Jurnal of Business and Audit Information System (JBASE) *Vol. 6 (No. 2): 1-15. Th. 2023*
Versi Online: http://journal.ubm.ac.id/index.php/jbase *p-ISSN: 2615-6431*
DOI: dx.doi.org/10.30813/jbase.v6i1.4670 *e-ISSN: 2620-7907*

Analisis Keamanan Informasi Terhadap Bencana Alam di Lab Komputer SMA XYZ

Analysis of Information Security Against Natural Disasters in XYZ High School Computer Lab

Hendy Tannady[1)], M. Fauzi Isputrawan[2)], Eirene[3)], Kenji Tjandra[4)], Martinez Nicholas[5)], Johanes Fernandes Andry[6)]

[1)] Program Studi Manajemen, Universitas Multimedia Nusantara
[2,3,4,5)]Program Studi Sistem Informasi, Universitas XYZ
[1)]hendy.tannady@gmail.com [2)]l1649@lecturer.ubm.ac.id [3)]s31220032@student.ubm.ac.id [4)]s31220010@student.ubm.ac.id
[5)]s31220022@student.ubm.ac.id [6)]jandry@bundamulia.ac.id

Diajukan 14 Juni 2023 / Disetujui 4 September 2023

Abstrak

Sistem Informasi Akademik atau Pendidikan sudah ada hampir di seluruh sekolah dan universitas di Indonesia. Informasi sangat mudah didapatkan dan disebarluaskan. Hal itu membuat informasi menjadi sebuah aset yang sangat berharga baik untuk perseorangan, organisasi pemerintah maupun swasta. Keamanan dari sistem informasi menjadi isu yang wajib diperhatikan. Keamanan informasi adalah sebuah konsep untuk mengamankan asset informasi terhadap berbagai ancaman yang dapat memberikan dampak pada perusahaan atau organisasi. Masalah ini sangat penting karena jika sebuah informasi dapat diakses oleh orang yang tidak berwewenang atau tidak bertanggung jawab, maka keakuratan informasi tersebut akan dipertanyakan, bahkan akan menjadi sebuah informasi yang menyesatkan. Tujuan penelitian ini adalah untuk mengembangkan security policy, menemukan metode menjalankan SOP yang tepat, dan membuat rancangan untuk daily activity. Metode yang digunakan adalah kualitatif. Hasil dari pelaksanaan pkm ini antara lain, security policy, SOP, dan daily activity yang terdapat di sekolah ini masih ada kerentanan maupun kekurangan sehingga kami membuat beberapa rekomendasi yang diperuntukan untuk memperbaiki security policy, SOP, dan daily activity yang terdapat di sekolah ini agar lebih baik. Security policy yang terdapat di sekolah ini sudah bagus, tetapi masih ada yang kurang tepat, SOP Dalam menghadapi bencana alam yang terdapat di sekolah ini sebagian besar sudah mengikuti standar SOP sekolah lainnya dan tetap tidak luput dari kekurangan yang dimana para murid jarang dibekali dengan tata cara menyelamatkan diri sendiri dari bencana alam, daily activity yang dilakukan oleh petugas lab komputer di sekolah ini masih kurang tepat yang dimana pada saat di luar jam pelajaran pintu lab komputer masih dalam keadaan terbuka dan bisa saja orang yang berlalu lalang di tempat itu masuk dan mencuri data - data yang terdapat di lab komputer tersebut.
Kata kunci: Perangkat Keras, Lab, Sistem Informasi, Komputer

Abstract

Academic or Educational Information Systems are already available in almost all schools and universities in Indonesia. Information is easily obtained and disseminated, making it a valuable asset for individuals, government organizations, and private companies. The security of information systems is an issue that must be addressed. Information security is a concept for securing information assets against various threats that can have an impact on a company or organization. This issue is crucial because if information can be accessed by unauthorized or irresponsible individuals, the accuracy of that information will be questioned and may even become misleading. The purpose of this study is to develop a security policy, find the appropriate method for implementing SOP, and design daily activity. The method are used for this research is qualitative. The results of this research include a security policy, SOP, and daily activity that still have vulnerabilities or shortcomings in this school. Therefore, we have made several recommendations to improve the security policy, SOP, and daily activity in this school. The security policy in this school is already good, but there are still some areas that need improvementin dealing with natural disasters in this school mostly follows standard school SOPs but still lacks proper guidance for students on how to protect themselves during a natural disaster. The daily activity carried out by the computer lab staff in this school is still inadequate, as the lab doors are often left open outside of class hours, which could allow unauthorized individuals to enter and steal data from the computer lab.
Keywords: *Hardware, Lab, Information Systems, Computer*

