Kajian Kebijakan Keamanan Sistem Informasi Sebagai Bentuk Perlindungan Kerahasiaan Pribadi Karyawan Perusahaan XYZ

Rio Jumardi[1]

[1] *Sekolah Tinggi Teknologi Bontang*
Jl. Letjen S. Parman No. 65, 75313 Indonesia
jumardirio@gmail.com

Abstract— ***Technology that interconnects computers in the world allows to be able to exchange information and data even communicate with each other in the form of images and video. The more valuable the information is required a security standard to maintain the information.Computer security target, among others, is as protection of information. The higher the security standards provided the higher the privacy protection of information. Protection of employee privacy within a company is one factor that must be considered in the information systems implementation. Information system security policies include: System maintenance, risk handling, access rights settings and human resources, security and control of information assets and server security policies. The policies that have been reviewed will not only be a form of protection of corporate information, but also become a form of protection against the personal confidentiality of XYZ Company employees.***

Abstrak— **Teknologi yang saling menghubungkan komputer didunia memungkinkan untuk dapat saling bertukar informasi dan data bahkan saling berkomunikasi berupa gambar dan video. Semakin berharga sebuah informasi maka diperlukan sebuah standar kemanan untuk menjaga informasi tersebut. Sasaran keamanan komputer antara lain adalah sebagai perlindungan terhadap informasi. Semakin tinggi standar keamanan yang diberikan semakin tinggi pula perlindungan privasi terhadap sebuah informasi. Perlindungan privasi karyawan dalam suatu perusahaan merupakan salah satu faktor yang harus diperhatikan dalam penerapan sistem informasi. Kebijakan keamanan sistem informasi meliputi: Pemeliharaan sistem, penanganan resiko, pengaturan hak akses dan sumber daya manusia, keamanan dan pengendalian asset informasi dan kebijakan keamanan server. Kebijakan-kebijakan yang telah dikaji tidak hanya akan menjadi bentuk perlindungan terhadap informasi perusahaan, tetapi juga menjadi salah satu bentuk perlindungan terhadap kerahasiaan pribadi karyawan Perusahaan XYZ.**

Keywords— **Keamanan Komputer, Kebijakan, Privasi, Sistem Informasi.**

I. Pendahuluan

Saat ini kita berada pada era digital dimana komunikasi dan pertukaran informasi berlangsung dalam suatu jaringan yang kian hari semakin meluas. Teknologi yang saling menghubungkan komputer didunia memungkinkan untuk dapat saling bertukar informasi dan data bahkan saling berkomunikasi berupa gambar dan video. Semakin berharga sebuah informasi maka diperlukan sebuah standar kemanan untuk menjaga informasi tersebut.

Sistem yang dapat diakses dengan ketersediaan yang tinggi saat ini dibutuhkan, keterbukaan dan terdistribusi pasti sudah menjadi keharusan untuk sistem yang terintegrasi. Manajemen keamanan sistem informasi dapat mengurangi terjadinya penyimpangan hak akses oleh pihak tertentu dan pernyalahgunaan data dan informasi sebuah organisasi atau perusahaan [1].

Sasaran keamanan komputer antara lain adalah sebagai perlindungan terhadap informasi. Komponen dari rencana keamanan meliputi: kebijakan, standard dan prosedur keamanan informasi (*policy*), kontrol pengelolaan Sumber Daya Manusia (SDM) untuk keamanan informasi (*people*), dan

kontrol teknologi keamanan informasi (*technology*) [2].

Semakin tinggi standar keamanan yang diberikan semakin tinggi pula perlindungan kerahasiaan pribadi terhadap sebuah informasi. Perlindungan kerahasiaan pribadi karyawan perusahaan XYZ merupakan salah satu faktor yang harus diperhatikan dalam implementasi sistem informasi. Pembuatan kebijakan keamanan sistem informasi diharapkan menjadi kontrol perilaku organisasi atau perusahaan terhdap sistem.

