

BAB I

PENDAHULUAN

1.1. Latar Belakang

Perkembangan teknologi saat ini mengakibatkan seluruh organisasi harus selalu beradaptasi serta mengimplementasikan kemajuan TI. Di dalam teknologi yang perkembangannya semakin pesat tersebut terdapat informasi yang diolah dan disimpan. Selain perkembangan jenis peralatan teknologi maupun software aplikasi pendukung, perkembangan juga berdasarkan pada semakin meratanya pengguna informasi[1].

Commented [V4]:

Pengguna informasi pada saat ini meningkat secara signifikan karena banyak aspek yang bisa dipermudah dengan adanya teknologi informasi. Informasi adalah data mentah yang diolah menjadi bentuk yang lebih berguna dan lebih berarti bagi penerimanya[1]. Oleh karena itu seperti pada dasarnya informasi adalah data yang telah diproses ke dalam suatu bentuk yang mempunyai arti bagi si penerima dan mempunyai nilai nyata dan terasa bagi keputusan saat itu atau keputusan mendatang. Penting bagi organisasi untuk memiliki kebijakan yang berkaitan dengan keamanan informasi organisasi terutama yang berkaitan dengan informasi rahasia yang seharusnya memiliki tingkat otoritas yang tinggi. Keamanan informasi melindungi semua informasi yang ada dari ancaman dari luar yang bisa mengancam keberlangsungan organisasi seperti adanya hak akses yang tidak memiliki otoritas dan mengurangi resiko kerugian. Manajemen Keamanan Informasi memastikan informasi bahwa informasi telah dikirim dan diterima oleh pengguna yang benar [2] [3].

Commented [V5]:

Teknologi yang mengalami perubahan secara terus menerus memaksa suatu organisasi untuk bisa menyesuaikan diri dengan perubahan yang ada. Teknologi informasi sekarang sudah dimanfaatkan ke berbagai sektor kehidupan, termasuk juga di dalam sektor penyelenggaraan pemerintahan maupun swasta. Institusi pemerintah atau swasta ketika melakukan penerimaan data, mengolah data dan

Commented [V6]:

melakukan distribusi data tentu memerlukan pengamanan untuk menjaga data tersebut agar tetap aman sekaligus untuk keamanan pengguna data tersebut. Di lingkungan pemerintahan saat ini penggunaan TIK sudah semakin tumbuh dan berkembang sejalan dengan kebutuhan instansi untuk memberikan pelayanan publik dengan cepat, andal dan aman. Dengan segala kemudahan yang timbul dari perkembangan teknologi dan internet tentu tidak semata-mata menghasilkan hal yang sepenuhnya baik. Tidak menutup kemungkinan bahwa semua hal tersebut juga membawa dampak yang buruk. Dampak buruk yang dapat terjadi adalah meningkatnya kejahatan siber atau *cyber crime*. Tentu dampak buruk ini menjadi sebuah permasalahan di dalam bidang keamanan informasi[3].

Commented [V7]:

Commented [V8R7]:

Keamanan adalah bagian yang penting menjadi perhatian dalam proses pelaksanaan tata kelola teknologi informasi guna meningkatkan performa tata kelola tersebut. Jika aspek tersebut mengalami gangguan, maka dapat timbul celah yang berpotensi mengancam keamanan data yang meliputi kerahasiaan, keutuhan dan ketersediaannya[4]. Kerahasiaan atau *confidentiality* merupakan jaminan kerahasiaan terhadap data pada suatu instansi yang tidak boleh diketahui oleh sembarang pihak. Keutuhan atau *integrity* merupakan keutuhan dari data itu sendiri. Data yang dimiliki oleh instansi harus diamankan dengan sedemikian rupa agar isinya tetap utuh dan tidak ada manipulasi atau rekayasa. Ketersediaan atau *availability* terkait dengan ketersediaan data saat diakses atau dibutuhkan oleh pihak yang memang memiliki wewenang untuk mengaksesnya. Keamanan informasi sering kali diabaikan oleh para elemen pemerintahan. Dampak dari mengabaikan keamanan informasi sangat berpengaruh terhadap semua elemen terutama elemen pemerintah yang mana harusnya memiliki tingkat keamanan informasi yang cukup tinggi. Beberapa hal yang mungkin terjadi ketika mengabaikan keamanan informasi antara lain, pencurian data penting, hilangnya asset penting organisasi, sabotase, spionase, hacking serta masih banyak hal yang bisa terjadi jika elemen-elemen penting pemerintah mengabaikan keamanan informasi[5].

Commented [V9]:

Commented [V10]:

Commented [V11]:

Commented [V12]:

Tingkat keamanan dari suatu sistem keamanan dapat diukur menggunakan ISO/IEC 27001 yang merupakan sebuah dokumen standar Sistem Manajemen Keamanan Informasi (SMKI) atau Information Security Management System (ISMS) yang memberikan gambaran secara umum mengenai apa saja yang harus dilakukan oleh sebuah organisasi atau enterprise dalam usaha rangka mengimplementasikan konsep konsep keamanan informasi[6]. ISO/IEC 27001 juga dijadikan Standar SNI yang ditetapkan oleh Badan Standarisasi Nasional (BSN) dalam mengelola keamanan informasi dan juga ISO/IEC 27001 melingkupi seluruh tipe organisasi serta sudah digunakan oleh sebagian besar organisasi di dunia sebagai acuan dalam keamanan informasi[7].

