Journal of International Multidisciplinary Research

Analisis Kebijakan Keamanan Sistem Informasi Untuk Melindungi Kerahasiaan Data Pribadi Karyawan Di Perusahaan XYZ

Jayadi[1], Tori Sutisna[2], Zamjam Ginanjar[3]
[1]Universitas Bandung, Bandung, Indonesia, [2]STMIK Tulus Cendekia, Bandung, Indonesia, [3]Universitas Halim Sanusi, Bandung, Indonesia
jayadi@bandunguniversity.ac.id[1], torisutisna77@tuluscendekia.ac.id[2], zamjamginanjar@uhs.ac.id[3]

Informasi Artikel
E-ISSN : 3026-6874
Vol: 2 No: 7 Juli 2024
Halaman : 73-79

Keywords:
Support System, Topsis Method.

Abstract
Global data exchange between computers enables communication involving information in the form of images and videos. Information that has high value requires security standards to safeguard it. The main goal of computer security is to protect that information, while enhancing privacy. Protecting employee privacy in a company is important in implementing information systems. Information system security policies include system maintenance, risk management, access rights settings and human resource management, asset information security, and server policies. This policy not only protects company information, but also protects employee confidentiality.

Abstrak
Pertukaran data antar komputer secara global memungkinkan komunikasi yang melibatkan informasi berupa gambar dan video. Informasi yang memiliki nilai tinggi memerlukan standar keamanan untuk menjaganya. Tujuan utama keamanan komputer adalah melindungi informasi tersebut, yang sekaligus meningkatkan privasi. Perlindungan privasi karyawan dalam sebuah perusahaan menjadi hal penting dalam implementasi sistem informasi. Kebijakan keamanan sistem informasi mencakup pemeliharaan sistem, manajemen risiko, pengaturan hak akses dan manajemen sumber daya manusia, keamanan aset informasi, dan kebijakan server. Kebijakan ini tidak hanya melindungi informasi perusahaan, tetapi juga menjaga kerahasiaan karyawan.

Kata Kunci : Keamanan, Sistem Informasi, Data Pribadi.

PENDAHULUAN

Pertukaran informasi antar komputer di seluruh dunia telah membuka jalan bagi komunikasi yang melibatkan data-data berharga seperti gambar dan video. Namun, dengan nilai informasi yang semakin tinggi, perlindungan yang serius diperlukan. Keamanan komputer menjadi kunci utama dalam menjaga kerahasiaan data yang vital ini, yang pada gilirannya meningkatkan privasi individu(Raharja, 2024). 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(Ramalinda, Jayadi, et al., 2024).

Di dalam konteks perusahaan, terutama di Perusahaan XYZ, perlindungan privasi karyawan merupakan elemen krusial dalam penerapan sistem informasi(Ramalinda & Raharja, 2024). Kebijakan keamanan sistem informasi menjadi pondasi yang kuat dalam menjaga kerahasiaan data pribadi karyawan(Ramalinda, Raharja, et al., 2024). Kebijakan ini mencakup berbagai aspek, mulai dari pemeliharaan sistem dan manajemen risiko hingga pengaturan hak akses, manajemen sumber daya manusia, dan kebijakan keamanan server. Manajemen keamanan sistem informasi dapat mengurangi terjadinya penyimpangan hak akses oleh pihak tertentu dan penyalahgunaan data dan informasi sebuah organisasi atau perusahaan.

Sasaran keamanan komputer antara lain adalah sebagai perlindungan terhadap informasi(Sutisna et al., 2024). Komponen dari rencana keamanan meliputi: kebijakan, standar dan prosedur keamanan informasi (policy), kontrol pengelolaan Sumber Daya Manusia (SDM) untuk keamanan informasi (people), dan kontrol teknologi keamanan informasi (technology)(Hariyanti et al., 2024).

