Journal Akuntansi Manajerial
ISSN (E): 2502-6704
Vol. 10, No 01 Jan-Juni 2025 Hal. 48 - 54
http://journal.uta45jakarta.ac.id/index.php/JAM/index

Peran Sistem Informasi Akuntansi Dalam Meningkatkan Keamanan Perusahaan Melalui Pengaplikasian Enkripsi

[1]Nadhifatul Lailiyah
[1]*Faculty of economics and business pascasarjana, Perbanas Institute*
nadhifatullailiyah90@gmail.com

[2]Mardani Supranata
[2]*Faculty of economics and business pascasarjana, Perbanas Institute*
mardanisupranata2016@gmail.com

Abstract— Untuk membantu eksekutif bisnis dan akuntan membuat keputusan yang tepat, sistem informasi akuntansi (SIA) dibuat untuk mengumpulkan data akuntansi, layanan pelanggan, kemudahan pengambilan keputusan, dan efisiensi akan meningkat dengan sistem yang baik. Kelangsungan bisnis dilindungi, risiko diminimalkan, dan pengambilan keputusan investasi dan peluang bisnis dipercepat berkat keamanan data. Karena kebocoran data dan Kegagalan sistem dapat menyebabkan kehilangan uang dan produktivitas, perusahaan harus memperhatikan keamanan aset informasinya. Di era perkembangan sistem informasi yang sangat cepat ini, sangat penting untuk memperhatikan keamanan informasi perusahaan agar tidak dimiliki oleh individu yang tidak memiliki hak atau tanggung jawab. Memanfaatkan teknologi informasi memiliki banyak keuntungan, terutama bagi bisnis. Bisnis dapat menyediakan, mengelola, dan melaporkan informasi keuangan dengan cepat, mudah, dan akurat dengan menggunakan teknologi informasi. Pencurian data, penggunaan sistem yang melanggar hukum, penghancuran data yang melanggar hukum, dan modifikasi yang melanggar hukum, dan kegagalan sistem adalah beberapa ancaman terhadap sistem informasi yang dapat dicegah.

***Kata Kunci*— Enkripsi, Keamanan Data, Sistem Informasi Akuntansi**

I. INTRODUCTION

Perkembangan sistem informasi saat ini sangat pesat, penting untuk memperhatikan keamanan data. Seseorang yang tidak bertanggung jawab dapat mengambil alih data. Sebagian orang mengatakan bahwa saat ini telah masuk dalam "masyarakat informasi", artinya masyarakat yang menjadikan penciptaan, distribusi, dan pengelolaan informasi sebagai kegiatan ekonomi, politik, dan budaya yang penting. Dalam masyarakat informasi, kualitas hidup, pembangunan ekonomi, dan prospek perubahan sosial bergantung pada peningkatan informasi dan pemanfaatnya. Setiap organisasi, baik itu perusahaan, sekolah, lembaga pemerintah, maupun individu, membutuhkan kemampuan untuk mengumpulkan dan menyampaikan data dengan cepat dan akurat. Pengamanan data sangat penting, tentu saja data pribadi maupun perusahaan. Kemampuan untuk mencegah penyalahgunaan data diperlukan untuk perlindungan data dari orang yang tidak bertanggungjawab. Semua data mengandung informasi penting yang harus disimpan secara rahasia. Untuk melindungi data, proses enkripsi perlu digunakan untuk mengubah data menjadi *ciphertext* atau informasi yang tidak dapat dipahami.

Sensitivitas data yang disimpan dalam database memengaruhi tingkat keamanan data, data yang tidak sensitif tidak memerlukan sistem perlindungan yang ketat, tetapi informasi yang sangat sensitif memerlukan sistem keamanan yang ketat untuk dapat mengakses ke data, (Wulandari, 2023). Sayangnya, pemilik dan pengelola sistem informasi seringkali mengabaikan keamanan data, yang merupakan salah satu dari komponen penting dari sebuah sistem data. Seringkali, keamanan dilemahkan atau dihilangkan jika mengganggu pengoperasian sistem. Banyak pengembang dan analisis pada saat itu membangun keamanan sistem informasi, pada akhirnya ditinggalkan oleh pengguna. Ini disebabkan oleh sistem yang dibangun dengan tujuan membuat sistem sulit untuk digunakan atau tidak cerdas, keamanan sistem informasi yang tidak terjamin, ketidaksamaan sistem yang mengharuskan pengguna mengikuti prosedur yang ada, dan tidak interaktif dan tidak nyaman.