Kerahasiaan pribadi (*privacy*) adalah kemampuan satu atau sekelompok individu untuk mempertahankan kehidupan dan urusan personalnya dari publik, atau untuk mengontrol arus informasi mengenai diri mereka [3] . Privasi kadang dihubungkan dengan anonimitas walaupun anonimitas terutama lebih dihargai oleh orang yang dikenal publik. Privasi dapat dianggap sebagai suatu aspek dari keamanan.

Kejahatan Komputer adalah perbuatan melawan hukum yang dilakukan memakai komputer sebagai sarana/alat atau komputer sebagai objek, baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain.

Kejahatan komputer yang diatur dalam UU ITE diatur dalam Bab VII tentang perbuatan dilarang. Perbuatan-perbuatan tersebut dikategorikan menjadi beberapa kelompok yaitu. [4]

1. Akses tidak sah
2. Penyadapan atau intersepsi tidak sah
3. Gangguan terhadap data komputer.

Kejahatan yang berhubungan erat dengan penggunaan teknologi yang berbasis utama komputer dan jaringan telekomunikasi ini dalam beberapa literatur dan prakteknya dikelompokkan dalam beberapa bentuk, antara lain: [4] [5]

1. *Unauthorized Acces Computer Sistem and Service*, Kejahatan yang dilakukan dengan memasuki/menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa ijin atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya.
2. *Contents*, Merupakan kejahatan dengan menggunakan data atau informasi ke internet tentang suatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hukum atau mengganggu ketertiban umum.
3. *Data Forgery*, Merupakan kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai scriptless document melalui internet.
4. *Cyber Espionage*, Merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer pihak sasaran.
5. *Cyber Sabotage and Extortion,* Kejahatan ini dilakukan dengan membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet.
6. *Offense Against Intellectual Property*, Kejahatan ini ditujukan terhadap hak atas kekayaan intelektual yang dimiliki pihak lain di internet. Contoh, peniruan tampilan pada web page suatu situs milik orang lain secara ilegal, penyiaran suatu informasi di internet yang ternyata merupakan informasi rahasia dagang orang lain dan sebagainya

Inti dari keamanan komputer adalah melindungi komputer dan jaringannya dengan tujuan mengamankan informasi yang berada di dalamnya. Keamanan komputer sendiri meliputi beberapa aspek , antara lain: [6]

1. *Authentication*, penerima informasi dapat memastikan keaslian pesan, bahwa pesan itu datang dari orang yang dimintai informasi. Dengan kata lain, informasi itu benar- benar datang dari orang yang dikehendaki.
2. *Integrity*, keaslian pesan yang dikirim melalui jaringan dan dapat dipastikan bahwa informasi yang dikirim tidak dimodifikasi orang yang tidak berhak.
3. *Non-repudiation*, merupakan hal yang berhubungan dengan si pengirim. Pengirim tidak dapat mengelak bahwa dialah yang mengirim informasi tersebut.
4. *Authority*, informasi yang berada pada sistem jaringan tidak dapat dimodifikasi oleh pihak yang tidak berhak untuk mengaksesnya.
5. *Confidentiality*, merupakan usaha untuk menjaga informasi dari orang yang tidak berhak mengakses. Kerahasiaan ini biasanya

berhubungan dengan informasi yang diberikan ke pihak lain.

6. *Privacy*, lebih ke arah data-data yang bersifat pribadi.
7. *Availability*, aspek availabilitas berhubungan dengan ketersediaan informasi ketika dibutuhkan. Sistem informasi yang diserang atau dijebol dapat menghambat atau meniadakan akses ke informasi.
8. *Access Control*, aspek ini berhubungan dengan cara pengaturan akses ke informasi. Hal ini biasanya berhubungan dengan masalah otentikasi dan privasi. Kontrol akses seringkali dilakukan dengan menggunakan kombinasi user id dan password ataupun dengan mekanisme lain.