*Korespondensi Penulis:

E-mail: hendy.tannady@gmail.com

Pendahuluan

1. Latar Belakang Masalah

Di zaman sekarang, Sistem Informasi menjadi sebuah kebutuhan yang menarik dalam berbagai bidang kehidupan manusia, salah satunya ada di bidang pendidikan. Sistem Informasi Akademik atau Pendidikan sudah ada hampir di seluruh sekolah dan universitas di Indonesia, bertujuan untuk mempromosikan penyediaan informasi kepada konsumen/penggunanya (siswa, staf pengajar dan staf administrasi) untuk mengelola informasi tersebut (Fathul, 2021). Informasi bisa dengan sangat mudahnya untuk didapatkan serta disebarluaskan. Hal itu membuat informasi menjadi sebuah aset yang sangat berharga baik untuk perseorangan, organisasi baik pemerintah maupun swasta, sehingga informasi ini perlu adanya pengamanan yang dilakukan (Nurul et al., 2022).

Keamanan dari sistem informasi menjadi isu yang perlu diperhatikan. Masalah ini sangat penting karena jika sebuah informasi dapat diakses oleh orang yang tidak berwewenang atau tidak bertanggung jawab, maka keakuratan dalam informasi tersebut akan dipertanyakan, bahkan akan menjadi sebuah informasi yang menyesatkan/*hoax* (Oktafiani, 2020). Keamanan informasi adalah konsep untuk mengamankan aset informasi dari berbagai ancaman yang dapat memberikan dampak buruk pada perusahaan atau organisasi yang memiliki aset informasi tersebut (Zulkarnain, 2020).

Dalam pelaksanaan pkm ini, pengumpulan data dan informasi dilakukan secara wawancara. Data-data tersebut kemudian kami analisis dan bandingkan dengan standar yang sudah teruji. Akhirnya, jika ada hal yang dapat dilakukan lebih baik lagi, akan diajukan proposal saran dari kami untuk SMA XYZ. Tujuan dari penulisan jurnal ini adalah mengembangkan Security Policy, SOP, serta kinerja keseharian keamanan sistem di lab komputer SMA XYZ agar pelaksanaanya dapat dijalankan secara maksimal, terlebih ketika ada bencana alam. Manfaat yang diperoleh atas penulisan jurnal ini adalah SMA XYZ dapat menjalankan Security Policy, SOP, serta keseharian keamanan sistem secara maksimal dan efisien.

2. Rumusan dan Batasan Masalah

Berdasarkan latar belakang diatas, maka rumusan masalah dalam penelitian ini adalah sebagai berikut :

1) Bagaimana Sistem Informasi di SMA XYZ sebagai media pembelajaran?
2) Bagaimana mengaplikasikan akses data informasi lab di SMA XYZsaat di jaga?
3) Bagaimana keamanan IT di SMA XYZ pada saat dijaga terhadap bencana alam?
4) Bagaimana penerapan SOP di SMA XYZ?
5) Bagaimana dengan Daily Activity yang terjadi di SMA XYZ?

Dalam penelitian ini ditetapkan batasan masalah sebagai berikut :

1) Penelitian yang dilakukan hanya pada sekolah XYZ
2) Penelitian hanya berfokus pada analisa hardware dan IT Security dalam lab.
3) Penelitian bertujuan untuk memahami aplikasi materi seputar SI dan IT untuk murid SMA XYZ
4) Praktek murid SMA XYZ sehari-hari dalam aplikasi IT Security dan penggunaan hardware di ruangan lab komputer.

3. Tujuan dan Manfaat

Berdasarkan rumusan masalah diatas, maka tujuan dalam penelitian ini adalah sebagai berikut:

1) Memaksimalkan dan memperbaiki penggunaan hardware di lab SMA XYZ.
2) Tingkatkan pengelolaan akses data informasi lab SMA XYZ.
3) Mengimplementasikan IT Security lab SMA XYZ.
4) Pastikan Proses SOP sekolah berjalan dengan efektif, efisien, dan konsisten.
5) Pastikan kegiatan harian di SMA XYZ berjalan dengan lancar dan efektif.

