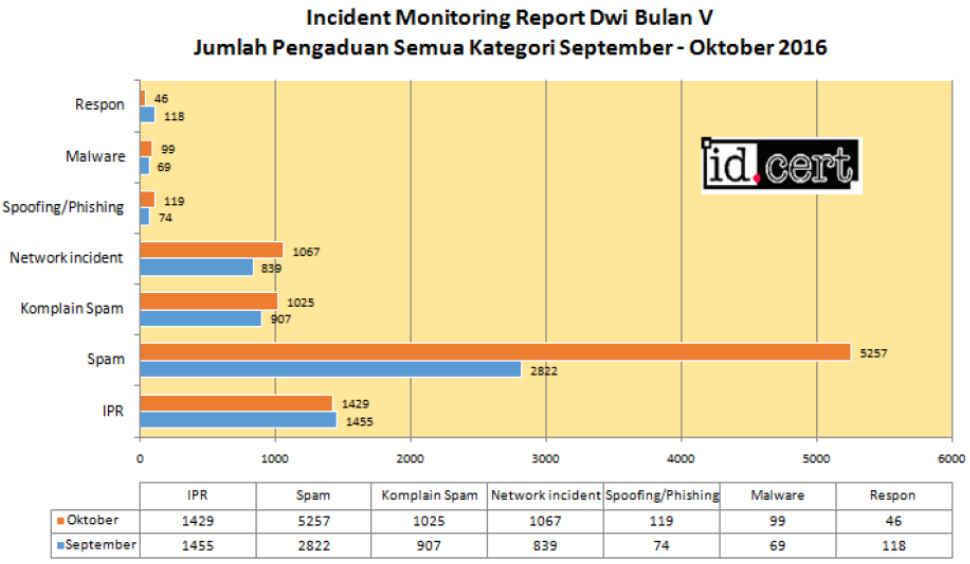
Rank	Domain Categories	2015 (%)	2016 (%)	Percentage Point Difference
1	Technology	23.2	20.7	-2.5
2	Business	8.1	11.3	3.2
3	Blogging	7.0	8.6	1.6
4	Hosting	0.6	7.2	6.6
5	Health	1.9	5.7	3.8
6	Shopping	2.4	4.2	1.8
7	Educational	4.0	4.1	< 0.1
8	Entertainment	2.6	4.0	1.4
9	Travel	1.5	3.6	2.1
10	Gambling	0.6	2.8	2.2

Gambar 1.2 Kejahatan terhadap situs web

Sumber : https://www.symantec.com/security-center/threat-report

Urutan pertama web yang paling sering mengalami kejahatan atau eksploitasi adalah situs web dibidang teknologi, dan rata – rata dari 10 besar kategori web site tersebut mengalami peningkatan sehingga hal tersebut dapat menjadi ancaman bagi institusi.

Indonesia *Computer Emergency Response Team* (ID-CERT) melaporkan jumlah insiden ancaman keamanan sistem informasi yang masuk pada September – Oktober 2016. Dari laporan insiden yang masuk dapat disajikan dalam bentuk gambar 1.2 berikut:

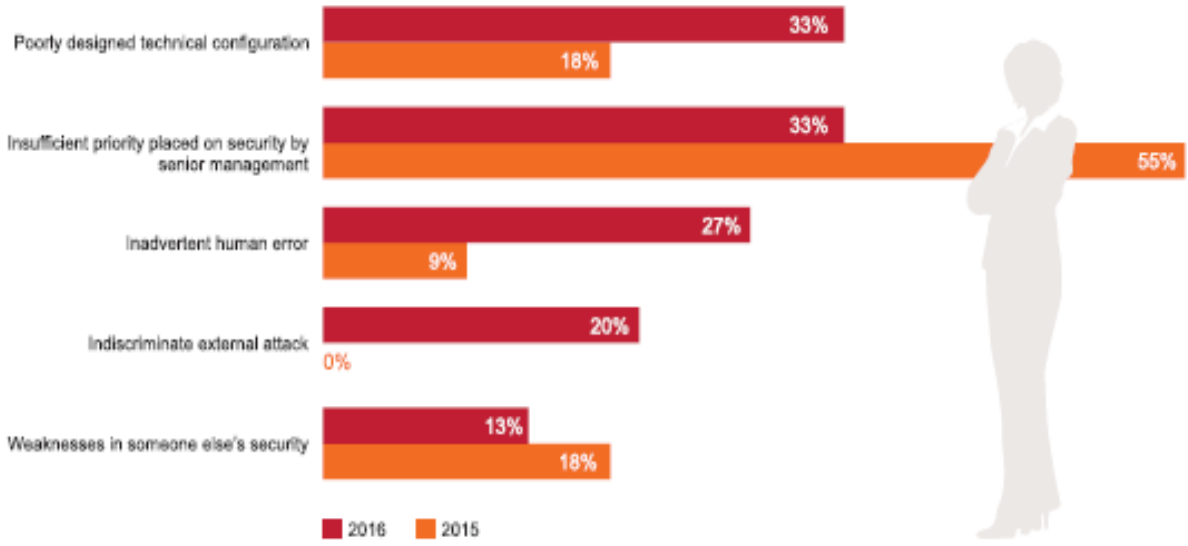


Gambar 1.3 Jumlah pengaduan semua kategori September – Oktober 2016.

Sumber : https://www.cert.or.id/

Dengan melihat gambar 1.2 tersebut, jumlah pengaduan yang paling tinggi adalah *spam* sebesar 5257 pengaduan, kemudian disusul dengan IPR (*Intellectual Property Rights*) sebesar 1429 pengaduan dan terdapat pengaduan – pengaduan yang lain, oleh karena itu keamanan informasi perlu diperhatikan oleh setiap organisasi.

Menurut *Information Security Breaches Survey* (ISBS) penyebab terjadinya pelanggaran pada keamanan informasi karena beberapa hal, seperti yang terdapat pada gambar 1.3 berikut :



Gambar 1.4 Penyebab terjadinya pelanggaran keamanan informasi

Sumber : https://www.gov.uk/government/publications/cyber-security-breaches-survey-2016

Penyebab terjadinya pelanggaran berdasarkan gambar 1.3 yang paling tinggi disebabkan oleh ketidakcukupan prioritas keamanan yang dilakukan oleh manajemen dan konfigurasi desain teknik yang buruk yaitu sebesar 33%, kemudian disebabkan oleh kesalahan yang tidak disengaja, kelemahan keamanan yang ada.

Dari gambar 1.3 tersebut dapat kita ketahui bahwa keamanan informasi sangat penting bagi institusi dan harus dijaga agar tidak terjadi pelanggaran. Oleh karena itu, agar penerapan teknologi informasi berjalan dengan baik diperlukan adanya tatakelola yang digunakan untuk mengelola segala sistem di bidang teknologi informasi tersebut.

Keamanan informasi pada era sekarang ini sangat penting, sehingga para pemimpin institusi berusaha menggunakan teknologi informasi sebaik-baiknya untuk mendukung pengambilan keputusan yang dilakukan.

Informasi dan teknologi digunakan untuk meningkatkan nilai-nilai dalam lembaga tersebut yaitu investasi yang dilakukan sesuai dengan hasil yang diperoleh dan memberikan dampak terbaik bagi lembaga dan tujuannya. Untuk itu teknologi harus digunakan dengan efisien dan pelaksanaannya secara maksimal.

Maraknya serangan yang dihadapi oleh sistem komputer yang semakin meningkat membuat institusi harus lebih berhati – hati. Pada tahun 2017 di indonesia terdapat serangan *cyber* yang disebut dengan nama *Ransomware WannaCry*. *Ransomware WannaCry* adalah bentuk malware yang mengenkripsi dokumen pada PC atau bahkan jaringan, sehingga data yang dimiliki oleh institusi tidak dapat diakses.

Serangan *Cyber* yang menyerang komputer tentunya memberikan dampak kerugian bagi institusi – institusi yang ada. Hal tersebut dapat menurunkan citra dari institusi tersebut, dimana dengan terjadinya serangan terhadap sistem komputer yang dimiliki oleh institusi menyebabkan terkendalanya sistem yang ada dalam institusi tersebut, sehingga dapat mengakibatkan gangguan dalam melayani konsumen sehingga dapat menurunkan *revenue* dan citra dari institusi tersebut.