Commented [V13]:

Penelitian ini menggunakan Indeks Keamanan Informasi (KAMI) merupakan aplikasi yang digunakan sebagai alat bantu untuk melakukan asesmen dan evaluasi tingkat kesiapan (Kelengkapan dan Kematangan) penerapan keamanan informasi berdasarkan kriteria SNI ISO/IEC 27001, yaitu Tata Kelola, Pengelolaan Risiko, Kerangka Kerja, Pengelolaan Aset, Aspek Teknologi dengan suplemen Pengamanan Keterlibatan Pihak Ketiga Penyedia Layanan, Pengamanan Layanan Infrastruktur Awan dan Perlindungan Data Pribadi. Indeks KAMI tidak ditujukan untuk menganalisis kelayakan atau efektivitas bentuk pengamanan yang ada, melainkan sebagai perangkat untuk memberikan gambaran kondisi kesiapan kerangka kerja keamanan informasi[5][8].

Commented [V14]:

Pemerintahan sebagai organisasi sektor publik merupakan pendorong dan fasilitator dalam keberhasilan pembangunan, oleh karena itu keberhasilan pembangunan perlu didukung oleh kecepatan arus informasi dan data antar instansi supaya terjadi keterpaduan sistem antara pemerintah dengan pihak pengguna lainnya serta keamanan informasi yang terjaga dengan baik maka dari itu sangat penting bagi Dinas Kominfo untuk menerapkan keamanan informasi agar tidak terjadinya hal yang merugikan bagi organisasi[9].

Commented [V15]:

Sebagai salah satu Instansi pemerintah, Dinas Komunikasi dan Informasi Kabupaten Penukal Abab Lematang Ilir memiliki tugas dan tanggung jawab untuk

pelaksanaan pemerintah di bidang komunikasi dan informatika. Pekerjaan terkait penyediaan informasi dan jaringan internet ditangani oleh divisi TIK (Teknologi informasi dan Komunikasi) yang berfokus pada keamanan informasi yang ada didalamnya. Divisi TIK (Teknologi Informasi dan Komunikasi) memiliki tugas dan tanggung jawab menjaga setiap informasi dan asset penting yang ada di organisasi serta memiliki prioritas keamanan informasi yang tinggi. Seperti halnya dengan instansi pemerintahan lainnya, Dinas Komunikasi dan Informasi Kabupaten Penukal Abab Lematang Ilir menerapkan keamanan informasi sesuai dengan peraturan pemerintah dan juga menganggap data adalah hal yang bernilai yang wajib dilindungi keamanannya yaitu Kerahasiaan, Integritas dan Ketersediaan. Dinas Komunikasi dan Informasi Kabupaten Penukal Abab Lematang Ilir sebagai instansi yang memanfaatkan teknologi informasi dalam proses bisnisnya.

Proses bisnis tersebut merupakan aset utama bagi Dinas Komunikasi dan Informasi Kabupaten Penukal Abab Lematang Ilir termasuk juga dengan sub-proses dan kegiatan-kegiatan di dalamnya. Berlangsungnya proses bisnis instansi dengan baik merupakan modal bagi Dinas Komunikasi dan Informasi Kabupaten Penukal Abab Lematang Ilir untuk memberikan layanan yang baik untuk masyarakat. Dari hal tersebut sudah seharusnya Dinas Komunikasi dan Informasi Kabupaten Penukal Abab Lematang Ilir menerapkan pengamanan informasi yang baik karena proses-proses bisnis yang berlangsung tentu berhubungan dengan banyak pihak baik internal maupun eksternal. Keamanan informasi sangat penting terutama dalam penggunaan TIK sebagai pendukung berjalannya proses bisnis yang dilakukan. Hal itu dilakukan bertujuan untuk meningkatkan kualitas layanan kepada setiap pemangku kepentingan[10].

Dinas Komunikasi dan Informasi Kabupaten Penukal Abab Lematang Ilir divisi TIK dalam mengatasi insiden keamanan informasi terkait kebocoran informasi dan asset penting organisasi masih belum memiliki kebijakan dalam menangani ancaman terhadap informasi dan asset penting yang ada , belum adanya standar yang diterapkan dalam pengamanan informasi serta keamanan server yang di kelola di Dinas Komunikasi dan Informasi Kabupaten Penukal Abab Lematang Ilir hanya berupa monitoring sedangkan untuk kendali penuh dalam keamanan

Commented [V16]:

informasi seperti di server masih ditangani oleh pihak Dinas Komunikasi dan Informasi Provinsi Sumatera Selatan, oleh karena itu sangat dibutuhkan bagi Dinas Komunikasi dan Informasi Kabupaten Penukal Abab Lematang Ilir untuk melakukan evaluasi keamanan informasi yang bisa membantu mengetahui tingkat kematangan keamanan informasi instansi dan meninjau prosedur keamanan kamanan informasi yang ada.