Penelitian ini diharapkan dapat memberikan manfaat sebagai berikut :

1) Meningkatkan efisiensi dan produktivitas pada saat di lab sekolah SMA XYZ.
2) Memudahkan pengelolaan dan penyimpanan data hasil praktikum selama di lab SMA XYZ.
3) Meningkatkan kepercayaan siswa, guru, dan orang tua terhadap sistem informasi di lab SMA XYZ.
4) Meningkatkan kualitas pelayanan, dan mencapai tujuan target.
5) Pastikan kegiatan rutin tepat waktu dan aman untuk siswa maupun guru

Landasan Teori

Hardware merupakan perangkat komputer yang terdiri dari komponen-komponen elektronik berbentuk fisik yang memiliki fungsi untuk mendukung proses komputerisasi. Ada beberapa jenis perangkat keras yang dapat dilihat dan disentuh langsung, seperti peralatan pemrosesan (CPU), input/output device (*keyboard*, monitor, *disk drive*, dll), dan perangkat penyimpanan (memori utama). Perangkat keras juga merupakan penghubung antara pengguna dan sistem pada komputer, yang memungkinkan pengguna untuk berinteraksi dengan komputer dan melaksanakan tugas-tugas tertentu.

Dalam perangkat keras, CPU (*Central Processing Unit)* berperan penting dalam memproses suatu perintah serta melaksanakan pengurusan melalui informasi pada sistem komputer (Simanullang, 2021). Selain itu, terdapat juga *input/output device* yang berfungsi untuk mendapatkan informasi dari luar dalam bentuk fisik atau nonfisik, seperti keyboard, monitor, *disk drive*, *camera*, web, *printer*, *scanner*, dan lain-lain. Terakhir, perangkat penyimpanan seperti memori utama sangat penting dalam menyimpan informasi pada sistem komputer. Dengan demikian, *hardware* adalah bagian penting dari komputer yang memiliki peran besar dalam mendukung berbagai proses komputerisasi.

Keamanan Sistem Informasi meliputi pencegahan dan deteksi penipuan pada sistem informasi yang tidak memiliki arti fisik. Ada tiga dimensi dalam mengukur keamanan sistem informasi yaitu pengetahuan, sikap, dan perilaku. Keamanan informasi harus dilindungi karena merupakan aset penting perusahaan, kebocoran informasi atau kegagalan sistem dapat menyebabkan kerugian finansial dan produktivitas (Abdul et al., 2019).

Dimensi atau indikator Keamanan SI memili 2 sisi yang berelevan dengan pengetahuan lingkungannya (*revelance*) dan patuh pada dasar yang sudah ditetapkan. Di dalam upaya penanganan dan pengendalian terhadap Keamanan Sistem Informasi, ada tiga aspek penting dalam keamanan informasi CIA (*Confidentiality* , *Intergrity, Availability*):

1. Kerahasiaan *(Confidentiality)*
   Aspek yang memastikan bahwa informasi hanya dapat diakses oleh orang yang memiliki wewenang.
2. Integritas *(Integrity)*
   Aspek penjaminan bahwa tidak ada pengubahan data tanpa seizin pihak yang berwenang demi menjaga keakuratan dan keutuhan informasi.
3. Ketersediaan(*Availabillity*)
   Aspek memberi sebuah jaminan terhadap ketersediaan data saat pihak pengguna membutuhkannya, kapanpun, dan dimanapun (Nurul et al., 2022).

Definisi dari bencana yang terdapat pada UU No. 24 Tahun 2007 adalah peristiwa atau rangkaian peristiwa yang disebabkan oleh faktor alam dan non alam yang mengancam dan mengganggu kehidupan dan penghidupan masyarakat. Seiring berjalannya waktu dan meningkatnya aktivitas manusia, degradasi lingkungan akan semakin parah dan meningkatkan jumlah bencana hidrometeorologi seperti banjir, tanah longsor, kebakaran hutan, gempa bumi dan kekeringan yang mengakibatkan kematian akibat kurangnya informasi/peringatan dini. Selain itu, bencana ini juga mempengaruhi keamanan Sistem Informasi yang ada di seluruh Indonesia, karena akibat bencana alam tersebut, kemananan SI mengalami banyak kegagalan sistem seperti pada saat banjir,

informasi penting yang terdapat di komputer bisa tenggelam dan mengalami kerusakan yang parah (Muhammad et al., 2018).