Menurut Husin *et al* berbagai bentuk trend serangan dan insiden pada saat ini menggunakan instrumen *cyberspace* sebagai saluran utama dalam melaksanakan tindakannya. Salah satu kebijakan yang dapat diambil oleh organisasi untuk mengatasi gangguan keamanan informasi adalah dengan menerapkan Sistem Manajemen Keamanan Informasi (SMKI). Walaupun kenyataannya sampai saat ini belum atau bahkan tidak akan ada sebuah keamanan Sistem Informasi yang sempurna sehingga dapat 100% mengamankan Informasi dari segala gangguan.

Institusi XYZ adalah institusi yang mempunyai tugas menyelenggarakan urusan pemerintahan untuk membantu Presiden RI dalam menyelenggarakan pemerintahan negara.

Institusi XYZ menggunakan sistem informasi yang dapat diakses oleh pegawai kepemerintahan maupun masyarakat umum. Teknologi informasi pada institusi XYZ harus dikelola dengan baik dan benar agar sesuai dengan tujuan yang diharapkan.

Pada institusi XYZ terdapat bidang Pusat Data dan Informasi (PUSDATIN) yang berfungsi untuk mengelola layanan informasi kepada masyarakat maupun operasional sehari – hari dilingkungan institusi tersebut.

Informasi dikelola secara elektronik untuk mewujudkan *good governance* , terdapat keterbukaan informasi bagi masyarakat dan pertukaran informasi antar institusi yang saling terkoneksi.

Data – data yang diproses pada bidang PUSDATIN terkoneksi dengan jaringan komputer. Data dan jaringan merupakan hal yang sangat berisiko dalam bidang keamanan informasi, risiko yang sering terjadi diantaranya penyebaran virus komputer dan terjadi pencurian data yang dimiliki oleh institusi yang dapat menyebabkan kerugian institusi.

Dalam penyelenggaraan evaluasi teknologi informasi, faktor keamanan informasi merupakan aspek yang sangat penting untuk diperhatikan pada institusi XYZ, kinerja teknologi informasi akan terganggu jika informasi sebagai salah satu objek utama tata kelola teknologi informasi mengalami masalah berupa gangguan dan ancaman yang menyangkut aspek kerahasiaan, keutuhan dan ketersediaan (Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik. Direktorat Keamanan Informasi, Direktorat Jenderal Aplikasi Informatika, Kemkominfo. 2011).

Dengan menyadari adanya risiko-risiko yang dapat menyebabkan terganggunya pelayanan publik dalam rangka mencapai target yang telah ditetapkan sehingga dibutuhkan adanya evaluasi terhadap keamanan informasi, untuk mengetahui apakah sistem dan keamanan informasi institusi sudah siap atau tidak terhadap risiko yang mungkin terjadi setiap saat.

Pada institusi XYZ terdapat beberapa informasi yang saya peroleh dari hasil wawancara awal dengan pegawai institusi XYZ yaitu terdapat akses kontrol yang belum dilaksanakan dengan baik diantaranya kurang keamanan atau pengawasan lokasi kerja penting (ruang server, ruang arsip) sehingga siapa saja bebas untuk melakukan akses, dan itu tentunya bisa merugikan institusi.

Institusi XYZ belum menerapkan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi dan password yang ada pada bidang PUSDATIN tidak diganti secara berkala, seharusnya harus melakukan penggantian password tiga bulan sekali sehingga dapat menghindari resiko pencurian atau kejahatan terhadap data yang dimiliki.

Untuk mengetahui kesiapan keamanan informasi institusi XYZ saya melakukan penelitian untuk mengetahui sejauh mana kesiapan dari institusi XYZ terhadap resiko keamanan informasi yang mungkin terjadi pada institusi tersebut.

Tanpa adanya sistem keamanan terhadap informasi membuat sistem informasi yang dimiliki individu, organisasi bahkan pemerintahan menjadi sangat rentan terhadap adanya upaya-upaya penyerangan (*attack*) sistem informasi, seperti virus, pencurian data dan penyalagunaan data dan informasi yang dimiliki. Serangan ini tentu saja tidak hanya merusak sistem, tetapi juga dapat menyebabkan kerugian baik itu materil maupun non-materil.

Pemerintah Indonesia melalui Kementerian Komunikasi dan Informatika (Kemkominfo) telah menghimbau kepada seluruh instansi pemerintahan, baik itu pusat maupun daerah, sebagai badan penyelenggara layanan publik untuk meningkatkan kesadaran akan pentingnya keamanan informasi.

