Jurnal Ilmiah dan Manajemen Sistem Informasi, Vol. 9, No. 2, Agustus 2023, Hal. 89-96
e-ISSN 2502-8995 p-ISSN 2460-8181

MANFAAT MANAJEMEN KEAMANAN INFORMASI TERHADAP PENGAMANAN DATA PRIBADI MAHASISWA PRODI AKUNTANSI UNIVERSITAS TRUNOJOYO MADURA

[1]Ghifari Robby Maulana, [2]Saskya Widya Aqila, [3]Nur Hijriyah Sakinah,

[4]Nanda Ika Wulandari, [5] Citra Nurhayati

Akuntansi, Fakultas Ekonomi dan Bisnis, Universitas Trunojoyo Madura

Email: [1]ghifarirobbymaulana@gmail.com,[2]saskyawidyaaqila@gmail.com, [3]nurhijraniyahsakinah@gmail.com, [4]ika7641@gmail.com, [5]citra@trunojoyo.ac.id

ABSTRAK

Informasi adalah salah satu contoh aset bagi suatu individu yang wajib untuk diamankan. Individu juga harus dapat memperhatikan mengenai keamanan informasi data pribadinya agar tidak bocor kepada orang yang tidak bertanggung jawab dan dapat disalahgunakan. Keamanan informasi juga bentuk upaya untuk mengamankan data komputer dan data non komputer dari penyelewengan. Maka dari itu, diperlukanya manajemen keamanan informasi yang dimulai dari kesadaran para pengguna terkait data pribadinya, manajemen resiko, serta etika terhadap segala bentuk data pribadi para pengguna yang meliputi foto, video, audio, dan sandi. Tujuan dari keamanan informasi adalah untuk memastikan kerahasiaan semua aset informasi data pribadi dan juga perangakat keras dan lunak. Tujuan utama dari jurnal ini adalah untuk meningkatkan mengenai literasi manajemen keamanan data pribadi khususnya mahasiswa akuntansi agar terhindar dari kebocoran data dan seluruh kejahatan siber yang ada. Metode penelitian yang digunakan dalam jurnal ini adalah kualitatif dengan sumber data wawancara kepada mahasiswa akuntansi secara acak. Setelah data diperoleh, observasi dilakukan guna untuk mengambil kesimpulan bagaimana cara mengamankan data pribadi mahasiswa akuntansi itu sendiri. Kesimpulan penelitian ini yakni ada 7 langkah dan langkah tambahan untuk mengamankan data pribadi mahasiswa, diantaranya: meningkatkan kesadaran akan keaman data pribadi, menerapkan kontrol data pribadi, mengevaluasi keamanan, melakukan tambahan keamanan, dan yang terakhir meningkatkan pemahaman dan perilaku terhadap data pribadi mahasiswa.

Kata kunci: *informasi, kemanan informasi, manajemen keamanan informasi, data pribadi*

Abstract

Information is one example of an asset for an individual to secure. That individual should be able to take attention to the security of personal data information so that it does not leak to irresponsible people and can be abused. Information security is also an effort to secure computer data, and non-computer data from fraud. So therefore, information security management is needed to start from user awareness regarding personal data, risk management, and ethics for all forms of users' data including photos, videos, audio, and passwords. Information security aims to ensure the confidentiality of all personal data information assets as well as hardware and software. The main purpose of this journal is to increase literacy regarding personal data security management, especially for students to avoid data leaks and all existing cyber crimes. The research method that we use in this journal is qualitative with data sources we interview accounting students randomly and after we obtain the data we observe it to draw conclusions about how to secure the personal data of accounting students themselves. We conclude that there are 7 additional steps and steps to secure student personal data including increasing awareness of personal data security, implementing personal data controls, evaluating security, carrying out additional security, and finally increasing understanding and behavior towards student personal data.

Keywords: *information, information security, information security management, personal data*

A. PENDAHULUAN

Universitas Trunojoyo Madura adalah sebuah universitas yang terletak di pulau Madura tepatnya dibangun dilahan seluas 30 hektar, yang terletak di Jalan Raya Telang, Kecamatan Kamal, Kabupaten Bangkalan, Jawa Timur. Universitas ini memiliki beberapa fakultas salah satunya adalah Fakultas Ekonomi dan Bisnis terdapat beberapa jurusan S1 yaitu Manajemen, Akuntansi, dan Ekonomi Pembangunan.