Dalam penulisan jurnal ini, analisis yang dilakukan atas data-data yang terkumpul didasarkan ataskontrol keamanan. Terdapat tiga jenis kontrol keamanan umum: kontrol fisik, kontrol administratif, dankontrol korektif. Sedangkan pada kontrol keamanan berdasarkan sifatnya dibagi menjadi tiga, yaitu kontrol keamanan preventif, kontrol keamanan detektif, serta kontrol keamanan korektif.

Kontrol fisik mengacu pada beberapa perangkat fisik yang mencegah atau menghalangi sesorang yang tidak berkepentingan melakukan akses terhadap lab komputer. Kontrol administratif (prosedural) bergantung pada prosedur-prosedur, contohnya memberikan pelatihan kepada karyawan mengenai betapa pentingnya keamanan dalam berorganisasi atau meminta manajer memeriksa kinerja kerja karyawan. Kontrol teknis mengacu pada perangkat lunak yang membuat kontrol logis, misalnya seperti kata sandi. Peraangkat keras khusus seperti *firewall* akan dianggap sebagai kontrol teknis karena berisi perangkat lunak yang diperlukan untuk membuat kontrol logis (Johnson & Easttom, 2020).

Kontrol preventif merupakan proses untuk menghentikan insiden atau memberikan pelanggaran secara langsung. Kontrol keamanan ini dirancang untuk menncegah dan berjalan secara otomatis. Kontrol keamana detektif merupakan proses dimana control keamanan ini tidak mencegah insiden atau memberi pelanggaran secara langsung, tetapi cara kerjanya seperti *alarm*, dimana ia hnaya akan memberi informasi bahwa terjadi suatu insiden dalam sebuah organisasi. Contohnyaketika *alarm*memberi tahu terjadinya kebakaran di suatu tempat, pemadam kebakaran terdekat akan diberi tahu dan tidak langsung sampau di lokasi. Kontrol keamanan ini merupakan sistem deteksi intrusi atau sistem pencegahan intrusi (*IDS/IPS*). Sistem tersebut mengamati aktivitas jaringan untuk anomali yang tampaknya terkait dengan serangan atau pelanggaran terhadap kebijakan/aturan tertentu. Kemudian, ketika anomali terdeteksi, mereka dicatat, dan personel yang tepat akan diberitahu(Johnson & Easttom, 2020).

Kontrol keamanan korektif tidak mencegah insiden atau pelanggaran secara langsung. kontrol keamanan korektif membatasi dampak terhadap bisnis dengan mengoreksi kerentanan terhadap suatu sistem dan seberapa cepat bisnis dapat memulihkan operasi yang menentukan efektivitas pengendalian.Kontrol keamanan korektif adalah tindakan untuk memperbaiki masalah yang terjadi baik kecil maupun besar. Strategi kontrol keamanan korektif dilaksanakan setelah kontrol keamanan detektif, manajemen dari organisasi ini yang akan memutuskan tindakan apa yang akan dilakukan dalam menghadapi masalah yang terjadi setelah proses kontrol keamanan detektif (Johnson & Easttom, 2020).

