

BAB I

PENDAHULUAN

1.1. Latar Belakang

Teknologi berkembang sangat pesat yang ditandai dengan banyaknya jenis pengolahan data yang bertumbuh dan dapat dimanfaatkan dalam kehidupan sehari-hari. Pengolahan data banyak digunakan untuk keperluan pendidikan, industri maupun teknologi komunikasi. Tidak terkecuali oleh lembaga pendidikan seperti universitas. Kemajuan yang sangat cepat ini berpengaruh dalam perkembangan dunia pendidikan yang dapat mengubah proses pembelajaran. Teknologi dapat mempermudah pekerjaan manusia dan meningkatkan produktivitas serta efektivitas kerja. Penggunaan teknologi yang tepat guna dalam hal pendidikan dapat berpengaruh positif dalam meningkatkan pengetahuan dan mempermudah jalannya proses belajar mengajar. Penggunaan teknologi juga membuat pola pendidikan konvensional dapat segera ditinggalkan dan diubah menjadi digital. Namun pemanfaatan teknologi harus dibarengi dengan kesadaran etika yang baik serta kebijakan yang berkaitan dengan keamanan informasi yang perlu diberlakukan untuk melindungi aset penting [1]. Oleh karena itu, keamanan informasi merupakan suatu hal yang harus diperhatikan. Melihat penjelasan diatas diketahui bahwa semakin berkembangnya era teknologi informasi, suatu organisasi telah menerapkan teknologi informasi. Upaya dalam meningkatkan keamanan informasi yang akan diterapkan. Tidak hanya kualitas keamanan informasi yang harus ditingkatkan, tetapi yang lebih penting lagi dalam konsistensi dan keberlangsungan dari keamanan informasi [2].

UPT TIK (Unit Pelaksana Teknis Teknologi Informasi dan Komunikasi) Universitas Trunojoyo Madura merupakan bagian yang berfungsi sebagai pendukung penyelenggaraan pendidikan dalam hal melayani hal-hal yang berhubungan dengan teknologi dan komunikasi secara berkualitas. Sebagai instansi yang telah memanfaatkan teknologi informasi dalam melaksanakan pelayanan akademik UPT TIK (Unit Pelaksana Teknis Teknologi Informasi dan Komunikasi) Universitas Trunojoyo Madura pastinya diperlukan pengawasan dan kontrol untuk mencegah tindak penyalahgunaan teknologi sehubungan dengan rentannya proses pelayanan terhadap serangan siber dan tindak pencurian data.

Berbagai bentuk faktor yang dapat menjadi sumber kerentanan keamanan antara lain faktor teknis, organisasi, peraturan manajemen, lingkungan, dan sistem manajerial lembaga. Informasi merupakan pemicu utama terjadinya kerentanan data. Tingkat kepentingan informasi yang disimpan dan dikelola akan menambah resiko kejahatan siber. Data-data penting dapat menjadi target perusakan, pencurian dan pengeksposan data ke pihak-pihak yang tidak diharapkan. Sehingga akan menambah beban pengamanan informasi di UPT TIK Universitas Trunojoyo Madura.

Keamanan informasi terdiri dari unsur CIA (*Confidentiality, Integrity, dan Availability*), dimana kerahasiaan (*confidentiality*) adalah jaminan keamanan dimana informasi tidak dapat dikendalikan atau diketahui pihak-pihak lain yang tidak dikehendaki. Keutuhan (*integrity*) adalah keaslian informasi yang terhindar dari pemalsuan, pengurangan atau penambahan data yang menyebabkan disinformasi. Kemudian unsur ketersediaan (*availability*) yaitu ketersediaan dimana informasi dapat diakses setiap waktu saat dibutuhkan dan dapat memberikan fungsi yang sesuai dengan kondisi aslinya. Oleh sebab itu kinerja dari tata kelola keamanan informasi yang ada menjadi sangatlah penting karena dengan tata kelola keamanan sistem informasi yang baik dan teratur dapat dijadikan acuan dalam melakukan setiap tindakan [3].

Pelaksanaan pelayanan teknologi informasi dan komunikasi suatu organisasi perlu memperhatikan tentang tata kelola keamanan informasi dari organisasi tersebut. Pemerintah telah menyusun berbagai kebijakan terkait pengelolaan keamanan data diantaranya yaitu Peraturan Menteri Komunikasi dan Informatika No.4 tahun 2021 tentang Sistem Manajemen Pengamanan Informasi. Peraturan ini mencakup berbagai pedoman yang menjadi acuan untuk pengelolaan keamanan data yang dianut oleh sistem internasional. Salah satu pedoman yang tercantum yaitu standar SNI ISO/IEC 27001 atau kerangka kerja Indeks Keamanan Informasi (KAMI) yang disusun oleh Badan Siber dan Sandi Negara. Peraturan perundang-undangan yang mengatur tentang keamanan informasi telah dibuat untuk menghadapi perkembangan tren ancaman dalam keamanan informasi.