Adanya peningkatan kesadaran mengelola sistem informasi dalam manajemen perusahaan. Tujuan keamanan data adalah untuk mencegah pencurian sistem data, terlepas dari kenyataan bahwa keamanan komputer mengacu pada

Vol. 10, No 01 Jan-Juni 2025 Hal. 48 - 54
http://journal.uta45jakarta.ac.id/index.php/JAM/index

keamanan data yang digunakan pada komputer dan jaringannya. Dunia telah menyaksikan sejumlah besar pelanggaran keamanan data dalam beberapa tahun terakhir. Kasus yang paling terkenal adalah peretasan akun data menkominfo Indonesia pada tahun 2022, peretasan akun Marriott International, dan kasus Facebook Cambridge Analytica. Akibatnya, sangat penting bagi perusahaan untuk mempertimbangkan dan meningkatkan tingkat keamanan data dan privasi pengguna. Didasarkan pada informasi di atas, dapat disimpulkan bahwa keamanan sistem informasi adalah hal yang sangat penting untuk Dunia saat ini dan harus dibangun dari perspektif pengguna sehingga proses pengambilan keputusan tidak terganggu.

II. METHODS

Artikel ini ditulis dengan metode penelitian kepustakaan atau penelitian literatur. Referensi dari penelitian sebelumnya dikumpulkan untuk membuat tinjauan pustaka, yang kemudian digabungkan menjadi kesimpulan. (Elim, 2014). Berbagai sumber dapat digunakan untuk mendapatkan tinjauan pustaka, seperti buku, dokumen, surat kabar, internet, dan perpustakaan. Penelitian kepustakaan mencakup berbagai tindakan yang berkaitan dengan pengelolaan makalah, membaca dan mencatat, dan teknik pengumpulan data pustaka (Syaharman, 2020). Menurut referensi yang diterima, penulis memutuskan: Apa peran penting sistem informasi akuntansi dalam bisnis dan faktor apa yang dapat mempengaruhi kekuatan enkripsi?

III. RESULTS AND DISCUSSION

Keamanan System Informasi

Keamanan informasi ialah upaya untuk mencegah situasi yang tidak diharapkan, misalnya kehilangan integritas atau kerahasiaan data. Sistem keamanan dirancang untuk melindungi sistem komputer dari penipuan dan penyalahgunaan lainnya, (Wulandari, 2023). Hal yang sama juga dikatakan oleh (Zahrani Fatni Hapsah, 2023). “Perangkat keras termasuk basis data, protokol, dan laporan komputer. Salah satu bagian dari organisasi yang menangani ancaman khusus terhadap sistem informasi terkomputerisasi adalah sistem keamanan computer”. Sistem keamanan informasi terdiri dari keamanan fisik dan non-fisik. Kesimpulan dari beberapa pendapat diatas ialah, upaya untuk mencegah kejadian atau risiko yang tidak diharapkan berkaitan dengan sistem informasi dan bagian-bagiannya, seperti kerahasiaan, kehilangan, atau integritas data. Keamanan data juga mengacu pada tindakan privasi digital yang mencegah individu yang tidak diinginkan mengakses komputer, database, atau situs web. Menurut G. J. Simons (2018) mendefinisikan keamanan sistem informasi sebagai upaya untuk mencegah penipuan pada sistem non-fisik. Namun, serangan siber lainnya juga harus dicegah.

Singkatnya, keamanan sistem informasi adalah prosedur yang digunakan untuk mencegah data dicuri, akses yang tidak sah, dan kerusakan sistem informasi perusahaan. Hardware, software, jaringan komunikasi, dan data dalam komputer adalah semua sistem keamanan yang digunakan untuk menjaga jaringan informasi aman. Prinsip utama keamanan sistem informasi adalah prinsip "lebih baik mencegah daripada mengobati". Sayangnya, banyak dari kita masih mengabaikan pentingnya hal ini. Mempertahankan keamanan sistem informasi membutuhkan investasi yang tidak sedikit. Namun, hal ini dapat mencegah kerugian bisnis karena kerusakan jaringan komputer atau kehilangan data penting.