Berbagai cara dilakukan untuk meningkatkan kesadaran bagi aparatur negara tentang keamanan informasi, mulai dari sosialiasasi maupun bimbingan teknis (bimtek).

Sosialisasi yang dilakukan berisikan materi-materi tentang definisi, pengertian, kontrol-kontrol, persyaratan dokumentasi keamanan informasi dan contoh-contoh

tindakan untuk mengamankan informasi. Sementara pada setiap bimbingan teknis, dijelaskan metode atau cara melakukan penilaian mandiri (*self assessment*) terhadap status keamanan informasi pada masing-masing instansi menggunakan alat bantu berupa perangkat penilaian yang bernama indeks Keamanan Informasi (KAMI).

Sesuai dengan peraturan Kementerian Komunikasi dan Informatika nomor 4 Tentang sistem manajemen penanganan informasi dijelaskan pentingnya menjaga keamanan informasi, terutama bagi badan / lembaga yang memiliki asset data nasional.

Dalam Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Pasal 15 ayat (1), Setiap Penyelenggara Sistem Elektronik harus menyelenggarakan Sistem Elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya Sistem Elektronik sebagaimana mestinya. Sementara itu, dalam Peraturan Pemerintah 82 Tahun 2012 tentang Penyelenggara Sistem dan Transaksi Elektronik Pasal 20 ayat (2), Penyelenggara Sistem Elektronik wajib menyediakan sistem pengamanan yang mencakup prosedur dan sistem pencegahan dan penanggulangan terhadap ancaman dan serangan yang menimbulkan gangguan, kegagalan, dan kerugian.

Penyusunan Peraturan Menteri tentang Sistem Pengamanan diamanatkan oleh Peraturan Pemerintah Penyelenggara Sistem dan Transaksi Elektronik dalam Pasal 20 Ayat (4), yaitu: Ketentuan lebih lanjut mengenai sistem pengamanan sebagaimana dimaksud pada ayat (2) diatur dalam Peraturan Menteri.

Peraturan Menteri yang dimaksud adalah Peraturan Menteri Kominfo nomor 4 tahun 2016 tentang Sistem Manajemen Pengamanan Informasi. Peraturan Menteri ini mengatur mengenai penerapan Sistem Manajemen Pengamanan Informasi (SMPI) mencakup Penyelenggara Sistem Elektronik untuk Pelayanan Publik berdasarkan asas resiko.

Institusi penyelenggara pelayanan publik, termasuk menkominfo, Badan Standarisasi Nasional (BSN), Badan Usaha Milik Negara (BUMN), Badan Usaha

Milik Daerah (BUMD), dan satuan kerja di lingkungan pemerintahan. UPT-UPT (Unit Pelaksana Teknis) yang menggunakan dana Anggaran Pendapatan dan Belanja Negara (APBN), Anggaran Pendapatan dan Belanja Daerah (APBD) juga termasuk. Definisi ini ada di Undang-Undang Pelayanan Publik korporasi, lembaga independen yang dibentuk berdasarkan UU: komisi-komisi, KPK, Komisi Yudisial, dan badan hukum lain yang menyelenggarakan pelayanan public dalam rangka pelaksanaan misi negara.

Oleh karena hal tersebut setiap institusi harus menjaga keamanan informasi atau data – data yang dimiliki oleh institusi sehingga diperlukan asesmen untuk mengetahui apakah institusi tersebut sudah memiliki sistem keamanan informasi yang baik atau tidak.

Surat Edaran Menteri Komunikasi dan Informatika Nomor: 5/SE/M.KOMINFO/07/2011 tentang Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik. Indeks KAMI adalah alat evaluasi untuk menganalisis tingkat kesiapan pengamanan informasi di instansi pemerintah.

Alat evaluasi Indeks KAMI tidak ditujukan untuk menganalisis kelayakan atau efektivitas bentuk pengamanan yang ada, melainkan sebagai perangkat untuk memberikan gambaran kondisi kesiapan (kelengkapan dan kematangan) kerangka kerja keamanan informasi kepada pimpinan Instansi.