Berbagai dampak dapat terjadi sebagai akibat dari resiko ancaman terhadap keamanan data diantaranya pencurian data, akses ilegal tanpa terverifikasi, penggunaan data secara ilegal, penanaman virus sehingga merusak aplikasi layanan atau bahkan merusak alat-alat pelayanan. Tentunya potensi-potensi ancaman seperti ini dapat dicegah dengan adanya sistem pengelolaan keamanan yang memadai. Respons yang cepat terhadap tindakan ancaman keamanan data juga sangat diperlukan sehingga ketika terjadi ancaman, dapat mengurangi dampak yang ditimbulkan lebih jauh [4].

Standar sistem manajemen keamanan informasi menjadi penting dimiliki guna menjamin keamanan informasi dan infrastruktur pelayanan. Sistem manajemen keamanan informasi pada dasarnya ditujukan untuk menjamin pengamanan kerahasiaan data, integritas informasi, dan ketersediaan informasi. Sistem Manajemen Keamanan Informasi (SMKI) terdiri dari 4 proses yaitu proses untuk merencanakan (*plan*), mengimplementasikan (*do*), meninjau ulang atau memonitor (*check*), dan memelihara (*act*) keamanan informasi guna mencapai tujuan organisasi. Pada penerapannya, SMKI dapat menghasilkan manual keamanan informasi, prosedur keamanan informasi, instruksi kerja, dan formulir keamanan informasi [5].

Instansi atau lembaga pelayanan dapat menyesuaikan standar keamanan yang sesuai dengan kebutuhannya untuk menunjang sistem manajemen keamanan informasi. Penelitian sebelumnya telah dilakukan evaluasi keamanan informasi di UPT TIK yang mengacu kepada dua jenis pedoman yang dapat digunakan untuk melakukan pengamanan informasi yaitu standar SNI ISO/IEC 27001 atau kerangka kerja Indeks Keamanan Informasi (KAMI) yang disusun oleh Badan Siber dan Sandi Negara. SNI ISO/IEC 27001 merupakan standar internasional yang fleksibel karena pengembangannya tergantung pada kebutuhan, tujuan, dan persyaratan keamanan organisasi, serta menyediakan sertifikat implementasi SMKI yang diakui secara nasional dan internasional yang disebut *Information Security Management System* (ISMS). SMKI yang menggunakan standar SNI ISO/IEC 27001: 2013 dapat diterapkan pada sebuah organisasi, perusahaan, instansi pemerintahan, dan institusi pendidikan yang menyelenggarakan TIK [4][6].

Berdasarkan kelanjutan penelitian sebelumnya mengenai evaluasi manajemen keamanan informasi pada UPT TIK Universitas Trunojoyo Madura yang melakukan pengukuran tingkat keamanan informasi menggunakan Indeks KAMI 4.2 berdasarkan ISO 27001:2013 sehingga menghasilkan saran rekomendasi untuk perbaikan tingkat keamanan informasi berupa pembuatan prosedur baku dengan acuan kontrol atau kode praktik berdasarkan ISO 27002:2013, yang pada dasarnya keunggulan yang dimiliki oleh ISO 27001 dan 27002 bersifat sama sebagai standar tata kelola keamanan informasi. ISO 27001 diusulkan pada penelitian sebelumnya sebagai standar untuk mengevaluasi tingkat keamanan informasi pada UPT TIK Universitas Trunojoyo Madura serta saran rekomendasi dari hasil penelitian sebelumnya menggunakan acuan kode praktik pada ISO 27002:2013 sebagai bentuk implementasinya. Penggunaan metode ini bertujuan untuk mengetahui standar yang tepat untuk diterapkan pada UPT TIK Universitas Trunojoyo Madura. Dalam memenuhi kebutuhan keamanan informasi sebagai bentuk implementasi berdasarkan hasil saran rekomendasi penelitian sebelumnya dengan menggunakan acuan kode praktik pada ISO 27002:2013 maka diperlukan adanya sebuah tata kelola dalam bentuk dokumen *Standard Operating Procedure* (SOP) keamanan informasi sehingga pada penelitian ini dijadikan sebagai acuan untuk mengusulkan suatu pendekatan praktis dalam penyusunan *Standard Operating Procedure* (SOP) di UPT TIK Universitas Trunojoyo Madura[7].