Keamanan komputer memberikan persyaratan terhadap komputer yang berbeda dari kebanyakan persyaratan sistem karena sering kali berbentuk pembatasan terhadap apa yang tidak boleh dilakukan komputer. Ini membuat keamanan komputer menjadi lebih menantang karena sudah cukup sulit untuk membuat program komputer melakukan segala apa yang sudah dirancang untuk dilakukan dengan benar. Persyaratan negatif juga sukar untuk dipenuhi dan membutuhkan pengujian mendalam untuk verifikasinya, yang tidak praktis bagi kebanyakan program komputer. Keamanan komputer memberikan strategi teknis untuk mengubah persyaratan negatif menjadi aturan positif yang dapat ditegakkan.

Prinsip utama keamanan sistem informasi terdiri dari *confidentiality* (kerhasiaan), *integrity* (integritas) dan *availability* (ketersediaan) atau sering disebut CIA [7].

Pendekatan yang umum dilakukan untuk meningkatkan keamanan komputer antara lain adalah dengan membatasi akses fisik terhadap komputer, menerapkan mekanisme pada perangkat keras dan sistem operasi untuk keamanan komputer, serta membuat strategi pemrograman untuk menghasilkan program komputer yang dapat diandalkan.

ISO adalah salah satu badan dunia yang membuat standarisasi yang digunakan oleh pengguna atau produsen dalam bidang tertentu. ISO 17799 : 27002 adalah standar yang berisi tentang pengaturan sistem keamanan informasi. [8]

Klausul keamanan dalam ISO diantaranya [8] : *Risk assessment and treatment, security policy, organization of information security, assets management, human resources security, physical and environmental security, communication and operation management, access control, information sistem acquisition, development and maintenance.*

Aspek keamanan informasi meliputi sepuluh aspek diantaranya: [9] kebijakan keamanan, pengorganisasian keamanan, klasisfikasi dan control asset, pengamanan personil, keamanan fisik dan lingkungan, komunikasi dan manajemen operasi, pengontrolan akses, pengembangan dan pemeliharaan sistem, menejemn kelangsungan bisnis, kesuaian.

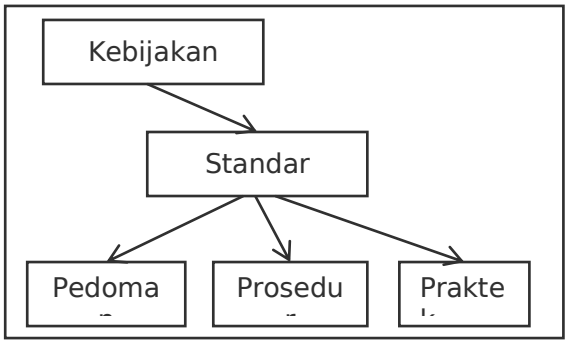
II. METODE PENELITIAN

Metode penelitian yang digunakan adalah metode deskriptif kualitatif yaitu hasil penelitian disajikan dalam bentuk narasi deskripsi. Pendekatan kualitatif dilakukan dalam penelitian ini yaitu dengan merincikan kebijakan keamanan sistem informasi di perusahaan XYZ dengan standard yang ada pada ISO 17799 : 27002, ISO/IEC 27005.

Pengumpulan data dilakukan dengan cara pengamatan langsung dilapangan dan waawancara langsung dengan pengguna akhir sistem dan pengelola sistem dalam hal ini orang yang berkompeten dalam bidang teknologi informasi.

Kebijakan Keamanan Informasi didefinisikan sebagai: Sebuah rencana tindakan untuk menangani masalah keamanan informasi, atau satu set peraturan untuk mempertahankan kondisi atau tingkat keamanan informasi tertentu. [10]

Pembuatan kebijakan (*policy*) didasarkan pada hirarki kebijakan, standar, pedoman, prosedur dan praktek.