Dari informasi data yang ada diatas, pada saat ini di era digitalisasi informasi seperti itu sangatlah mudah diperoleh dan disebarluaskan, Oleh karena itu informasi menjadi aset yang sangat berharga untuk semua orang. Aset informasi ini sangatlah rentan mengalami serangan dunia maya karena banyaknya data sensitif yang mereka simpan termasuk informasi pribadi Mahasiswa. Pada Mahasiswa Akuntansi saat ini terdapat banyak aset data-data yang disimpan oleh Mahasiswa, Agar aset informasi mereka tetap aman maka harus ada sistem keamanan pada data pribadinya. Maka dari itu, Penelitian ini bertujuan untuk mengetahui manfaat manajemen keamanan informasi untuk melindungi data pribadi Mahasiswa Akuntansi di Fakultas Ekonomi dan Bisnis Universitas Trunojoyo Madura.

B. LANDASAN TEORI

B.1. Pengertian Resiko dan Manajemen Resiko

Definisi resiko pada sistem keamanan informasi manajemen (SKIM) adalah kemungkinan terjadinya kerugian atau ketidakpastian yang ada dalam pengamanan dan perlindungan data, informasi, dan sistem yang digunakan oleh suatu organisasi maupun individu [8]. Resiko pada SKIM sendiri dapat meliputi seperti serangan siber, kebocoran data, kerentanan keamanan, pelanggaran privasi, dan kerusakan perangkat keras atau lunak, antara lain.

Manajemen resiko pada SKIM adalah proses bagaimana cara pengidentifikasian, penilaian, dan pengelolaan resiko yang ada dengan keamanan sistem informasi. Tujuannya adalah untuk memastikan keamanan dan integritas data dan sistem yang digunakan oleh organisasi dan meminimalkan dampak resiko negatif pada operasi bisnis. Manajemen resiko pada SKIM melibatkan beberapa tahapan, yaitu tahapan pertama adalah identifikasi resiko dalam tahap ini mengidentifikasi semua potensi resiko pada sistem keamanan informasi yang digunakan oleh organisasi, tahap kedua ada penilaian resiko atau *assessment risk* tahap ini dilakukan untuk menilai tingkat resiko dan dampak yang mungkin terjadi pada setiap resiko yang teridentifikasi, tahapan ketiga ada pengembangan strategi pengelolaan resiko yang efektif dan efisien untuk meminimalkan dampak resiko negatif pada operasi bisnis, tahapan keempat yaitu tahapan implementasi pengelolaan resiko yang telah disusun dan memonitor hasilnya. Tahapan terakhir yaitu tahapan evaluasi serta pembaruan secara teratur dan memperbarui sesuai kebutuhan.

Manajemen resiko pada SKIM dapat melibatkan teknologi dan kebijakan keamanan, pemantauan dan pengendalian akses pengguna, dan perencanaan keamanan data dan pemulihan bencana. Penting untuk menjaga manajemen resiko pada SKIM menjadi bagian integral dari strategi bisnis dan pengambilan keputusan dan diimplementasikan secara berkelanjutan.

B.2. Keamanan Informasi

Menurut [2], keamanan informasi adalah praktik menjaga data sensitif tetap aman dari gangguan. Secara tidak langsung, keamanan informasi ini menjamin kelangsungan bisnis, memitigasi risiko, dan memaksimalkan ROI. Sistem Informasi Manajemen-Keamanan Informasi, yang menyatakan bahwa keamanan informasi diperlukan untuk menjamin operasi yang sedang berlangsung, mengurangi kemungkinan kerugian, dan memperluas cakupan kemungkinan keuntungan finansial [8].

B.3. Risiko Keamanan Informasi

Potensi konsekuensi yang tidak diinginkan sebagai akibat dari pelanggaran keamanan informasi dikenal sebagai risiko keamanan informasi. Semua bahaya ini adalah hasil dari perilaku ilegal. Potensi bahaya meliputi *Interruption* merupakan ancaman terkait ketersediaan, yaitu mengenai data dan informasi yang ada didalam sistem komputer dirusak dan dibuang sehingga tidak ada lagi atau menjadi tidak berguna. Risiko kedua ada *Interception* terdapat risiko terhadap kerahasiaan, seperti individu yang tidak berwenang mendapatkan akses ke informasi melalui sistem komputer [4]. Resiko selanjutnya ada *Modification* merupakan bahaya bagi integritas sistem yang ditimbulkan oleh pengguna yang tidak sah yang tidak dapat mengakses atau mengedit data dan

informasi. Resiko terakhir *Fabrication*: adanya orang-orang yang tidak memiliki wewenang, orang tersebut meniru atau memalsukan suatu objek didalam sistem.