ISO 27001 memiliki kelebihan di bidang sistem manajemen keamanan informasi dalam lingkup pengelolaan, lingkungannya, pelatihan dan kesadaran. Metode ini harus dimaksimalkan oleh organisasi terhadap *user* atau *brainware* yang mengelolanya, sedangkan 27002 bersifat hampir mirip dengan 27001, namun 27002 lebih fokus kepada teknis pemberdayaan atau pemeliharaan aset dan tingkat keamanan yang dimiliki oleh organisasi dalam bentuk fisik berupa alat atau aset lainnya yang mencakup kedalam tahapan *maintenance* (pemeliharaan) jika dibutuhkan. ISO 27002 adalah seperangkat standar yang berkaitan dengan keamanan dan kontrol informasi yang memungkinkan bisnis untuk menerapkan keamanan yang tepat. Standar ini sebagian besar dilengkapi dengan ISO 27001 yang merinci tugas pengelolaan seperti manajemen resiko dan evaluasi keamanan. Di lain pihak, ISO 27002 banyak berbicara tentang aspek kontrol. ISO 27002 dan

27001 memiliki kesamaan dalam hal pengelolaan yaitu pada poin 7.5 *document information* (27001) & poin 7 *Human resource security* & 8 *Asset management* (27002), poin 7.4 *communication* (27001) & poin 13 *communication security* (27002), poin 8 *operation* (27001) & poin 16 *information security incident management* & 17 *information security aspek of business continuity management* (27002), poin 5 *information security policies* (27001) & poin 7 *Human resource security* (27002), sehingga penggunaan kedua standar ini harus secara berkelanjutan [7].

Pada penelitian sebelumnya dengan judul “Pembuatan *Standard Operating Procedure* (SOP) Keamanan Informasi Berdasarkan *Framework* ISO/IEC 27001:2013 dan ISO/IEC 27002:2013 pada Dinas Komunikasi dan Informatika Pemerintah Kota Madiun” pada tahun 2020 peneliti telah berhasil menyusun 20 prosedur keamanan informasi, termasuk 1 prosedur berupa instruksi kerja yang membahas tata cara bekerja di area yang aman. Selain SOP yang dihasilkan, dalam pembuatan SOP dilengkapi dengan formulir – formulir sebagai instrumen pendukung SOP. Sebagai saran terkait penelitian tersebut, disarankan agar dokumen SOP dan formulir yang telah disusun untuk diuji, diimplementasikan, dan diaudit secara internal. Hal ini bertujuan untuk mengevaluasi sejauh mana dampak penerapan SOP terhadap keamanan informasi di Diskominfo Kota Madiun[7].

Berdasarkan permasalahan yang sudah dipaparkan diatas, penulis ingin melakukan penelitian untuk skripsi dengan judul **“Pembuatan *Standard Operating Procedure* (SOP) Keamanan Informasi Berdasarkan Standar ISO 27002:2013”**. Penelitian ini merupakan lanjutan dari penelitian sebelumnya yang melakukan evaluasi manajemen keamanan informasi dengan menggunakan indeks KAMI 4.2 berdasarkan ISO 27001:2013 yang berfungsi untuk mengukur tingkat keamanan dan kesiapan pada UPT TIK dalam menjaga keamanan informasi disana. Dengan menghasilkan saran rekomendasi berdasarkan acuan kode praktik ISO 27002:2013 tentang pembuatan dokumen prosedur yang baku sebagai bentuk implementasi berdasarkan pada hasil evaluasi tingkat keamanan informasi yang telah dilakukan pada penelitian sebelumnya pada UPT TIK Universitas Trunojoyo Madura[8].

1.2. Perumusan Masalah

Dari penjelasan latar belakang diatas mengenai alasan dilakukannya penelitian ini, maka diperoleh perumusan masalah sebagai berikut:

1. Kontrol objektif dan kontrol keamanan terkait dengan keamanan informasi di UPT TIK belum ada.
2. Hasil pengukuran dan penilaian terhadap tingkat keamanan informasi yang dilakukan oleh penelitian sebelumnya[9] di UPT TIK masih dikategorikan “Tidak Layak” sehingga dibutuhkan dokumen *Standard Operating Procedure* (SOP) sebagai acuan proses pengelolaan keamanan informasi.

1.3. Pertanyaan Penelitian

Dari penjelasan latar belakang diatas mengenai alasan dilakukannya penelitian ini, maka diperoleh pertanyaan penelitian sebagai berikut:

1. Bagaimana menyusun kontrol objektif dan kontrol keamanan terkait dengan keamanan informasi?
2. Bagaimana membuat dokumen *Standard Operating Procedure* (SOP) untuk keamanan informasi yang berdasarkan ISO 27002:2013 pada UPT TIK Universitas Trunojoyo Madura?
3. Apakah hasil dokumen *Standard Operating Procedure* (SOP) keamanan informasi sudah sesuai dengan kebutuhan keamanan pada UPT TIK Universitas Trunojoyo Madura?