Sistem Informasi Akuntansi

Terdapat tiga kata dalam sistem informasi akuntansi: akuntansi, informasi, dan sistem. Setiap kata memiliki arti yang berbeda, dan jika kata-kata ini digabungkan, akan muncul arti baru. George H. Bodnar (2011:43) mendefinisikan "Informasi sebagai data yang bermanfaat yang diolah untuk digunakan sebagai dasar pengambilan keputusan". Wijayanto (2012:225) “Informasi adalah dasar pengendalian. Salah satu ciri sistem kontrol yang baik adalah kemampuan untuk memberikan informasi yang tepat kepada orang yang tepat pada waktu yang tepat. Data yang berasal dari fakta yang tercatat dan kemudian diproses menjadi bentuk yang bermanfaat atau berguna bagi pengguna adalah jenis informasi lainnya.

SIA terdiri dari lima bagian, menurut Marshall B Romney dan Paul John Steinbart (2015:3):

1. Individu yang bertanggung jawab atas sistem dan bertanggung jawab atas berbagai fungsinya
2. Prosedur yang digunakan untuk mengumpulkan, memproses, dan menyimpan data yang berkaitan dengan operasi perusahaan
3. Data yang berkaitan dengan operasi perusahaan
4. Program yang digunakan untuk memproses informasi perusahaan
5. Infrastruktur teknologi informasi terdiri dari komputer, periferal, dan peralatan komunikasi jaringan.

Vol. 10, No 01 Jan-Juni 2025 Hal. 48 - 54
http://journal.uta45jakarta.ac.id/index.php/JAM/index

Menurut Turner, Weickgenannt, & Copeland (2017:4), Sistem informasi akuntansi mencakup metode, prosedur, dan sistem yang mengumpulkan data akuntansi dari operasi bisnis, mencatatnya dalam catatan, memprosesnya dengan mengklasifikasikan, merangkum, dan mengkonsolidasikan data, dan melaporkannya secara ringkas kepada pengguna internal dan eksternal. Patel (2015) menyatakan bahwa sistem informasi akuntansi adalah bagian dari sistem informasi organisasi. Bertanggung jawab untuk mengumpulkan informasi dari subsistem entitas yang berbeda dan kemudian mengirimkannya ke subsistem pemrosesan informasi organisasi. Sistem informasi akuntansi biasanya berfokus pada pengumpulan, pemrosesan, analisis, dan komunikasi data keuangan kepada pihak eksternal, seperti bankir, investor, kreditor, dan agen pajak, serta pihak internal, seperti manajemen dan pemilik.

Tujuan Sistem Informasi Akuntansi

Tujuan sistem informasi akuntansi, menurut Susanto (2008:8-9), adalah:

1. Untuk tetap beroperasi, suatu organisasi atau perusahaan harus melakukan transaksi seperti pembelian, penyimpanan, produksi, dan penjualan.
2. Memfasilitasi proses pengambilan keputusan dengan menyediakan informasi yang diperlukan selama proses pengambilan keputusan. Tujuan evaluasi sistem informasi akuntansi adalah sama pentingnya dengan mendukung proses pengambilan keputusan. Keputusan harus dibuat mengenai perncanaan dan pengendalian operasi bisnis.
3. Setiap perusahaan harus memenuhi tanggung jawab hukum untuk membantu manajemen bisnis dalam memenuhi kewajibannya kepada pihak eksternal. Memberikan informasi kepada pihak-pihak yang berada di luar perusahaan, seperti pemasok, pelanggan, pemegang saham, kreditor, investor, serikat kerja, analis keuangan, lembaga keuangan, dan bahkan masyarakat umum, adalah salah satu tugasnya yang paling penting.