Gbr. 1 Hirarki Pembuatan Kebijakan [8]

Kebijakan keamanan informasi meliputi tiga kategori umum diantaranya *Enterprise Information Security Policy* (EISP), *Issue Spesific Security Policy* (ISSP) dan *System Spesific Policy* (SSP). [10]

Penelitian ini akan membahas mengenai EISP yang meliputi pemeliharaan sistem, penanganan resiko, kebijakan hak akses dan sumber daya manusia dan kebijakan keamanan dan pengendalian aset informasi dalam perusahaan serta membahas mengenai ISSP meliputi kebijakan keamanan *server*.

III. HASIL DAN DISKUSI

Dari pendahuluan diatas maka sebuah kajian yang membahas tentang pembuatan kebijakan keamanan sistem informasi akan menjadi salah satu bentuk perlindungan terhadap kerahasiaan pribadi karyawan Perusahaan XYZ.

Diantara beberapa kebijakan yang harus dibuat berdasarkan pada standar ISO 17799 : 27002 dan juga standar yang dikeluarkan oleh ID SIRTII meliputi EISP, ISSP dan SSP.

1. Kebijakan Tentang Perawatan Sistem

   Kebijakan perawatan sistem diperlukan untuk memaksimalkan perawatan terhadap sistem yang berjalan, Kebijakan perawatan sistem Perusahaan XYZ meliputi:

   1) Tujuan: memastikan bahwa sistem informasi yang diimplentasikan berjalan dengan baik.
   2) Standar : yang digunakan adalah standar dari ISO 17799 : 27002 dan Indeks KAMI sebagai alat evaluasi.
   3) Cakupan: penerapan kebijakan ini diperuntukkan kepada pemangku kepentingan dan pegawai yang berkepentingan di bagian Teknologi Informasi dan juga pihak ketiga yang menjadi vendor.
   4) Pedoman perawatan: perawatan sistem harus sesuai dengan pedoman yang berlaku.
   5) Prosedur : membuat prosedur-prosedur yang berkaitan dengan perawatan sistem yang meliputi perawatan korektif, perawatan adaptif, perawatan prefektif dan perawatan preventif.
   6) Monitoring: monitoring diperlukan untuk memantau semua kegiatan yang berhubungan dengan perawatan sistem Perusahaan XYZ

2. Kebijakan Penanganan Resiko

   Kebijakan penanganan resiko diperlukan untuk menangani resiko-resiko yang mungkin ada pada saat implemntasi sistem, Kebijakan penanganan resiko Perusahaan XYZ meliputi:

   1) Tujuan: mengidentifikasi dan menganalisis kemungkinan resiko yang ada pada implemntasi sistem informasi diperusahaan XYZ.
   2) Standar : yang digunakan adalah standar dari ISO 17799 : 27002, ISO/IEC 27005, Metode Octave Allegro.
   3) Cakupan: penerapan kebijakan ini diperuntukkan kepada semua pegawai di lingkungan perusahaan XYZ yang berhubungan dengan asset informasi.
   4) Pedoman pengangan resiko: pengangan resiko terhadap sistem dan asset informasi yang berjalan harus sesuai dengan pedoman yang berlaku.
   5) Prosedur : membuat prosedur-prosedur yang berkaitan dengan manajemen resiko yang meliputi mengembangkan kriteria pengukuran resiko, mengembangkan profil asset informasi, mengidentifikasi container dari aset informasi, mengidentifikasi area masalah, mengidentifikasi scenario ancaman, mengidentifikasi resiko, menganalisis resiko, dan memilih pendekatan pemilihan pemilihan penangan risiko.
   6) Monitoring: monitoring diperlukan untuk memantau semua kegiatan yang berhubungan dengan penanganan resiko Perusahaan XYZ

3. Kebijakan Sumber daya Manusia Pengaturan Hak Akses

   Kebijakan sumber daya manusia dan pengaturan hak akses diperlukan untuk mengatur batasan-batasan dari pengguna sistem informasi di

lingkungan Perusahaan XYZ. Kebijakan sumber daya manusia dan pengaturan hak akses perusahaan XYZ meliputi:

1) Tujuan: mengendalikan akses pengguna sistem informasi dengan mengatur hak akses pengguna. Tujuan lainnya sebagai upaya pengurangan resiko dari penyalahgunaan fungsi atau wewenang akibat kesalahan manusia.
2) Standar : yang digunakan adalah standar dari ISO 27002 dan Information Technology Infrastructur Library (ITIL) V3.
3) Cakupan: penerapan kebijakan ini diperuntukkan kepada pemangku kepentingan dan pimpinan perusahaan untuk menentukan atau mengelola penentuan sumber daya manusia dengan pengaturan hak akses terhadap sistem.
4) Pedoman: penetuan pengaturan hak akses terhadap sistem harus sesuai dengan pedoman dan aturan yang berlaku dilingkungan Perusahaan XYZ. Disesuaian juga dengan kemampuan sistem informasi mengelola hak akses
5) Prosedur: membuat prosedur-prosedur yang berkaitan dengan pengaturan hak akses yang meliputi permintaan akses, pemberian akses, pemantauan identitas pengguna, penilaian kinerja pegawai, perilaku kerja pegawai, pembatasan akses, penghapusan akses, permasalahan akses dan pencatatan akses.
6) Monitoring: monitoring diperlukan untuk memantau semua kegiatan yang berhubungan dengan pengelolaan sumber daya manusia dan pengaturan hak akses sistem infromasi di Perusahaan XYZ.

4. Kebijakan Keamanan dan Pengendalian Aset Informasi

Kebijakan keamanan dan pengendalian asset diperlukan untuk mengatur dan mengelola asset informasi perusahaan. Kebijakan keamanan dan pengendalian asset informasi perusahaan XYZ meliputi:

1) Tujuan: memberikan perlindungan terhadap asset perusahaan berdasarkan tingkat perlindungan yang diberikan.
2) Standar : yang digunakan adalah standar dari ISO 17799:27002.
3) Cakupan: penerapan kebijakan ini diperuntukkan kepada pemangku kepentingan dan pimpinan perusahaan beserta seluru pegawai terhadap keamanan asset informasi dalam penggunaan sistem informasi.
4) Pedoman: Pedoman keamanan dan pengendalian asset informasi di lingkungan perusahaan XYZ harus disesuaian dengan aturan-aturan yang berlaku baik aturan dari sistem informasi maupun aturan dari perusahaan.
5) Prosedur: membuat prosedur-prosedur yang berkaitan dengan keamanan asset dan pengendalian asset informasi meliputi klasifikasi informasi dan tanggungjawab informasi.
6) Monitoring: monitoring diperlukan untuk memantau semua kegiatan yang berhubungan dengan pengendalian aset informasi sistem informasi di Perusahaan XYZ.

5. Kebijakan Keamanan *Server*

Kebijakan lain yang harus diperhatikan oleh perusahaan XYZ adalah kebijakan keamanan *server*. Kebijakan ini diperlukan untuk memaksimalkan keamanan terhadap *server* data yang secara langsung juga akan menjaga kerahasiaan data Perusahaan XYZ dan data privasi karyawan Perusahaan XYZ terhadap kejahatan komputer yang akan merugikan Perusahaan XYZ.

Kebijakan Keamanan *Server* Perusahaan XYZ meliputi:

1) Tujuan: memaksimalkan keamanan sistem informasi Perusahaan XYZ dari *server* yang digunakan.
2) Standar : yang digunakan adalah standar dari ISO 17799 : 27002 dan Indeks KAMI untuk sebagai alat evaluasi.
3) Cakupan: penerapan kebijakan ini diperuntukkan kepada pemangku kepentingan dan pegawai yang berkepntingan di bagian Teknologi Informasi