1.2. Perumusan Masalah

Berdasarkan latar belakang yang dikemukakan, maka pokok permasalahan yang dapat dirumuskan pada penelitian ini adalah Dinas Kominfo Kabupaten Penukal Abab Lematang Ilir yang belum melakukan pengamanan informasi terkait dengan keamanan informasi yang berguna untuk mengamankan informasi dan asset penting organisasi. Penerapan SMKI ini sangat dibutuhkan oleh organisasi pemerintah mengingat pentingnya keamanan informasi pada organisasi serta anjuran dari pemerintah mengenai keamanan informasi bagi setiap pelayanan publik

1.3. Pertanyaan Penelitian

1. Bagaimana menilai keamanan informasi yang sesuai menggunakan Indeks KAMI?
2. Apa saja rekomendasi keamanan informasi yang dapat diterapkan berdasarkan penilaian Indeks KAMI?

1.4. Tujuan Penelitian

Penelitian ditujukan untuk menemukan jawaban dari rumusan masalah yang telah ditentukan, yaitu :

1. Menilai keamanan informasi yang sesuai dengan menggunakan Indeks KAMI.
2. Memberikan rekomendasi keamanan informasi yang dapat diterapkan berdasarkan hasil penilaian Indeks KAMI.

1.5. Batasan Masalah

1. Penelitian ini terbatas pada Dinas Kominfo Kabupaten Penukal Abab Lematang Iilir.
2. standar yg digunakan adalah Indeks KAMI.
3. Penelitian ini menghasilkan dokumen rekomendasi keamanan informasi dan hasil rekomendasi berdasarkan penilaian keamanan informasi Indeks KAMI.

1.6. Manfaat Penelitian

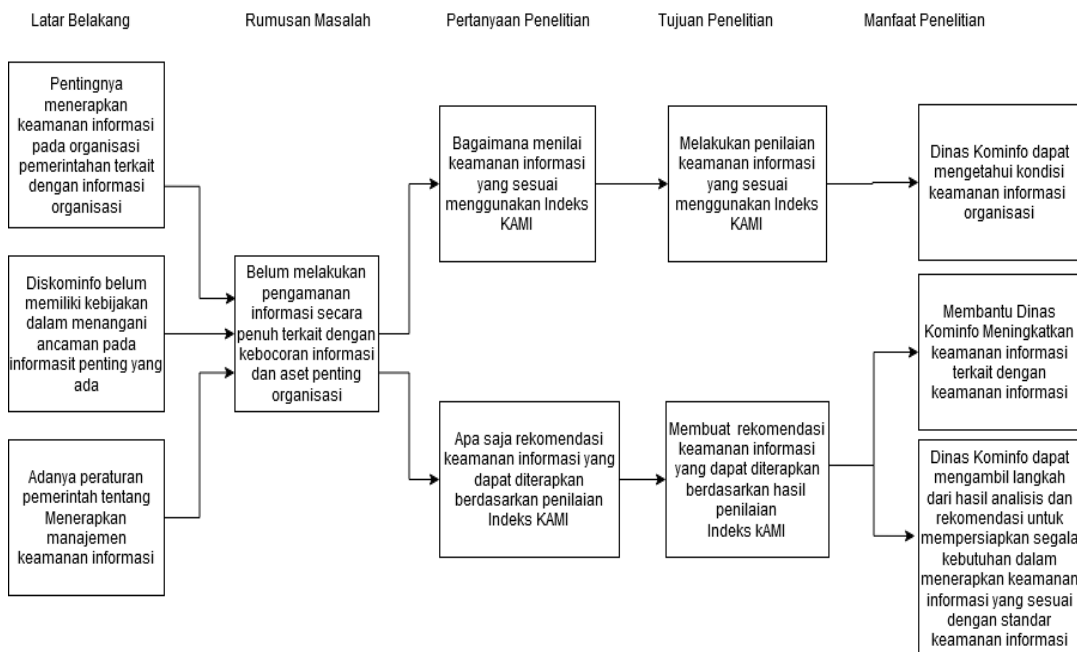
Berdasarkan permasalahan dan tujuan penelitian yang telah ditentukan, maka manfaat yang diperoleh dari penelitian ini sebagai berikut :

1. Memberikan pengetahuan mengenai kondisi keamanan informasi yang sesuai dengan Dinas Kominfo.
2. Memberikan rekomendasi keamanan informasi yang dapat diterapkan pada Dinas Kominfo Kabupaten Penukal Abab Lematang Iilir.
3. Meningkatkan tingkat keamanan informasi setelah penerapan keamanan informasi.

1.7. Bagan Keterkaitan

Commented [V17]:

Evaluasi Keamanan Informasi menggunakan Indeks KAMI pada Organisasi Pemerintah (kasus Dinas Komunikasi dan Informasi Kabupaten Penukal Abab Lematang Ilir)



Gambar 1.1. Bagan Keterkaitan