B.4. Aspek-Aspek Sistem Manajemen Keamanan Informasi

Adapun beberapa tiga aspek yang perlu diperhatikan dalam manajemen keamanan sistem informasi. Kerahasiaan merupakan aspek yang menjaga data atau informasi, menjamin hanya pihak berwenang yang dapat melihatnya, dan memastikan bahwa data atau informasi tersebut dikirim, diterima, dan disimpan dengan aman [3] [10].

Kedua, Integritas merupakan sebuah komponen yang menjamin data tidak dapat diubah tanpa otorisasi dari pihak otoritas yang sesuai, serta menggunakan prosedur yang menjaga kebenaran dan integritas data.

Ketiga, Ketersediaan merupakan jaminan data dapat diakses bila diperlukan, memungkinkan pengguna yang berwenang menggunakan data dan peralatan yang terhubung.

C. METODE PENELITIAN

Metode Penelitian memberikan penjelasan tentang langkah-langkah, data, lokasi penelitian, metode evaluasi yang digunakan serta penjelasan terstruktur tentang algoritma atau metode dari penelitian yang dibahas. Berikut ini adalah penjelasan yang terperinci mengenai Gambar 1. Pada Gambar 1 terlihat sebuah alur metode penelitian yang dimulai dari:

C.1. Identifikasi Masalah

Pada tahapan ini, dilakukan pengecekan seberapa banyak masalah yang terjadi terkait keamanan data mahasiswa. Masalah yang terjadi tersebut seperti, kurangnya kesadaran dan pemahaman tentang manfaat manajemen keamanan informasi di kalangan mahasiswa, sistem atau infrastruktur yang digunakan mahasiswa rentan terhadap serangan dan pelanggaran keamanan, banyak mahasiswa yang sering menggunakan aplikasi dan platform online rentan terhadap eksploitasi jika keamanan aplikasi dan platform tersebut tidak memadai. Dengan mengatasi masalah-masalah ini, langkah-langkah dapat diambil untuk memperkuat manajemen keamanan informasi dan melindungi data pribadi mahasiswa dengan lebih baik.

Gambar 1. Alur Metode Penelitian

C.2. Studi Literatur

Studi literatur ini bertujuan untuk mengeksplorasi manfaat dari penerapan manajemen keamanan informasi dalam melindungi data pribadi mahasiswa. Pada saat ini data pribadi mahasiswa banyak mengandung informasi sensitif, seperti informasi pribadi, akademik, dan finansial, sehingga perlindungan data yang tepat sangatlah penting untuk mencegah potensi ancaman keamanan dan pelanggaran privasi [6] [9].

C.3. Pengumpulan Data Wawancara dan Observasi

Pengumpulan data wawancara ini melalui proses jawab pertanyaan oleh kami dan dijawab oleh narasumber berupa pernyataan maupun pengalaman yang pernah dialami oleh narasumber mengenai informasi data pribadi.

C.4. Identifikasi Keamanan Data Pribadi

Setelah diperoleh timbal balik dari para narasumber kami yaitu mahasiswa akuntansi Univessitas Trunojoyo Madura, kami mengidentifikasi kembali apa saja yang termasuk kedalam golongan data pribadi dan bagaimana mahasiswa mengamankannya.

C.5. Analisa Ancaman dan Resiko

Sesudah memperoleh informasi klasifikasi data pribadi mahasiswa dan bagaimana cara mengamankanya. Kami menganalisa ancaman dan resiko yang kemungkinan terjadi kepada data pribadi mahasiswa akuntansi Universitas Trunojoyo Madura.

C.6. Kesimpulan dan Saran

Pada alur terakhir dapat menarik kesimpulan apakah Mahasiswa perlu menerapkan control terhadap data pribadinya masing-masing. Serta, melakukan penyaringan terhadap memberikan data pribadinya.

D. HASIL DAN PEMBAHASAN

Pengumpulan data dan informasi yang berkaitan dengan manajemen risiko sistem informasi berdasarkan perlindungan data pribadi Mahasiswa Akuntansi di Universitas Trunojoyo Madura. Beberapa tugas dilakukan, termasuk pembuatan profil risiko data pribadi, identifikasi kelemahan keamanan dalam informasi data pribadi, dan pengembangan metode perlindungan rencana keamanan.

D.1. Identifikasi Data Pribadi Pada Mahasiswa

Data pribadi merujuk pada informasi yang mengidentifikasi individu secara pribadi. Ini mencakup segala jenis informasi yang dapat digunakan untuk mengidentifikasi, menghubungi, atau mengidentifikasi secara individual seseorang. Data pribadi mencakup berbagai jenis informasi, baik dalam format manual maupun dalam format yang ditemukan di internet.