Enkripsi

Menurut Wicaksono dan Setiawan (2020), enkripsi adalah salah satu metode kriptografi yang tersedia dan digunakan untuk mengubah data asli (*plain text*), yaitu teks biasa, menjadi data yang hanya dapat dibaca oleh pemilik kunci (*encrypted text*). Mengubah data yang mudah dipahami menjadi kode yang sulit dipahami dikenal sebagai enkripsi. Tujuan utama enkripsi adalah untuk menjaga keamanan data untuk memerangi kejahatan *cyber* atau dunia maya seperti phishing, peretasan email, pencurian data, carding, dan sebagainya. Dengan kata lain, data sensitif diacak agar tidak sama dengan yang asli. Ini adalah alasan mengapa platform digital saat ini, seperti situs web dan media sosial, menggunakan enkripsi. Enkripsi menyandikan informasi atau pesan menjadi teks yang tidak dapat dibaca (Ferguson et al., 2010). Kriptografi, sebuah teknik untuk menjaga pesan agar pihak ketiga tidak dapat membacanya, terkait dengan enkripsi. *Block Cipher* dan *Stream Cipher* adalah dua metode enkripsi yang berbeda (Ferguson dkk, 2010). *Block Cipher* menggunakan transformasi yang tidak bervariasi untuk mengenkripsi blok bit dengan panjang tetap. *Block Cipher* memproses blok berukuran tetap secara bersamaan, yang membuatnya lebih aman daripada *stream cipher*. Sedangkan *Stream Cipher* dapat mengenkripsi dan dekripsi data lebih cepat daripada *block cipher*. Ini dapat mengenkripsi kumpulan data seperti bit, byte, nible, atau per 5 bit, menggunakan transformasi yang berbeda untuk setiap bit.

Data dapat dilindungi atau dirahasiakan dengan enkripsi. Seseorang harus memiliki akun atau hak akses terhadap data yang dimaksud karena data yang telah terenkripsi masih dapat didekripsi dan diubah kembali menjadi teks seperti sebelumnya. Salah satu cara untuk melindungi privasi dan kerahasiaan adalah dengan menggunakan kontrol pencegahan yang dikenal sebagai enkripsi. Saat data bergerak melalui internet dan mencegah penyusup mendapatkan akses tidak sah ke datanya. Teks biasa, yang disebut *plaintext*, diubah menjadi teks *ciphertext* yang tidak dapat dibaca melalui proses enkripsi. Faktor-faktor berikut memengaruhi kekuatan enkripsi:

1. Panjang kunci enkripsi
   Panjang kunci adalah jumlah bit dalam kunci enkripsi. Semakin panjang kunci, semakin banyak kombinasi yang mungkin digunakan untuk memecahkan kunci dengan *brute force.* Karena kunci yang lebih panjang memberikan enkripsi yang lebih kuat dengan mengurangi jumlah balok berulang pada *chipertext*, menunjukkan pola pola *chipertext* yang menyerupai pola *plaintext* asli menjadi lebih sulit. Setiap huruf dalam bahasa Inggris diwakili oleh 8 bit, ini memudahkan penggunaan informasi yang berkaitan dengan frekuensi kata yang relative. Untuk sebagian besar kunci enkripsi, biasanya mencapai 1.024 bit atau lebih panjang, dan setidaknya mencapai 256 bit, setara dengan 42 huruf bahasa Inggris.
2. Alogaritme enkripsi
   Algoritma modern yang digunakan untuk mengubah *plaintext* menjadi *ciphertext* dimaksudkan untuk meningkatkan efisiensi dan keamanan. Sangat penting untuk mempertimbangkan jenis algoritma yang digunakan untuk menghubungkan kunci ke *plaintext*; algoritma ini sangat kompleks dan kuat dan hampir

Vol. 10, No 01 Jan-Juni 2025 Hal. 48 - 54
http://journal.uta45jakarta.ac.id/index.php/JAM/index

tidak mungkin diretas dengan kekuatan *brute force*. Kekuatan tidak bergantung pada kerahasiaan operasi; algoritma ini telah diuji secara ketat dan memiliki kemampuan untuk melawan serangan *brute force*.