Indeks KAMI dapat digunakan mengevaluasi tingkat kematangan, tingkat kelengkapan penerapan SNI ISO/IEC 27001 serta peta area tata kelola keamanan sistem informasi di suatu instansi pemerintah.dan standar komprehensif yang membantu institusi dalam mencapai tujuan dan menghasilkan nilai melalui tata kelola dan manajemen teknologi informasi yang efektif.

Evaluasi dilakukan terhadap beberapa area target penerapan keamanan informasi dengan ruang lingkup pembahasan yang juga memenuhi semua aspek keamanan yang didefinisikan oleh standar SNI ISO/IEC 27001, yaitu :

1. Kategori Sistem Elektronik

2. Tata Kelola Keamanan Informasi
3. Pengelolaan Risiko Keamanan Informasi
4. Kerangka Kerja Keamanan Informasi
5. Pengelolaan Aset Informasi, dan
6. Teknologi dan Keamanan Informasi

1.3 Perumusan Masalah

Berdasarkan latar belakang yang telah disampaikan, berikut ini adalah uraian permasalahan yang akan dibahas dalam penelitian ini :

1. Berapakah total skor dari penilaian kelima area Indeks KAMI pada institusi XYZ?
2. Bagaimana rekomendasi untuk meningkatkan manajemen keamanan informasi pada institusi XYZ?

1.4 Pernyataan Penelitian

Berdasarkan perumusan masalah tersebut diperlukan ada nya tata kelola menggunakan Indeks KAMI untuk menjawab pertanyaan sebagai berikut:

a. Bagaimana gambaran kondisi kesiapan (kelengkapan dan kematangan) kerangka kerja keamanan informasi pada institusi XYZ?
b. Bagaimana cara meningkatkan manajemen keamanan informasi berdasarkan tingkat keamanan dan kelengkapan keamanan informasi pada institusi XYZ saat ini sampai mencapai indeks KAMI level layak?

1.5 Tujuan Penelitian

Tujuan dari penelitian ini adalah;

a. Mengetahui nilai kematangan dan skor penilaian keamanan informasi institusi XYZ.

b. Memberikan rekomendasi kepada pihak institusi XYZ untuk keamanan informasi yang harus dijalankan.

1.6 Manfaat Penelitian

1.6.1 Aspek Teoritis

Penelitian ini dapat digunakan untuk mengetahui tingkat kematangan keamanan penggunaan teknologi informasi dan untuk mengetahui apakah sistem yang dibuat telah sesuai dengan standar rencana strategis pada institusi XYZ sehingga memberikan kemudahan bagi pengambil keputusan untuk membuat keputusan-keputusan dimasa yang akan datang.

1.6.2 Aspek Praktis

Dengan penelitian ini dapat memberikan analisis dan rekomendasi yang tepat yang dapat digunakan oleh institusi XYZ untuk memperbaiki pengelolaan keamanan teknologi informasi dalam meningkatkan *capability* pada institusi XYZ.

1.7 Ruang Lingkup Penelitian

1.7.1 Lokasi dan Objek Penelitian

Lokasi : Gedung Institusi XYZ

Objek Penelitian : Pusat Data dan Informasi

1.7.2 Waktu dan periode Penelitian

Juni – Desember

1.8 Sistematika penulisan Tugas Akhir

Untuk memberikan gambaran yang jelas mengenai penelitian yang dilakukan, maka sistematika penulisan penelitian ini adalah:

BAB I : PENDAHULUAN

Bab ini berisikan penjelasan secara umum, ringkas, dan padat serta menggambarkan dengan tepat isi penelitian.

BAB II : TINJAUAN PUSTAKA

Bab ini berisikan landasan teori mengenai hal-hal yang berkaitan dengan penelitian dan model penelitian. Serta beberapa penelitian terdahulu yang akan mendukung penelitian ini dalam mengembangkan hipotesis.

BAB III : METODE PENELITIAN

Bab ini berisikan pendekatan, metode, dan teknik yang digunakan untuk mengumpulkan data yang dapat menjawab atau menjelaskan masalah penelitian.

BAB IV : HASIL PENELITIAN DAN PEMBAHASAN

Bab ini berisikan hasil pengolahan data dan analisis atas pengolahan data tersebut.

BAB V : KESIMPULAN DAN SARAN

Bab ini berisikan kesimpulan dan hasil penelitian serta saran.