Tabel 1. Identifikasi Data Pribadi

Data Pribadi Manual		Data Pribadi Internet	
Nama Lengkap	Informasi ini adalah identifikasi pribadi yang umum. Misalnya, “Richie Rayen”	Alamat Email	Alamat email individu, seperti "richierayen@example.com".
Alamat Rumah	Informasi mengenai alamat atau tempat tinggal seseorang, seperti contoh "Jl. Sistem No. 123, Kota Manajemen".	Nama Pengguna Media Sosial	Nama pengguna yang digunakan seseorang di platform media sosial seperti Instagram, TikTok, Facebook, atau Twitter.
Nomor Telepon	Nomor telepon yang digunakan seseorang untuk berkomunikasi, misalnya, "081234567890".	Data Akun Bank Online	Jika seseorang menggunakan layanan perbankan online, informasi seperti nama pengguna dan nomor rekening dapat dianggap sebagai data pribadi.
Nomor Identifikasi	Ini bisa berupa nomor identitas nasional, seperti nomor Kartu Tanda Penduduk (KTP), Kartu Tanda Mahasiswa (NIM), atau nomor paspor, dll.	Riwayat Penelusuran Internet	Jejak pencarian yang ditinggalkan seseorang di mesin pencari seperti Google, Yahoo, Mozila Firefox, dll. termasuk pertanyaan, minat, atau preferensi pribadi.
Tanggal Lahir	Tanggal lengkap lahir seseorang, seperti "29 Februari 2003".	Informasi Lokasi	Informasi tentang lokasi seseorang yang diunggah atau dibagikan secara sukarela melalui media sosial, aplikasi berbasis lokasi, atau layanan peta online, dll.

Berikut adalah penjelasan terperinci mengenai Tabel 1. Dimulai dari data pribadi manual mencakup nama lengkap "Richie Rayen" dan alamat rumahnya di "Jl. Sistem No. 123, Kota Manajemen". Di sisi lain, data pribadi internet mencakup beberapa informasi penting seperti alamat email individu "richierayen@example.com", serta beragam nama pengguna media sosial seperti Instagram, TikTok, Facebook, atau Twitter. Tidak hanya itu, data pribadi internet juga melibatkan nomor telepon yang digunakan, dalam contoh ini adalah "081234567890", serta informasi terkait akun bank online, termasuk nama pengguna dan nomor rekening yang digunakan untuk layanan perbankan online.

Sebagai tambahan, nomor identifikasi juga termasuk dalam data pribadi internet, yang bisa berupa nomor identitas nasional seperti Kartu Tanda Penduduk (KTP), Kartu Tanda Mahasiswa (NIM), atau nomor paspor. Seiring dengan perkembangan

teknologi, riwayat penelusuran internet menjadi bagian penting dari data pribadi internet, mencakup jejak pencarian dan informasi lain yang ditinggalkan seseorang di mesin pencari seperti Google, Yahoo, atau Mozila Firefox. Informasi ini termasuk pertanyaan, minat, atau preferensi pribadi.

Terakhir, data pribadi internet juga mencakup informasi lokasi seseorang yang diunggah atau dibagikan sukarela melalui media sosial, aplikasi berbasis lokasi, atau layanan peta online, serta berbagai platform lainnya. Semua informasi ini perlu dijaga keamanannya untuk melindungi privasi individu dan mencegah penyalahgunaan data.

D.2. Evaluasi Praktik Keamanan Informasi Data Pribadi

Praktik keamanan merupakan tindakan yang dipakai untuk menjelaskan tentang cara mengamankan data pribadi. Setelah kami melakukan wawancara serta observasi kepada Mahasiswa Akuntansi Universitas Trunojoyo Madura yang notabenya sudah mempelajari terkait sistem informasi manajemen. Dan di dalam mata kuliah tersebut para Mahasiswa yang kami wawancarai sudah mengerti mengenai manajemen keamanan data pribadinya.

Menurut Mahasiswa yang kami wawancarai berbependapat bahwa informasi data pribadi yang sering mengalami kebocoran data adalah media sosial. Hal tersebut dilatar belakangi oleh pengguna media sosial di Indonesia sangatlah banyak. Dengan maraknya pengguna media sosial menjadikan rentanya kebocoran data pada platform tersebut. Hal ini dikuatkan oleh data penggunaan internet tahun 2018 dari kelompok perdagangan ISP Indonesia (APJII). Enam puluh empat koma delapan persen, atau sekitar 171 juta orang, di Indonesia memiliki akses ke internet. Dengan kedatangan Revolusi Industri Keempat, ini hanya akan semakin penting. Berbagi informasi pribadi oleh orang Indonesia di media sosial secara langsung berkorelasi dengan tingginya tingkat melek internet di negara ini (APJII. Survey Penetrasi Internet 2018. https://apjii.or.id/survei2018 Diakses pada tanggal 21 Mei 2023).