3. Keamanan Kunci
   Kerahasiaan kunci enkripsi sangat penting karena enkripsi menjadi tidak berguna jika pihak yang tidak berwenang mengetahuinya. Aspek Keamanan Kunci; Penyimpanan kunci secara aman, protokol berbagi kunci yang aman (terutama untuk enkripsi simetris), rotasi kunci secara periodik untuk mengurangi risiko. Untuk mendekripsi data, kunci yang bocor atau tidak diamankan dengan baik dapat dengan mudah digunakan.
4. Kebijakan yang berkaitan dengan penggalian kunci kriptografi
   Salah satu bagian yang paling rentan dari sistem enkripsi biasanya adalah manajemen kunci kriptografi. Selain itu, jika ada alasan untuk percaya bahwa kunci telah disusupi, kunci harus dikembalikan dengan cepat. Selain itu, penting untuk memberi tahu orang lain yang mungkin mengira kunci tersebut salah.
5. Faktor Teknologi
   Kekuatan enkripsi dipengaruhi oleh kemajuan teknologi, terutama dalam hal daya komputasi. Misalnya, komputer dengan daya pemrosesan tinggi, mempercepat serangan *brute force* dapat mempengaruhi algoritma, dan seiring perkembangan teknologi, panjang kunci harus ditingkatkan untuk menjaga keamanan. Faktor teknologi sangat memengaruhi kekuatan dan efektivitas enkripsi. Perkembangan perangkat keras, perangkat lunak, dan metode kriptografi memerlukan peningkatan terus-menerus untuk menjaga relevansi dan keamanan enkripsi.

Jenis Sistem Enkripsi

1. Sistem enkripsi simetris, juga dikenal sebagai *symmetric encryption system*, menggunakan kunci yang sama untuk proses enkripsi dan dekripsi. Standar enkripsi data (DES) dan Standar enkripsi maju (AES) adalah beberapa contoh sistem enkripsi simetris.
2. Sistem enkripsi asimetris menggunakan dua kunci. Kunci publik (*public key*) adalah kunci yang umum dan dapat diakses oleh semua orang, sedangkan kunci privat (*private key*) adalah kunci yang rahasia dan hanya diketahui oleh pemiliknya. Meskipun kedua kunci publik dan privat dapat digunakan untuk mengenkripsi, hanya satu kunci yang dapat mendiskripsi teks yang dichiper. Sistem enkripsi asimetris termasuk RSA dan ECC.

Tabel 1
Perbandingan Sistem Enkripsi Simetris Dan Asimetris

Aspek	Simetris	Asimetris
Jumlah Key	Satu Kunci Kunci rahasia yang digunakan untuk deskripsi dan mengenkripsi adalah sama.	Dua kunci Satu publik, yang lainnya pribadi. Hanya satu yang dapat mendekripsi, tetapi keduanya dapat mengenkripsi.
Kelebihan	Kecepatan yang jauh lebih tinggi	• Semua orang dapat berbicara dengan pemilik dengan kunci publik. • Setiap orang yang ingin berbicara dengan pemilik tidak perlu menyimpan kunci. • Dapat membuat tanda tangan digital yang sah.
Kekurangan	• Semua orang yang ingin berkomunikasi membutuhkan kunci yang berbeda. • Metode yang aman untuk berbagi kunci rahasia dengan orang lain harus ditemukan. • Keamanan seluruh sistem terancam jika kunci bocor.	• Kecepatan yang jauh lebih rendah • Memerlukan kunci elektronik publik untuk menvalidasi kepemilikan kunci publik • Hanya pengguna tertentu yang terancam jika kunci privat bocor.

Vol. 10, No 01 Jan-Juni 2025 Hal. 48 - 54
http://journal.uta45jakarta.ac.id/index.php/JAM/index

Resiko	Melindungi kunci rahasia bersama agar tidak hilang atau dicuri	Menghindari kehilangan atau pencurian kunci privat
Kegunaan Utama	Enkripsi untuk data yang sangat besar	• Tanda tangan digital • Pertukaran kunci sinetris keamanan melalui email
Efesiensi	Lebih efisien dalam hal penggunaan sumber daya komputasi.	Kurang efisien, membutuhkan lebih banyak sumber daya.
Contoh Algoritma	AES, DES, Triple DES, Blowfish.	RSA, ECC, Diffie-Hellman.
Contoh Penggunaan	Enkripsi file, disk, dan data yang disimpan.	SSL/TLS untuk komunikasi web, autentikasi digital.