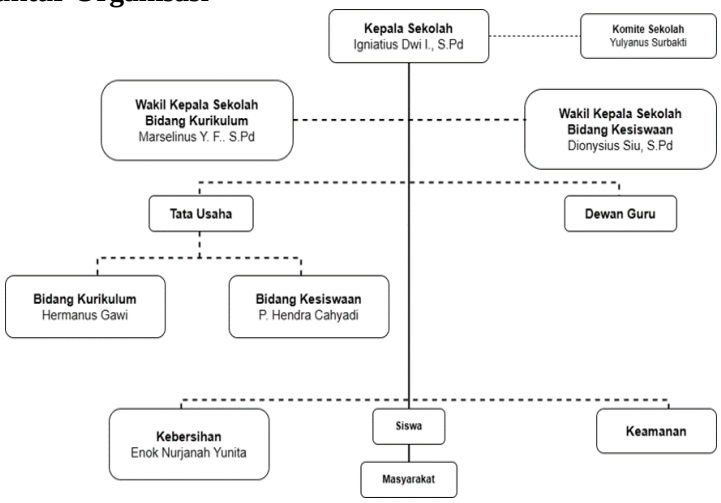
Keamanan sistem operasi adalah bagian penting dari keamanan sistem komputer secara keseluruhan (Abdul et al., 2019). Selain pengamanan secara fisik untuk membatasi pengaksesan langsung ke fasilitas komputer, keamanan sistem operasi juga dibagi menjadi tiga bagian utama: keamanan eksternal, interface pemakai, dan internal. Keamanan eksternal berkaitan dengan ancaman dari penyusup dan bencana alam, sedangkan keamanan interface pemakai berkaitan dengan identifikasi pengguna sebelum diizinkan mengakses program dan data yang disimpan. Keamanan internal melibatkan kendali terhadap *hardware* serta sistem operasi dalam menjaga integritas suatu program dan data. Meskipun sering digunakan secara bergantian, istilah keamanan mengacu pada masalah keamanan secara keseluruhan, sedangkan istilah mekanisme proteksi mengacu pada mekanisme sistem yang digunakan untuk melindungi informasi pada sistem komputer.

Maintenance (perawatan) adalah suatu kegiatan untuk menjaga dan memelihara fasilitas maupun mengadakan perbaikan, penyesuaian atau penggantian, agar terdapat suatu keadaan operasi produksi yang memuaskan sesuai dengan yang diharapkan. Perawatan ini bertujuan untuk mencegah dan mengurangi ataupun menghindari kerusakan lebih jauh dari peralatan dengan memastikan tingkat keandalan dan kesiapan serta meminimalisir biaya perawatan. Lalu juga untuk menjamin ketersediaan, keandalan fasilitas baik secara ekonomis maupun teknis, dengan begitu penggunaannya dapat dioptimalkan sebaik mungkin. Perawatan juga memperpanjang usia fasilitas, menjamin kesiapan operasional fasilitas dan yang paling penting adalah menjamin keselamatan kerja, keamanan dalam penggunaannya

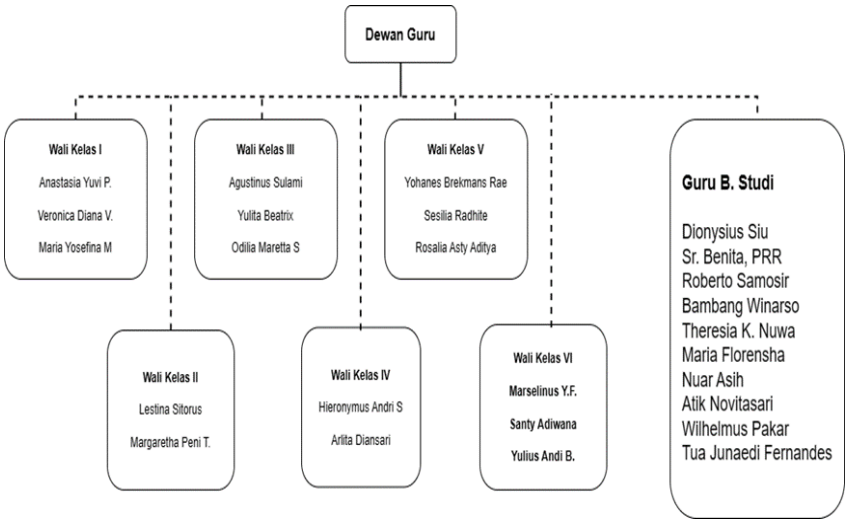
Kontrol keamanan dapat dikategorikan berdasarkan jenis kontrol dan apa yang dilakukan oleh kontrol tersebut. Kategori pertama mencakup kontrol administratif, teknis, dan kontrol fisik. Kategori kedua mencakup kontrol detektif atau responsif dan kontrol korektif. Contoh dari kontrol ini termasuk proses manajemen perubahan, sistem *antivirus*, dan pagar untuk kontrol fisik. (Johnson & Easttom, 2020).