Sebagai Mahasiswa juga sudah mengetahui mengenai internet yang digunakan oleh Mahasiswa untuk untuk sarana komunikasi, belajar, maupun bermedia sosial. Dan menurut Mahasiswa beralasan mengapa media sosial adalah salah satu informasi data pribadi yang rentan dan sering mengalami kebocoran data dikarenakan di media sosial anda diharuskan untuk memasukan data pribadi anda untuk mendaftar pada suatu platform di media sosial seperti halnya, nomor telepon, nama lengkap, tempat dan tanggal lahir, dan usia penggunanya. Dan tak sadar anda sering mengizinkan kepada platform media untuk mengakses penyimpanan data pada telepon genggam anda. Maka dari itulah manajemen keamanan data pribadi diperlukan untuk meminimalisir kebocoran data pribadi.

Namun data yang kami peroleh masih banyak Mahasiswa yang kami wawancarai belum menerapkan manajemen keamanan data pribadi. Rata-rata Mahasiswa hanya memenuhi salah satu aspek dari manajemen keamanan informasi yaitu kerahasiaan *confidentiality*. Mahasiswa hanya sebatas merahasiakan mengenai data pribadi di media sosial seperti halnya nama pengguna *username* dan *password.*

Dari wawancara yang dilakukan kepada Mahasiswa, diperoleh bahwa rata-rata Mahasiswa belum pernah mengalami kebocoran data pribadi atau kejahatan siber seperti *hacking*, *cracking*, dan kejahatan siber lainya. Ada satu saja Mahasiswa yang diwawancarai pernah mengalami kasus kebocoran data pribadi dalam bentuk SMS *short message service* yang mengatas namakan Mahasiswa tersebut dan digunakan untuk meminta pulsa kepada kerabat dan teman Mahasiswa tersebut. Hal tersebut sangat sering terjadi dikalangan Mahasiswa bahkan Dosen, seringkali mengatasnamakan Dosen maupun Mahasiswa untuk medapatkan pulsa. Masalah ini bisa dikendalikan dengan adanya konfirmasi kepada pihak terkait dan harus mengecek lebih rinci lagi apabila mendapatkan pesan dari nomer yang tidak dikenal dan menjadi pelajaran bagi Mahasiswa agar lebih hati-hati dalam menyebarkan informasi data pribadinya.

Karena itulah Mahasiswa harus lebih selektif dalam pemberian informasi data pribadi kepada pihak yang membutuhkan. Seperti halnya pihak kampus yang membutuhkan data pribadi para Mahasiswanya untuk keperluan administrasi maupun kepada organisasi yang diikuti oleh Mahasiswa. Tidak jarang juga memberikan informasi data pribadi kepada instansi pemerintahan untuk keperluan administrasi penduduk yang notabenya pihak kampus, organisasi maupun pemerintahan mempunyai integritas untuk menyimpan informasi data pribadi tersebut.

D.3. Evaluasi Praktik Keamanan Informasi Data Pribadi

Ancaman keamanan sistem informasi adalah suatu peristiwa yang dapat merusak aset informasi bagi suatu entitas baik perseorangan maupun kelompok. Ancaman terhadap keamanan sistem informasi dapat datang dari dua sumber utama, yaitu ancaman internal dan ancaman eksternal. Ancaman internal muncul di dalam lingkup organisasi, entitas pendidikan, dan rekanan yang berada dalam lingkungan sekitarnya. Sementara itu, ancaman eksternal terjadi di luar lingkup wewenang entitas tersebut dan bisa diatasi oleh pihak yang memiliki kekuasaan yang kuat, seperti kepolisian atau pemerintahan. Ancaman terbagi menjadi dua jenis, yaitu ancaman aktif yang melibatkan usaha langsung untuk merusak atau mengganggu sistem, dan ancaman pasif yang cenderung mencuri atau mengakses informasi tanpa sepengetahuan pemiliknya. Untuk menjaga keamanan data, organisasi dan entitas pendidikan harus tetap waspada terhadap kedua jenis ancaman ini [5].

Ancaman aktif dalam keamanan data mencakup berbagai hal yang berpotensi merusak atau mengganggu integritas informasi. Pertama, ada pencurian data, di mana informasi pribadi dapat diakses secara paksa oleh pihak yang tidak berwenang melalui praktik hacking, cracking dan pembobolan data suatu serangan yang disengaja yang dapat menembus sistem sehingga data pribadi bisa diakses [1]. Selanjutnya, ancaman modifikasi ilegal terjadi ketika informasi data pribadi mengalami perubahan tanpa izin dari pihak berwenang. Selain itu, ada juga ancaman penghancuran data ilegal yang dilakukan oleh penjahat sistem dengan tujuan mencuri informasi sensitif atau menyebabkan kerusakan pada sistem. Penggunaan sistem secara ilegal juga menjadi ancaman aktif, di mana peretas dapat mencuri atau mengakses data sensitif secara tidak sah.