Kecurian atau kehilangan kunci enkripsi merupakan ancaman besar bagi kedua jenis sistem enkripsi. Data yang dienkripsi tidak dapat dipulihkan jika kunci ini hilang atau dicuri. Jika kunci yang dienkripsi hilang atau dicuri, Data yang dienkripsi tidak dapat dipulihkan. Salah satu cara untuk menghindari risiko ini adalah menggunakan perangkat lunak enkripsi, yang membuat kunci utama built-in yang dapat digunakan untuk mendiskripsi apa pun yang dienkripsi oleh perangkat lunak tersebut. Alternatifnya ialah kunci escrow, yang menyiapkan salinan aman dari semua kunci enkripsi yang digunakan oleh staf.

Sementara enkripsi simetris jauh lebih cepat daripada enkripsi asimetris, meskipun kunci publik dianggap umum, kunci privat harus disimpan dengan aman. Jika kunci rahasia sistem simetris dicuri, pencuri dapat mengakses semua data yang dienkripsi. Karena setiap orang yang memiliki kemampuan untuk memotong e-mail akan mengetahuinya, e-mail bukanlah solusi. Oleh karena itu, beberapa pendekatan untuk mengintegrasikan strategi kunci dengan pendekatan lain diperlukan.

Contoh pengaplikasian enkripsi

1. Pengaplikasian SSL/TLS

   SSL/TLS mengenkripsi data yang dikirimkan oleh browser pengguna ke server web untuk melindungi informasi pribadi seperti nomor kartu kredit, kredensial login, atau informasi pribadi. SSL/TLS adalah contoh enkripsi yang digunakan pada website. Website yang menggunakan enkripsi SSL/TLS dapat diidentifikasi dengan logo gembok atau awalan https. Dengan demikian, memasang SSL/TLS adalah langkah pertama untuk meningkatkan keamanan website.
2. Pengaplikasian SSH

   SSH adalah singkatan dari *secure shell connection*, dan digunakan untuk mendapatkan akses aman ke perangkat jarak jauh. Biasanya digunakan untuk mengakses, mengontrol, dan mengelola server secara remote melalui internet, SSH menggunakan enkripsi untuk memastikan bahwa data antara client dan server tetap aman dan konsisten.
3. Pengaplikasian E2EE

   E2EE menjamin bahwa data hanya dapat dibaca oleh penerima dan pengirim dan tidak oleh pihak ketiga, termasuk penyedia layanan. Sering digunakan dalam aplikasi chat. Untuk memastikan bahwa pesan tidak bocor, pesan harus dienkripsi. Namun, karena enkripsi E2EE adalah enkripsi pengguna ke pengguna, pihak penyedia layanan masih dapat melihat data pengguna.

Kekurangan utama sistem enkripsi asimetris adalah kecepatan; itu jauh lebih lambat daripada enkripsi simetris, sehingga tidak masuk akal untuk digunakan dalam pertukaran data yang lebih besar melalui internet. Akibatnya, perusahaan *e-commerce* menggunakan kedua jenis sistem enkripsi. Sementara enkripsi asimetris mengirimkan kunci simetris secara aman ke penerima melalui email untuk digunakan mendeskripsi *ciphertext*, prediksi simetri digunakan untuk menyanding atau *encode* sebagian besar data yang dipertukarkan. Bahkan kunci rahasia yang dikirim melalui email tetap aman. Jika pengiriman dienkripsi dengan kunci publik penerima, hanya penerima yang dikehendaki memiliki kunci privat yang terkait dan dapat menjelaskan kunci simetris yang dibagikan. Setiap bisnis pasti memiliki data sensitif atau rahasia, jadi bisnis harus mengambil tindakan untuk melindungi data mereka. Ada beberapa cara untuk melakukan pembangunan keamanan data bisnis, seperti:

1. Menciptakan aturan untuk menangani berbagai jenis data

   Bisnis sulit melindungi informasi sensitif karena mereka tidak dapat membedakan data rahasia dari non-rahasia. Akibatnya, diperlukan kebijakan data yang menjelaskan berbagai jenis data dan menetapkan prosedur ketat untuk mengidentifikasi, menangani, dan melindungi berbagai jenis data.
2. Mentransfer data dengan enkripsi

   Banyak bisnis telah menyadari betapa pentingnya menerapkan langkah-langkah keamanan informasi untuk mencegah orang yang tidak berwenang mengakses data yang ada di sistem informasi dan jaringan

Vol. 10, No 01 Jan-Juni 2025 Hal. 48 - 54
http://journal.uta45jakarta.ac.id/index.php/JAM/index

perusahaan. Karena semua orang dan aplikasi selalu mengakses dan berinteraksi dengan data sensitif, bisnis harus mengenkripsi data penting untuk melindunginya.