Metode Penelitian

1. Struktur Organisasi

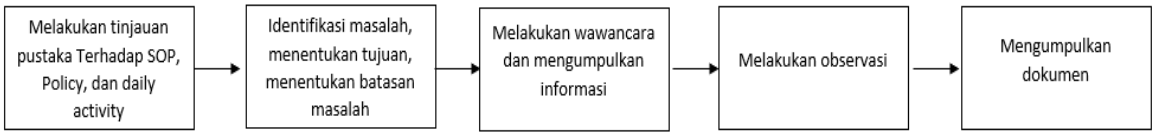


Gambar 1. Struktur Organisasi Guru dan Karyawan
Tahun Ajaran 2022 - 2023



Gambar 2 . Struktur Organisasi Guru dan Karyawan (2)

Pelaksanaan PKM yang kami lakukan untuk memperoleh informasi mengenai lab komputer SMA XYZ yaitu dengan cara mendatangi Sekolah XYZ secara langsung dan berdiskusi dengan kepala sekolah SMA XYZ yaitu Ibu Anastasia Sri Prihartini pada hari Kamis tanggal 9 Februari 2023 Di Sekolah XYZ dan kami melakukan sesi wawancara dengan yang bersangkutan yaitu Pak Sumitro Siahaan selaku guru Komputer di SMA XYZ pada tanggal 13 Februari 2023. Lalu tim pelaksana PKM melaksanakan proses penyusunan jurnal dari 13 Februari 2023 sampai 9 Maret 2023. Berikut merupakan skema/*flowchart* kunjungan pelaksanaan PKM yang kami jalankan.



Gambar 1. Skema pelaksanaan PKM

Melalui *flowchart* ini, langkah-langkah penting dalam pelaksanaan PKM untuk tinjauan lab komputer SMA XYZ tergambar dengan jelas.*Flowchart* tersebut menggambarkan langkah-langkah dalam pelaksanaan Program Kreativitas Mahasiswa (PKM) terkait tinjauan lab komputer di SMA XYZ. Tahap pertama adalah melakukan tinjauan pustaka terhadap SOP, kebijakan, dan aktivitas harian terkait lab komputer. Tinjauan pustaka ini bertujuan untuk memperoleh pemahaman yang mendalam tentang prosedur yang berlaku, kebijakan yang diterapkan, dan kegiatan rutin di lab komputer tersebut.

Setelah tinjauan pustaka, langkah selanjutnya adalah identifikasi masalah, menetapkan tujuan, dan membatasi ruang lingkup masalah. Identifikasi masalah dilakukan untuk mengidentifikasi permasalahan yang ada di lab komputer, sementara menetapkan tujuan membantu menentukan arah penelitian yang akan diambil. Pembatasan masalah penting untuk memfokuskan penelitian pada aspek yang relevan dan memungkinkan pemecahan masalah yang lebih spesifik. Pada tahap identifikasi, tim PKM melakukan wawancara dan mengumpulkan informasi dari pihak terkait. Wawancara dilakukan dengan Kepala Sekolah dan Guru Komputer untuk memperoleh pemahaman langsung tentang lab komputer, termasuk masalah yang dihadapi, kebijakan yang diterapkan, infrastruktur, dan aktivitas sehari-hari. Informasi yang diperoleh dari wawancara memberikan gambaran yang lebih komprehensif tentang kondisi lab komputer.

Selanjutnya, tim PKM melakukan observasi langsung di lab komputer. Observasi ini memberikan kesempatan untuk melihat langsung kondisi fisik lab komputer, penggunaan perangkat dan teknologi, serta kegiatan yang dilakukan oleh siswa dan guru. Observasi membantu dalam mengidentifikasi masalah yang mungkin tidak terungkap selama wawancara dan memperoleh pemahaman yang lebih mendalam tentang operasional lab komputer.Selama proses wawancara dan observasi, tim PKM juga mengumpulkan dokumen terkait lab komputer. Dokumen ini mencakup SOP, kebijakan, laporan kegiatan, dan dokumentasi lainnya yang relevan. Pengumpulan dokumen ini penting untuk mendukung analisis lebih lanjut dan memberikan data tambahan yang dibutuhkan.Setelah melalui semua langkah tersebut, tim PKM menganalisis data dan informasi yang telah dikumpulkan untuk mengidentifikasi temuan dan pola. Hasil analisis ini digunakan untuk merumuskan rekomendasi atau solusi yang dapat membantu meningkatkan lab komputer di SMA XYZ. Hasil penelitian kemudian disusun dalam bentuk jurnal yang mencakup tinjauan pustaka, metodologi, temuan, analisis, dan rekomendasi.