Di sisi lain, ancaman pasif lebih berkaitan dengan ketidakberesan dalam sistem atau kesalahan manusia. Pertama, ada kemungkinan kegagalan sistem yang bisa terjadi akibat kerusakan pada perangkat keras atau perangkat lunak, menyebabkan data tidak konsisten atau bahkan hilang. Selain itu, kesalahan manusia juga dapat mengancam integritas database dan sistem, karena kesalahan dalam fungsi sistem atau pengelolaan data dapat membuka celah bagi ancaman lainnya. Semua ini menunjukkan pentingnya menjaga keamanan data dan menerapkan langkah-langkah perlindungan untuk melindungi informasi pribadi dan menghadapi berbagai jenis ancaman dengan efektif.

D.4. Evaluasi Rekomendasi Kontrol

Berdasarkan hasil analisis identifikasi data pribadi pada Mahasiswa dan evaluasi praktik keamanan informasi data pribadi, melahirkan beberapa rekomendasi kontrol yang dapat digunakan untuk memberikan saran yang tepat, serta kontrol keamanan teknis tersebut sudah dengan prosedur yang telah disarankan, dievaluasi, ditelaah dan diimplementasikan.

Rekomendasi kontrol ini merupakan langkah awal untuk mengontrol keamanan data pribadi. Rekomendasi kontrol ini selain membantu meningkatkan keamanan data pribadi perorangan atau Mahasiswa, tetapi juga dapat membantu setiap individu untuk mempertimbangkan konteks spesifik mereka dan mengadopsi pengendalian atau kontrol tambahan yang sesuai dengan kebutuhan dan situasi mereka serta meminimalkan tingkat resiko yang diperoleh dari berbagai ancaman yang terjadi seperti akses yang tidak sah, penggunaan yang tidak sah, perubahan yang tidak sah, atau kerugian lainnya. Berikut adalah rekomendasi kontrol mengenai jenis, aspek, pengendalian, dan rekomendasi untuk menjaga keamanan data pribadi.

Adapun serangkaian rekomendasi pengendalian untuk menjaga keamanan data pribadi, rekomendasi ini mencakup aspek-aspek penting seperti kesadaran akan privasi pribadi baik dalam lingkungan online maupun offline, pengelolaan kata sandi yang kuat, dan peningkatan pengetahuan tentang keamanan data. Langkah-langkah yang diusulkan meliputi memastikan bahwa individu dan semua yang terlibat dalam pengelolaan data pribadi memahami esensi privasi dan memiliki kemampuan untuk melindungi data tersebut. Selain itu, disarankan untuk mengimplementasikan kebijakan akses yang berbasis peran, mempertimbangkan penggunaan otentikasi ganda, serta memberikan akses hanya kepada personel yang berwenang. Membuat kata sandi yang unik dan kuat untuk setiap akun, serta mengaktifkan autentikasi dua faktor, juga merupakan bagian integral dari langkah-langkah tersebut. Dalam upaya memperdalam pemahaman tentang keamanan data, diakui pentingnya akses ke sumber daya online, tutorial, dan seminar yang relevan serta menjaga

keterkiniannya agar selalu sesuai dengan perkembangan terbaru dalam praktik keamanan data.

Dalam konteks perangkat lunak, langkah-langkah penting untuk menjaga keamanan data Menurut Hidayat et al. Meliputi enkripsi data sebagai upaya melindungi informasi pribadi. Selain itu, perlindungan dari serangan malware dan virus, serta upaya pencegahan terhadap spam, phishing, dan serangan malware melalui email, merupakan aspek yang tidak boleh diabaikan. Mengamankan proses menjelajah di internet juga menjadi perhatian utama.

Untuk mencapai tujuan ini, disarankan untuk mengambil langkah-langkah seperti mengenkripsi data pribadi guna menjaga kerahasiaan informasi, dan menggunakan perangkat lunak keamanan seperti firewall, antivirus, dan antimalware. Penggunaan alat keamanan email yang dapat memblokir ancaman, serta alat keamanan penjelajahan web untuk mengidentifikasi dan memblokir situs web berbahaya atau mencurigakan juga penting.