Kejahatan komputer adalah tindakan ilegal atau tidak sah yang melibatkan penggunaan komputer atau teknologi informasi untuk merugikan orang lain, memperoleh keuntungan secara tidak sah, atau merusak sistem komputer(Erwis et al., 2024). Ini bisa berupa aksi yang dilakukan dengan menggunakan komputer sebagai alat atau sarana untuk melakukan kejahatan, atau juga melibatkan aksi yang ditujukan pada komputer itu sendiri sebagai objek kejahatan. Kejahatan komputer yang diatur dalam UU ITE diatur dalam Bab VII tentang perbuatan dilarang. Perbuatan- perbuatan tersebut dikategorikan menjadi beberapa kelompok yaitu: akses tidak sah, penyadapan atau intersepsi tidak sah, gangguan terhadap data komputer.

Kejahatan yang berhubungan erat dengan penggunaan teknologi(Muchsam et al., 2023) yang berbasis utama komputer dan jaringan telekomunikasi(Rismayadi et al., 2024) ini dalam beberapa literatur dan prakteknya dikelompokkan dalam beberapa bentuk

Keamanan komputer memberikan strategi teknis untuk mengubah persyaratan negatif menjadi aturan positif yang dapat ditegakkan. Prinsip utama keamanan sistem informasi terdiri dari confidentiality (kerahasiaan), integrity (integritas) dan availability (ketersediaan) atau sering disebut CIA(Ramalinda, Jayadi, et al., 2024).

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(Rahayu et al., 2024).

Klausul keamanan dalam ISO diantaranya: 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 system acquisition, development and maintenance. Aspek keamanan informasi meliputi seluruh aspek diantaranya:(Raharja et al., 2004) kebijakan keamanan, pengorganisasian keamanan, klasifikasi dan control asset, pengamanan personil, keamanan fisik dan lingkungan, komunikasi dan manajemen operasi, pengontrolan akses, pengembangan dan pemeliharaan sistem, manajemen kelangsungan bisnis, kesesuaian.

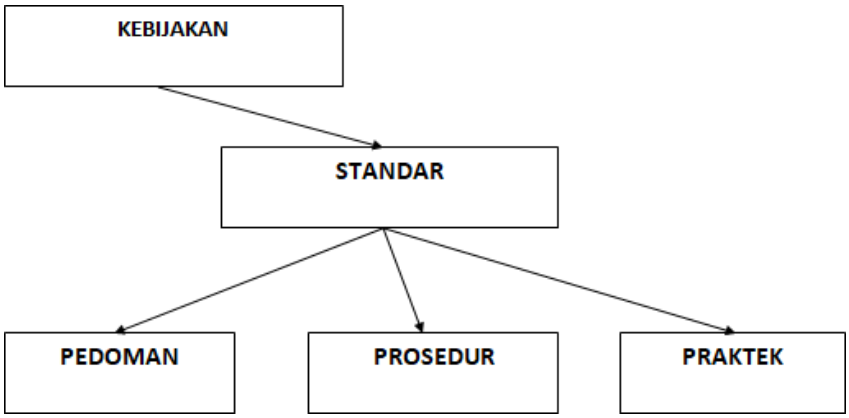
Dalam pandangan ini, kebijakan keamanan sistem informasi bukan hanya tentang melindungi informasi perusahaan, tetapi juga tentang menjaga privasi individu karyawan. Dengan mempertimbangkan kompleksitas tantangan keamanan informasi saat ini, penelitian ini akan menganalisis secara mendalam kebijakan keamanan sistem informasi yang diterapkan di Perusahaan ABC, dengan fokus khusus pada perlindungan kerahasiaan data pribadi karyawan.

METODE

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 ABC dengan standar yang ada pada ISO 17799 : 27002, ISO/IEC 27005.

Pengumpulan data dilakukan dengan cara pengamatan langsung dilapangan dan wawancara 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.



Gambar 1. Hirarki Pembuatan Kebijakan [8]

Kebijakan keamanan informasi meliputi tiga kategori umum diantaranya Enterprise Information Security Policy (EISP), Issue Specific Security Policy (ISSP) dan System Spesific Policy (SSP). . Penelitian ini akan membahas mengenai EISP yang meliputi pemeliharaan sistem, penanganan risiko, kebijakan hak akses dan sumber daya manusia dan kebijakan keamanan dan pengendalian aset informasi dalam perusahaan serta membahas mengenai ISSP meliputi kebijakan keamanan server.