4) Pedoman konfigurasi umum: Konfigurasi *server* harus sesuai dengan pedoman yang berlaku.
5) Prosedur: membuat prosedur-prosedur yang berkaitan dengan keamanan *server* melitputi: prosedur pembuatan *server* sendiri, prosedur penyimpanan *server*, prosedur keamanan ruangan *server*, penjaga *server*, dan penggunaan *sever*.
6) Monitoring: monitoring diperlukan untuk memantau semua kegiatan yang berhubungan dengan keamanan *server* Perusahaan XYZ

IV. KESIMPULAN

Penerapan kebijakan-kebijakan yang berkaitan dengan keamanan sistem informasi adalah penting dilakukan sebagai bentuk perlindungan terhadap informasi perusahaan XYZ.

Kebijakan-kebijakan yang diperlukan antara lain: Pemeliharaan sistem, penanganan resiko, pengaturan hask akses dan sumber daya manusia, keamanan dan pengendalian asset informasi dan kebijakan keamanan *server*.

Perlindungan yang diberikan tidak hanya terhadap informasi Perusahaan XYZ akan tetapi perlindungan juga akan diberikan terhadap kerahasiaan pribadi karyawan Perusahaan XYZ.

Saran berkaitan dengan penelitian ini adalah perusahaan XYZ dapat mengevaluasi kebijakan keamanan informasi menggunakan metode-metode yang ada seperti Indeks KAMI, ITIL dan metode-metode yang lain.

REFERENSI

V.

[1] Wildan Radista Wicaksana, Anisah Herdiyanti , and Tony Dwi Susanto, "Pembuatan Standar Operasional Prosedur (SOP) Manajemen Akses Untuk Aplikasi E-Performance Bina Program Kota Surabaya Berdasarkan Kerangka Kerja ITIL V3 Dan ISO 27002," *Jurnal Sisfo*, vol. 06, no. 01, pp. 105-120, September 2016.

[2] Aan AlBOne, "Pembuatan Rencana Keamana Informasi Berdasarkan Analisis dan Mitigasi Risiko Teknologi Informasi," *Jurnal Informatika*, vol. 10, pp. 44-52, Mei 2009.

[3] "http://id.wikipedia.org/wiki/Kerahasiaan_pribadi," 2013.

[4] Ana Maria F. Pasaribu, "Kejahatan Siber Sebagai Dampak Negatif dari Perkembangan Teknologi dan Internet di Indonesia Berdasarkan Undang-undang No. 19 Tahun 2016 Perubahan atas Undang-undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik dan Perspektif Hukum Pidana," Universitas Sumatera Utara, Medan, Thesis 2017.

[5] Dodo Zaenal Abidin, "Kejahatan dalam Teknologi Informasi dan Komunikasi," *Jurnal Ilmiah Media Processor*, vol. 10, no. 2, pp. 509-516, Oktober 2015.

[6] Muhammad Siddik Hasibuan, "Keylogger Pada Aspek Keamanan Komputer," *Jurnal Teknovasi*, vol. 03, no. 1, pp. 8-15, 2016.

[7] Deni Ahmad Jakaria, R. Teduh Dirgahayu, and Hendrik, "Manajemen Risiko Sistem Informasi Akademik pada Perguruan Tinggi Menggunakan Metoda Octave Allegro," in *Seminar Nasional Aplikasi Teknologi Informasi (SNATI)*, Yogyakarta, 2013, pp. E- 37-42.

[8] Deris Stiawan, "Kebijakan Sistem Informasi Manajemen Keamanan IT (Information Security Management Policy) Standard ISO 17799 : 27002," Universitas Sriwijaya, Palembang, 2009.

[9] Prof. Richardus Eko Indrajit, "ISO17799. Kerangka Standar Keamanan Infromasi," id-SIRTII, Jakarta, 2018.

[10] Iwan Sumantri. (2018, Mei) ID SIRTII. [Online]. http://cdn.woto.com/dsfile/49ba65ea-0804-46c3-aa21-86d156d167f9