Pentingnya menggunakan algoritma enkripsi yang kuat dalam penyimpanan data, baik dalam penyimpanan fisik maupun dalam database elektronik, tidak boleh diabaikan. Rutin memperbarui perangkat lunak keamanan guna melindungi sistem dari ancaman terbaru, dan menggunakan Virtual Private Network (VPN) saat terhubung ke internet untuk mengamankan data dari mata-mata dan serangan jaringan, juga merupakan langkah-langkah yang dianjurkan.

Selain itu, kehati-hatian dalam menghadapi email yang mencurigakan sangatlah penting, seperti tidak mengklik tautan atau lampiran yang mencurigakan, serta berhati-hati terhadap email yang meminta informasi pribadi. Penggunaan ekstensi atau add-on keamanan penjelajahan web yang terpercaya serta menghindari kunjungan ke situs yang mencurigakan, juga perlu diperhatikan, begitu pula saat memasukkan informasi pribadi secara online.

Dalam konteks perangkat keras, langkah-langkah penting untuk menjaga keamanan data pribadi pada perangkat seluler meliputi perlindungan data pribadi, aktivasi fitur keamanan perangkat, dan penggunaan aplikasi keamanan yang mampu melindungi data serta menjaga akses fisik dan jaringan. Disarankan untuk mengaktifkan fitur pengaman perangkat, mengunci perangkat saat tidak digunakan, dan tidak meninggalkannya tanpa pengawasan. Selain itu, penting untuk melakukan backup data secara berkala, menyimpannya di tempat aman, dan memastikan kemampuan pemulihan data jika diperlukan.

Dalam upaya menjaga keamanan perangkat keras, disarankan juga untuk menggunakan aplikasi keamanan yang terpercaya, memperbarui perangkat lunak secara berkala, serta mengaktifkan fitur keamanan seperti penguncian layar dan enkripsi data. Aktifkan dan manfaatkan fitur keamanan yang ada pada perangkat Anda, termasuk penggunaan kombinasi kata sandi, PIN, pola, atau sidik jari yang kuat untuk membuka kunci perangkat. Selalu ingat untuk mengunci perangkat saat tidak digunakan, bahkan jika hanya dalam waktu singkat, dan hindari meninggalkan perangkat tanpa pengawasan, terutama di tempat umum atau di sekitar orang yang tidak dikenal.

Dalam hal perlindungan jaringan, langkah-langkah penting termasuk penggunaan firewall dan Intrusion Detection System (IDS) untuk memantau dan mengontrol lalu lintas jaringan serta mendeteksi aktivitas mencurigakan atau serangan. Disarankan juga untuk menggunakan jaringan Wi-Fi yang aman dengan protokol keamanan seperti WPA2 atau WPA3, serta menghindari mengirim atau mengakses data sensitif melalui jaringan Wi-Fi publik yang tidak aman. Penting untuk mengenkripsi koneksi Wi-Fi Anda dengan protokol keamanan yang kuat dan menjaga ketidakamanan saat terhubung ke jaringan Wi-Fi publik. Dengan menerapkan langkah-langkah ini, Anda dapat memitigasi risiko terhadap potensi ancaman dan menjaga keamanan data pribadi Anda.

E. KESIMPULAN

Penelitian ini bertujuan untuk mengidentifikasi dan melindungi data pribadi Mahasiswa/i Akuntansi Angkatan di Fakultas Ekonomi dan Bisnis Universitas Trunojoyo Madura. Hasil dari penelitian ini menyimpulkan beberapa langkah yang dapat diambil untuk meningkatkan keamanan data pribadi para Mahasiswa Akuntansi.

Pertama, Universitas Trunojoyo Madura dan Fakultas Ekonomi dan Bisnis perlu meningkatkan kesadaran dan pendidikan tentang pentingnya keamanan informasi kepada Mahasiswa akuntansi. Para mahasiswa harus memahami betapa pentingnya menjaga kerahasiaan data pribadi mereka.

Kedua, Mahasiswa Akuntansi perlu menerapkan kontrol keamanan teknis tambahan yaitu enkripsi data, penggunaan kata sandi yang kuat, dan pengaturan

privasi yang tepat di media sosial. Langkah-langkah ini dapat membantu melindungi data pribadi mereka dari akses yang tidak sah seperti yang dikutip pada penelitian [7].

Selanjutnya, Universitas dan Fakultas perlu memperbarui dan mengevaluasi kebijakan keamanan informasi secara berkala untuk memastikan keamanan data pribadi Mahasiswa. Hal ini akan membantu memastikan bahwa sistem keamanan selalu diperbarui sesuai dengan perkembangan teknologi dan ancaman baru.