HASIL DAN PEMABAHASAN

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 ABC.

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 ABC meliputi:

   a. Tujuan: memastikan bahwa sistem informasi yang diimplementasikan berjalan dengan baik.
   b. Standar : yang digunakan adalah standar dari ISO 17799 : 27002 dan Indeks KAMI sebagai alat evaluasi.
   c. Cakupan: penerapan kebijakan ini diperuntukkan kepada pemangku kepentingan dan pegawai yang berkepentingan di bagian Teknologi Informasi dan juga pihak ketiga yang menjadi vendor.
   d. Pedoman perawatan: perawatan sistem harus sesuai dengan pedoman yang berlaku.
   e. Prosedur : membuat prosedur- prosedur yang berkaitan dengan perawatan sistem yang meliputi perawatan korektif, perawatan adaptif, perawatan preventif dan perawatan preventif.
   f. Monitoring: monitoring diperlukan untuk memantau semua kegiatan yang berhubungan dengan perawatan sistem Perusahaan ABC

2. Kebijakan Penanganan Risiko

Kebijakan penanganan risiko diperlukan untuk menangani resiko- resiko yang mungkin ada pada saat implementasi sistem, Kebijakan penanganan risiko Perusahaan ABC meliputi:

a. Tujuan: mengidentifikasi dan menganalisis kemungkinan resiko yang ada pada implementasi sistem informasi di perusahaan ABC.
b. Standar : yang digunakan adalah standar dari ISO 17799 : 27002, ISO/IEC 27005, Metode Octave Allegro.
c. Cakupan: penerapan kebijakan ini diperuntukkan kepada semua pegawai di lingkungan perusahaan ABC yang berhubungan dengan aset informasi.
d. Pedoman penanganan resiko: pengurangan resiko terhadap sistem dan aset informasi yang berjalan harus sesuai dengan pedoman yang berlaku.
e. Prosedur : membuat prosedur- prosedur yang berkaitan dengan manajemen risiko yang meliputi mengembangkan kriteria pengukuran risiko, mengembangkan profil asset informasi, mengidentifikasi container dari aset informasi, mengidentifikasi area masalah, mengidentifikasi skenario ancaman, mengidentifikasi risiko, menganalisis risiko, dan memilih pendekatan pemilihan pemilihan penanganan risiko.
f. Monitoring: monitoring diperlukan untuk memantau semua kegiatan yang berhubungan dengan penanganan risiko Perusahaan ABC

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 ABC. Kebijakan sumber daya manusia dan pengaturan hak akses perusahaan ABC meliputi:

a. 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.
b. Standar : yang digunakan adalah standar dari ISO 27002 dan Information Technology Infrastructure Library (ITIL) V3.
c. 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.
d. Pedoman: penentuan pengaturan hak akses terhadap sistem harus sesuai dengan pedoman dan aturan yang berlaku di lingkungan Perusahaan ABC. Disesuaikan juga dengan kemampuan sistem informasi mengelola hak akses
e. 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.
f. Monitoring: monitoring diperlukan untuk memantau semua kegiatan yang berhubungan dengan pengelolaan sumber daya manusia dan pengaturan hak akses sistem informasi di Perusahaan ABC.

4. Kebijakan Keamanan dan Pengendalian Aset Informasi

Kebijakan keamanan dan pengendalian aset diperlukan untuk mengatur dan mengelola aset informasi perusahaan. Kebijakan keamanan dan pengendalian aset informasi perusahaan ABC meliputi:

a. Tujuan: memberikan perlindungan terhadap aset perusahaan berdasarkan tingkat perlindungan yang diberikan.
b. Standar : yang digunakan adalah standar dari ISO 17799:27002.

c. Cakupan: penerapan kebijakan ini diperuntukkan kepada pemangku kepentingan dan pimpinan perusahaan beserta seluruh pegawai terhadap keamanan aset informasi dalam penggunaan sistem informasi.
d. Pedoman: Pedoman keamanan dan pengendalian aset informasi di lingkungan perusahaan ABC harus disesuaikan dengan aturan- aturan yang berlaku baik aturan dari sistem informasi maupun aturan dari perusahaan.
e. Prosedur: membuat prosedur- prosedur yang berkaitan dengan keamanan aset dan pengendalian aset informasi meliputi klasifikasi informasi dan tanggungjawab informasi.
f. Monitoring: monitoring diperlukan untuk memantau semua kegiatan yang berhubungan dengan pengendalian aset informasi sistem informasi di Perusahaan ABC.