1.4. Tujuan Penelitian

Dari beberapa point permasalahan yang telah dipaparkan, didapatkan beberapa tujuan penelitian yang dapat dilihat seperti:

1. Menyusun dokumen kontrol objektif dan kontrol keamanan berdasarkan ISO 27002:2013.
2. Menyusun dokumen *Standard Operating Procedure* (SOP) keamanan informasi pada UPT TIK Universitas Trunojoyo Madura yang berdasarkan hasil analisis keamanan informasi dan sesuai dengan kerangka kerja ISO 27002:2013.
3. Melakukan verifikasi dan validasi dokumen *Standard Operating Procedure* (SOP) oleh pihak UPT TIK serta mengetahui hasilnya sehingga dapat digunakan oleh UPT TIK Universitas Trunojoyo Madura untuk mendukung pengelolaan keamanan informasi.

1.5 Manfaat Penelitian

1. Secara Teoritis
 - a. Mengembangkan keilmuan mengenai ISO 27002:2013.
 - b. Penelitian ini bisa dijadikan sebagai bahan untuk analisis proses pembuatan dokumen *Standard Operating Procedure* (SOP) sebagai panduan maupun acuan dalam hal manajemen keamanan informasi, tak hanya perguruan tinggi, instansi pendidikan, dan lembaga swadaya masyarakat.
 - c. Penelitian ini bisa dijadikan sebagai pedoman bagi peneliti lainnya yang ingin melakukan analisis proses pembuatan dokumen terkait keamanan informasi sebuah dengan ISO 27002:2013 pada UPT TIK Universitas Trunojoyo Madura.
2. Secara Praktis
 - a. Menghasilkan dokumen *Standard Operating Procedure* (SOP) keamanan informasi yang dapat digunakan oleh UPT TIK Universitas Trunojoyo Madura sebagai panduan maupun acuan dalam hal manajemen keamanan informasi.
 - b. Meningkatkan operasional layanan TI yang berkaitan dengan manajemen keamanan informasi dan sesuai dengan kerangka kerja ISO 27002:2013.

1.5. Batasan Masalah

Dari penjelasan latar belakang hingga rumusan masalah dapat ditarik beberapa batasan masalah yang nantinya penelitian ini hanya berfokus pada:

1. Pembuatan *Standard Operating Procedure* (SOP) ditujukan kepada bagian UPT TIK Universitas Trunojoyo Madura.
2. Justifikasi analisis keamanan informasi berdasarkan hasil wawancara dan diskusi dengan pihak UPT TIK Universitas Trunojoyo Madura.
3. Pembuatan dokumen *Standard Operating Procedure* (SOP) keamanan informasi berdasarkan dari hasil rekomendasi penelitian sebelumnya dengan mengacu pada standar ISO 27002:2013.

1.6. Sistematika Laporan

Sistematika penulisan proposal skripsi berformat penulisan Program Studi Sistem Informasi Fakultas Teknik Universitas Trunojoyo Madura.

BAB I PENDAHULUAN

Bab ini membahas tentang permasalahan yang menjadi alasan dari penelitian pada tugas akhir ini, tujuan serta manfaat untuk permasalahan yang ada pada tugas akhir ini.

BAB II KAJIAN PUSTAKA

Bab ini akan membahas mengenai perluasan dari kerangka pemikiran. Di dalamnya dikemukakan definisi-definisi, teori-teori, konsep-konsep yang diperlukan sebagai alat untuk menganalisis gejala dan atau kejadian dan atau situasi yang diteliti. Di dalam bab ini dikemukakan hasil-hasil penelitian yang termaktub di buku-buku teks ataupun makalah-makalah di jurnal-jurnal ilmiah yang terkait.

BAB III METODELOGI PENELITIAN

Bab ini akan membahas mengenai langkah – langkah atau alur jalannya proses penyusunan dokumen *Standard Operating Procedure* (SOP) mengenai keamanan informasi pada UPT TIK UTM.

BAB IV HASIL DAN PEMBAHASAN

Bab ini akan menjelaskan serta menguraikan hasil dan pembahasan dari tahapan yang dilakukan untuk pembuatan dokumen *Standard Operating Procedure* (SOP) berdasarkan dari hasil rekomendasi penelitian sebelumnya dengan mengacu pada standar ISO 27002:2013.

BAB V PENUTUP

Bab ini merupakan penutup yang berisi kesimpulan dari uraian yang sudah diterangkan pada bab-bab sebelumnya dan saran guna untuk pengembangan penelitian yang lebih lanjut.