3. Memilih software bisnis yang aman
   Mencari tahu perangkat lunak mana yang disarankan oleh pakar keamanan informasi untuk digunakan sesuai dengan standar keamanan. Hacker dapat mendapatkan data sensitif jika perangkat lunak perusahaan tidak mengikuti metode keamanan yang andal.
4. Memperbaiki keamanan password
   Melalui pelatihan dan pengenalan berbagai aplikasi manajemen kata sandi, keamanan sangat ditingkatkan. Menggunakan kata sandi atau kata sandi yang lemah adalah masalah yang sangat umum. Beberapa kesalahan keamanan dasar bertanggung jawab atas sebagian besar pencurian data sensitif.
5. Implementasi sistem untuk mengelola keamanan data
   Secara singkat ISO/IEC 27001 (ISMS), Sistem manajemen keamanan informasi adalah teknik yang dirancang khusus untuk menjaga keamanan data yang diakui secara internasional. Berdasarkan praktik terbaik keamanan informasi, dokumen sistem manajemen keamanan informasi (ISMS) memberikan arahan tentang apa yang harus dilakukan perusahaan atau organisasi untuk menilai, menerapkan, dan memelihara keamanan informasi.

Metode ini dapat membantu melindungi aset informasi dari pihak yang tidak berwenang yang dapat digunakan untuk kepentingan perusahaan. Karena sumber daya ini sangat berharga bagi individu, otoritas, dan sektor swasta, penting bagi individu untuk menjaga sumber daya tersebut agar tidak disalahgunakan oleh individu yang tidak bertanggung jawab. Menggunakan teknologi informasi yang sangat besar, khususnya untuk bisnis. Melaporkan, mengelola, dan menyediakan informasi keuangan menjadi mudah, cepat, dan akurat dengan bantuan teknologi informasi. Peran sistem informasi akuntansi (SIA) dalam bisnis adalah sesuatu yang harus diketahui setiap orang yang belajar akuntansi. Ada banyak keuntungan untuk menggunakan teknologi informasi, terutama bagi bisnis. Semua bagian SIA harus terintegrasi dengan baik agar hasilnya akurat, up-to-date, dan bermanfaat bagi pengguna. Data yang dimasukkan oleh individu diolah untuk menghasilkan data akuntansi sesuai dengan prosedur yang berlaku. Beberapa hal yang perlu diketahui tentang keuntungan menggunakan sistem informasi akuntansi untuk bisnis:

1. Memberikan informasi yang akurat dan mudah dipahami yang berdampak pada kemajuan bisnis
2. Meningkatkan efisiensi operasi perusahaan, yang pada akhirnya meningkatkan pendapatan.
3. Memungkinan bahwa kemampuan perusahaan untuk membuat keputusan rasional akan meningkat.
4. Meningkatkan komunikasi informasi bisnis.
5. Sistem informasi akuntansi dapat meningkatkan produktivitas departemen keuangan perusahaan.
6. Untuk menurunkan biaya produksi dan jasa selama proses produksi produk perusahaan dan meningkatkan kualitas produk tersebut.

Dengan demikian, sistem informasi akuntansi memainkan peran penting dalam kemajuan bisnis. SIA memainkan peran penting bagi bisnis. Dalam perusahaan, SIA memiliki tiga fungsi utama. seperti meningkatkan pengambilan keputusan, mengurangi biaya, dan meningkatkan kualitas produk dan jasa. Pengelolaan aset perusahaan, pengumpulan, penyimpanan, dan pemrosesan data menjadi data yang dapat digunakan kembali adalah contoh lain dari hal ini. Dengan SIA yang baik, organisasi dapat melakukan proses operasional dan informasi dengan lebih efisien dan efektif. Kontrol mengatur proses tersebut sehingga hasil yang dicapai dapat disesuaikan dengan tujuan organisasi. Investor, pemasok, dan pelanggan yang tidak terkait langsung dengan perusahaan juga dapat menggunakan data akuntansi SIA untuk membuat keputusan keuangan perusahaan. Jika SIA suatu perusahaan tidak berjalan dengan baik, misalnya karena beberapa komponennya tidak bekerja dengan baik, pasti akan mempersulit sistem, menyebabkan bisnis tidak berjalan dengan sempurna, informasi yang dihasilkan tidak benar, dan tujuan perusahaan sulit dicapai. Oleh karena itu, SIA harus dirancang dan diimplementasikan dengan sangat baik agar operasi perusahaan berjalan dengan baik dan tujuan perusahaan dapat dicapai. Selain itu, menjalankan bisnis juga memerlukan administrasi keuangan yang baik. Hasil yang lebih baik akan dicapai dengan SIA dan administrasi keuangan yang baik.