5. Kebijakan Keamanan Server

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

a. Tujuan: memaksimalkan keamanan sistem informasi Perusahaan ABC dari server yang digunakan.
b. Standar : yang digunakan adalah standar dari ISO 17799 : 27002 dan Indeks KAMI untuk sebagai alat evaluasi.
c. Cakupan: penerapan kebijakan ini diperuntukkan kepada pemangku kepentingan dan pegawai yang berkepentingan di bagian Teknologi Informasi
d. Pedoman konfigurasi umum: Konfigurasi server harus sesuai dengan pedoman yang berlaku.
e. Prosedur: membuat prosedur- prosedur yang berkaitan dengan keamanan server meliputi: prosedur pembuatan server sendiri, prosedur penyimpanan server, prosedur keamanan ruangan server, penjaga server, dan penggunaan sever.
f. Monitoring: monitoring diperlukan untuk memantau semua kegiatan yang berhubungan dengan keamanan server Perusahaan ABC.

KESIMPULAN

Implementasi kebijakan-kebijakan terkait keamanan sistem informasi menjadi krusial dalam menjaga integritas informasi di Perusahaan ABC. Kebijakan-kebijakan tersebut mencakup pemeliharaan sistem, manajemen risiko, pengaturan hak akses, pengelolaan sumber daya manusia, pengendalian aset informasi, dan kebijakan keamanan server. Perlindungan yang diberikan tidak hanya terbatas pada informasi perusahaan, tetapi juga meliputi kerahasiaan pribadi karyawan Perusahaan ABC.

Saran yang dapat diberikan adalah agar Perusahaan ABC melakukan evaluasi terhadap kebijakan keamanan informasi dengan menggunakan berbagai metode yang tersedia, seperti Indeks KAMI, ITIL, dan metode-metode lainnya. Dengan demikian, upaya peningkatan keamanan dan perlindungan informasi serta privasi karyawan dapat dilakukan secara lebih efektif dan terukur.

REFERENCES

Erwis, F., Jixiong, C. ., Rahayu, N. ., Raharja, A. R. ., & Zebua, R. S. Y. . (2024). Use of Augmented Reality (AR) in Mobile Learning for Natural Science Lessons. Journal of Social Science Utilizing Technology, 2(1), 338–348. https://doi.org/10.55849/jssut.v2i1.784

Hariyanti, I., & Raharja, A. R. (2024). Perbandingan Algoritma Decision Tree dan Naive Bayes dalam Klasifikasi Data Pengaruh Media Sosial dan Jam Tidur Terhadap Prestasi Akademik Siswa. Technologia: Jurnal Ilmiah, 15(2), 332-340.

Muchsam, Y., Sucipto, B., Rismawati, R., Rusdianti, I. S., & Raharja, A. R. (2023). Forming the Character of a Physically Healthy Young Generation Through Military Education. TGO Journal of Community Development, 1(2), 90-95.

Rachmat, A. R. A., Jayadi, J., & Ginanjar, Z. G. Z. (2023). DESIGN AND IMPLEMENTATION OF ATTENDANCE USING RFID CARDS USING C# AT BANDUNG UNIVERSITY. ABDITEK NUSANTARA, 5(2), 1-9.

Rachmat, R. A., & Ifani, H. (2023). Design of EMR (Electronic Medical Record) Applications Using RFID Cards to Record Patient Medical Record Data at The Sukajadi Bandung Health Center. 66–72.

Raharja, A. R. (2024). KEAMANAN JARINGAN. PENERBIT KBM INDONESIA.