Metode pengumpulan data yang digunakan oleh tim pelaksanan pkm adalah metode pengumpulan data secara kualitatif, yang dimana tim PKMmewawancarai seorang narasumber dari SMA XYZ, yakni dengan guru TIK (Teknologi Informasi dan Komunikasi) yang bernama Bapak Sumitro Siahaan dalam mengumpulkan data-data yang diperlukan untuk pelaksanaan PKM yang kami teliti pada 13 Februari 2023 di SMA XYZ. Proses survei tersebut kami laksanakan bersamaan dengan wawancara terhadap narasumber kami.

Analisis Dan Pembahasan

Current

Berdasarkan data-data dan informasi yang kami telah kumpulkan dari observasi dan wawancara yang dilakukan, berikut merupakan hal-hal untuk keamanan sistem informasi yang diterapkan di SMA XYZ:

a. *Security Policy*
- *Passwordwifi* hanya dapat diakses oleh bidang *IT* dan sebagian guru, untuk siswa hanya diperkenankan menggunakan *password* di dalam lab komputer saja yang dimana *password*

tersebut bisa diketahui dari *passworduser*/kata sandi pengguna yang harus diketahui oleh semua siswa SMA XYZ dari masing–masing kelas, karena *password user* dari semua kelas di SMA XYZ berbeda. Jika ada peretasan yang terdeteksi, maka akan diganti *password*nya.
- Tersedia APAR (Alat Pemadam Api Ringan) di samping pintu masuk lab komputer.
- Terdapat sebuah *CCTV* di bagian depan ruangan lab komputer.

b. SOP
- Siswa harus berpakaian rapi dan lengkap pada di dalam ruangan kelas maupun di lab komputer.
- Harus menempati tempat duduk yang sama selama satu semester penuh, jika tidak maka penilaian masing–masing siswa akan terdapat kendala.
- Saat menggunakan fasilitas lab, siswa-siswi wajib untuk menjaga kebersihan dan kerapihan lab.
- Tidak boleh membawa makanan dan minuman ke dalam lab komputer pada saat pembelajaran TIK berlangsung.
- Minimal keterlambatan dalam memasuki ruangan lab komputer yaitu 15 menit setelah pembelajaran mulai.
- Jika terjadi banjir, sekolah akan diliburkan, lalu pihak sekolah mengambil Tindakan untuk melindungi server agar tidak rusak dengan cara mengambil *harddisk* yang isinya berupa *file-file* penting yang ada di lab komputer.
- Jika terjadi kebakaran, di gedung disediakan alat pendeteksi asap yang disambungkan ke sebuah alarm. Jadi ketika terdeteksi asap, alarm tersebut akan berbunyi. Pihak guru dan keamanan sekolah (satpam) menuntun para siswa-siswi untuk menjalankan proses evakuasi dengan jalur yang disediakan.
- Jika terjadi gempa bumi, pihak guru dan keamanan sekolah (satpam) menuntun para siswa-siswi untuk menjalankan proses evakuasi dengan jalur yang disediakan.
- Lift akan dimatikan selama terjadi bencana alam.
- Demonstrasi untuk hal yang perlu dilakukan saat ada bencana alam jarang dilakukan.
- Pengecekan suhu sebelum memasuki gedung .

c. *Daily Activity*
- Saat pergantian pelajaran TIK, para siswa-siswi diwajibkan untuk memasuki lab komputer paling lambat 15 menit setelah pelajaran dimulai. Jika ada keterlambatan, dikenakan sanksi.
- Kemudian para siswa diwajibkan untuk duduk ke tempat masing-masing dan *login* sesuai *username* kelas.
- Setelah pembelajaran selesai, guru yang bertanggung jawab akan mengecek *file-file* dari masing-masing komputer murid. Jika ditemukan *file* yang tidak berhubungan dengan pelajaran, maka *file* akan di *delete* agar tidak mengganggu sistem pembelajaran selanjutnya. Lalu, guru akan mem*backupfile-file* murid melalui server secara manual.
- Selain itu, para siswa *logout* dari *username* kelas sebelum meninggalkan lab.