Keempat, Mahasiswa Akuntansi harus secara selektif membagikan data pribadi mereka dan hanya memberikannya kepada pihak yang berwenang dan terpercaya. Dengan berhati-hati dalam membagikan informasi, mereka dapat mengurangi risiko penyalahgunaan data.

Langkah berikutnya adalah melakukan langkah-langkah pengamanan tambahan, seperti menyediakan pelatihan keamanan informasi kepada mahasiswa akuntansi, mengimplementasikan sistem deteksi intrusi, dan melakukan audit keamanan secara rutin. Hal ini akan membantu meningkatkan sistem keamanan secara keseluruhan.

Keenam, Fakultas harus mendorong Mahasiswa akuntansi untuk mempertimbangkan pengendalian tambahan yang sesuai dengan kebutuhan mereka, seperti mengaktifkan otentikasi dua faktor dan menggunakan aplikasi keamanan pihak ketiga. Langkah-langkah ini akan memberikan lapisan keamanan ekstra untuk data pribadi mereka.

Terakhir, kampanye kesadaran keamanan informasi secara teratur perlu dilakukan untuk meningkatkan pemahaman dan perilaku Mahasiswa terkait dengan perlindungan data pribadi mereka. Dengan meningkatkan kesadaran, mahasiswa akan lebih waspada dan bertanggung jawab dalam menjaga data pribadi mereka.

Dengan mengikuti saran-saran tersebut dan menerapkan manajemen keamanan informasi yang tepat, Fakultas Ekonomi dan Bisnis Universitas Trunojoyo Madura dapat lebih melindungi data pribadi Mahasiswa Akuntansi dan mengurangi risiko kebocoran dan penyalahgunaan data yang mungkin terjadi. Upaya ini akan membantu menciptakan lingkungan yang aman dan terpercaya bagi seluruh komunitas akademik.

REFERENSI

[1] E. Pertiwi, D. Delvina Nuraldini, G. Tri Buana, and A. Arthacerses, “Analisis Yuridis Terhadap Penyalahgunaan Data Pribadi Pengguna Media Sosial”, *J.Rechten*, vol. 3, no. 3, pp. 18-24, Dec. 2021.

[2] S. Nurul, Shynta Anggrainy, and Siska Aprelyani, “Faktor-Faktor Yang Mempengaruhi Keamanan Sistem Informasi: Keamanan Informasi, Teknologi Informasi dan Network (Literature Review Sim)”, JEMSI, vol. 3, no. 5, pp. 564-573, May 2022.

[3] Putra, M. S. (2021). Keamanan Informasi dalam Pemanfaatan Teknologi Informasi pada Aplikasi Mobile Adaptif PK - Melissa Santoso 43217120008

[4] Agustina, D., Nazzilla Pramadista, F., & Fara Regyna, T., Sistem Manajemen Keamanan Informasi.

[5] Damayanti, K., Fardinal., 2019, *The Effect of Information Technology Utilization, Management Support, Internal Control, and User Competence on Accounting Information System Quality. Schollars Bulletin, 5(12), 751-758*

[6] M. Mirnayanti, J. Judhariksawan, and M. Maskum, "Analysis of Personal Data Security Settings in Indonesia," Living Law, vol. 15, no. 1, pp. 16-30, 2023.

[7] A. M. Ujung and M. I. P. Nasution, “Pentingnya Sistem Keamanan Database Untuk Melindungi Data Pribadi”, *jiska*, vol. 1, no. 2, pp. 44-47, Jun. 2023.

[8] F. Nasher, 2020, "Perancangan Sistem Manajemen Keamanan Informasi Layanan Pengadaan Barang/Jasa Secara Elektronik (LPSE) Di Dinas Komunikasi Dan Informatika Kabupaten Cianjur Dengan Menggunakan Sni Iso/Iec 27001:2013," Media Jurnal Informatika, vol. 10, 2020, pp. 10.35194/mji.v10i1.465.

[9] M. W. Hidayat, H. Ramli, P. M. Bulan Ikhram, S. Sidrayanti, A. R. Ridhawi, N. A. Mukhtar, and R. Junedy, "Analisa Clustering Phising Untuk Meningkatkan Kesadaran Mahasiswa Terhadap Keamanan Data Pribadi Mahasiswa Universitas Negeri Makassar," Vokatek: Jurnal Pengabdian Masyarakat, vol. 1, no. 1, pp. 28-33, Feb. 2023.

[10] A. Pramestyarani and Y. Putra, "Keamanan Informasi dalam Pemanfaatan Teknologi Informasi pada PT Bank Mandiri," Jurnal Keamanan Informasi, vol. x, no. x, hal. xx, Tanggal Publikasi: 07-Nov-2020.