IV. CONCLUSION

Enkripsi digunakan untuk mengonversi data menjadi informasi atau *ciphertext* yang tidak dapat dipahami, melindungi data saat bergerak melalui internet. Tingkat keamanan data dalam database dipengaruhi oleh sensitivitas data; data yang tidak terlalu sensitif tidak memerlukan peraturan keamanan yang ketat. Perusahaan dapat melakukan semua tugasnya dengan lebih baik dan lebih efisien dengan bantuan SIA, seperti meningkatkan pengambilan keputusan, menurunkan biaya produksi barang dan jasa, dan menghasilkan keuntungan kompetitif. Bisnis juga membutuhkan manajemen keuangan yang baik; SIA pasti akan meningkatkan hasil.

Vol. 10, No 01 Jan-Juni 2025 Hal. 48 - 54
http://journal.uta45jakarta.ac.id/index.php/JAM/index

REFERENCES

Bodnar, George H, William S. Hopwood. 2011. *Accounting Informasi System*, United State America. Pearson Education Inc. Publishing as Prentice Hall.

Elim, L. P. K. J. M. I. (2014). *Peranan Sistem Informasi Akuntansi Dalam Efektifitas Pelaporan Informasi Akuntansi Pertanggungjawaban Pada PT. Pos Indonesia (Persero) Manado*. *2*(2), 1528–1538.

Ferguson, S. (2010) 'Dosen Fakultas Pertanian UKI Toraja Mahasiswa Fakultas Pertanian UKI Toraja 1', I(4), pp. 44–52.

Marshall B. Romney dan Paul John Steinbart. 2015. *Sistem Informasi Akuntansi*. Edisi 13, ahlibahasa: Kikin Sakinah Nur Safira dan Novita Puspasari, Salemba Empat, Jakarta.

Patel, F. (2015). Effects of accounting information system on Organizational Profitability. International Journal of Research and Analytical Reviews, 2(1), 168-174.

Simons, S.O., Mulder, A., van Ingen, J., Boeree, M.J., dan van Soolingen, D. 2013. Role of rpsA gene sequencing in diagnosis of pyrazinamide resistance. Journal of clinical microbiology 51(1), 382. http://www.ncbi.nlm.nih.gov/pubmed/23269981.

Susanto, Azhar. 2008. *Sistem Informasi Akuntansi*. Lingga Jaya, Bandung.

Syaharman. (2020). *Peranan sistem informasi akuntansi dalam mengambil keputusan manajemen pada pt walet solusindo*. *3*(2), 186–189.

Turner, L., Weickgenannt, A., Copeland, M.K., 2017. Accounting Information Systems Controls and Processes. Third Edition. John Wiley & Sons, Inc.

Wicaksana, B. and Setiawan, M., 2020. Penerapan Algoritma Advanced Encryption Standard (AES) Untuk Pengamanan Berkas Soal Ujian. Teknois : Jurnal Ilmiah Teknologi Informasi dan Sains, 10(1), pp.25–34.

Wijayanto. 2012. *Pengantar Manajemen*. Jakarta : PT Gramedia Pustaka Utama.

Wulandari, I. W. (2023). *Peran sistem informasi akuntansi dalam pengaplikasian enkripsi terhadap peningkatan keamanan perusahaan*. *1*(1), 12.

Zahrani Fatni Hapsah, M. I. P. N. (2023). *Analisis Tingkat Keamanan data Perusahaan yang Rentan*. *1*(2), 338