Raharja, A. R., Pramudianto, A., & Muchsam, Y. (2024). Penerapan Algoritma Decision Tree dalam Klasifikasi Data " Framingham " Untuk Menunjukkan Risiko Seseorang Terkena Penyakit Jantung dalam 10 Tahun Mendatang. nawalaeducation, 1(1). https://doi.org/10.62872/cwgzp962

Raharja, A. R., Ramalinda, D., Hariyanti, I.(2024). ALGORITMA DAN PEMROGRAMAN MENGGUNAKAN PYTHON DENGAN APLIKASI GOOGLE COLLABS. Mafy Media Literasi.

Raharja, A. R., Setiyono, R., & Hariyanti, I. (2024). Implementasi Aplikasi Surface Roughness Tester atau Alat Ukur Kekasaran Permukaan Jalan Menggunakan C# dan Arduino. Media Informatika, 23(1), 1-9.

Raharja, A. R., Setiyono, R., & Hariyanti, I. (2024). PERANCANGAN DAN IMPLEMENTASI CALIFORNIA BEARING RATIO (CBR) DENGAN MENGGUNAKAN C# DAN ARDUINO. Jurnal Responsif: Riset Sains dan Informatika, 6(1), 54-62.

Rahayu, T., Yayat, E., & Raharja, A. R. (2024). Analisis Tata Ruang Penyimpanan Guna Menunjang Sistem Pelayanan Kesehatan Di Santosa Hospital Bandung Central Tahun 2021. Journal of Public Health Indonesian, 1(1).

Ramalinda, D., & Raharja, A. R. (2024). DECISION SUPPORT SYSTEM FOR SELECTING RECIPIENTS OF HOME RENOVATION ASSISTANCE USING THE TOPSIS METHOD. International Journal of …, 42(1), 17–24. https://jicnusantara.com/index.php/jicn/article/view/535

Ramalinda, D., Raharja, A. R., Sali Setiatin, M. H., & Angga Pramudianto, J. (2024). PENGANTAR TEKNOLOGI INFORMASI PADA REKAM MEDIS. Mafy Media Literasi.

Ramalinda, D., Raharja, A. R., Sali Setiatin, M. H., & Angga Pramudianto, J. (2024). PENGANTAR TEKNOLOGI INFORMASI PADA REKAM MEDIS. Mafy Media Literasi.

Rismayadi, A. A., Wiguna, W., Muchsam, Y., Rumaisa, F., Jayadi, Pramudianto, A., & Raharja, A. R. (2024). PEMBELAJARAN C#. In Mafy Media Literasi.

Sutisna, T., Raharja, A. R., Solihin, S., Hariyadi, E., & Cahaya Putra, V. H. (2024). Penggunaan Computer Vision untuk Menghitung Jumlah Kendaraan dengan Menggunakan Metode SSD (Single Shoot Detector). Innovative: Journal Of Social Science Research, 4(2), 6060–6067. https://doi.org/10.31004/innovative.v4i2.10071

Tiur, M., & Raharja, A. R. (2024). ANALISIS ALUR PENDAFTARAN PASIEN RAWAT JALAN PADA MASA PANDEMI COVID-19 DI PUSKESMAS SARIJADI. EMPIRIS: Jurnal Sains, Teknologi dan Kesehatan, 1(1), 24-36.

Tiur, M., & Raharja, A. R. (2024). TINJAUAN KETIDAK LENGKAPAN PENGISIAN FORMULIR INFORMED CONSENT POLI BEDAH PADA BULAN JANUARI 2022. Journal of Ostetricia, 1(1), 10-15.

Tiur, M., Setiatin, S., Ramalinda, D., & Raharja, A. R. (2024). ANALISIS DIMENSI MUTU TERHADAP TINGKAT KEPUASAN PELAYANAN KESEHATAN PADA ERA PANDEMI COVID-19 (Di Puskesmas Cikembar Tahun 2020). 19.

Tiur, M., Setiatin, S., Ramalinda, D., & Raharja, A. R. (2024). Analysis of Quality Dimensions on The Level of Satisfaction of Health Services in The Covid-19 Pandemic Era (at Cikembar Health Center in 2020). Journal of Student Collaboration Research, 1(1), 30-35.