Masalah

Dari data-data tersebut, kami menganalisis dan mendapati bahwa ada beberapa celah yang dari sistem yang ada sebagai berikut:

a. *Security Policy*
- *Passwordwifi* yang berada di lab komputer sangat mudah sekali untuk di *hack*/diretas oleh pihak yang tidak bertanggung jawab.
- Tidak adanya pelatihan dalam menggunakan APAR (Alat Pemadam Api Ringan) bagi para siswa.
- Kurangnya *CCTV* untuk melakukan pengawasan terhadap siswa-siswi dalam lab komputer, sedangkan ruangannya cukup besar sehingga guru akan sulit untuk mengawasi siswa-siswi yang berada diluar jangkauan *CCTV*.
- Kurangnya personil untuk melakukan pengawasan terhadap siswa-siswi di lab komputer dikarenakan guru yang bertanggung jawab hanya satu.

b. SOP
- Demonstrasi untuk hal yang perlu dilakukan saat ada bencana alam jarang dilakukan.
- Peraturan tertulis yang ada di dalam lab seperti, tidak boleh membawa makanan dan minuman, tidak boleh tidur di dalam lab komputer, tidak boleh men*downloadgame*; masih mudah dilupakan oleh siswa-siswi.
- Karena lab komputer SMA di lantai 1 dan di *lobby* ada resiko besar berupa orang yang berlalu Lalang bisa memasuki ruangan lab komputer SMA.
- Jika terjadi kebakaran dan alat pendeteksi asap telah mendeteksi asap dan alarm sudah berbunyi, ada kemungkinan bahwa tidak ada bantuan yang datang untuk menolong memadamkan api tersebut, maka akan menerima kerugian yang parah.

c. *Daily Activity*
- Banyak file-file yang tidak ada hubungannya dengan pelajaran yang tidak terhapus oleh guru-guru pada saat melakukan pengecekan pada komputer-komputer yang ada di lab.
- Pada saat mem-*backup* data, masih dilakukan dengan cara *manual* dengan mendatangi komputer siswa-siswi secara satu per satu.
- Sebagian siswa-siswi lupa *username* kelas mereka.
- Masih banyak siswa-siswi yang selalu lupa *logout username* mereka pada saat selesai belajar.

Rekomendasi

Dari masalah-masalah yang kami dapati, berikut adalah rekomendasi yang dapat kami berikan kepada SMA XYZ agar sistemnya lebih kuat:

a. *Security Policy*
- Melakukan pergantian *password* secara rutin setidaknya seminggu sekali untuk menghindari terjadinya aksi peretasan/*hacking*.
- Mengadakan sebuah acara bagi siswa/siswi untuk pendemostrasian dalam menggunakan APAR/*fire extinguisher* agar para siswa-siswi bisa menggunakan APAR/*fire extinguisher* dengan tepat.
- Menambahkan *CCTV* lagi di bagian belakang lab komputer agar guru bisa mengawasi siswa/siswi dalam menggunakan komputernya masing-masing, dan juga ini bisa membantu guru untuk menegur murid yang men*download*/memainkan sebuah *game* pada saat pembelajaran berlangsung.
- Menambahkan personil (bisa wakil atau guru lain) untuk melakukan pengawasan terhadap siswa-siswi di lab komputer. Hal ini juga akan membantu saat guru yang bersangkutan tidak dapat hadir untuk mengajar.

b. SOP
- Melakukan demonstrasi ketika terjadi bencana alam, agar siswa-siswi bisa melakukan hal yang tepat ketika terjadinya bencana alam tersebut dan bisa menyelamatkan diri.
- Menggunakan poster yang ditempel mengenai peraturan yang ada di dalam lab tersebut, atau memasangkan peraturan tersebut di *desktop* masing-masing komputer.
- Memperketat keamanan di sekitar lab komputer SMA yang berada di lantai 1 yang berdekatan dengan *lobby* dengan memberi *security* tambahan untuk menjaga lab komputer.
- Menyambungkan alat pendeteksi asap yang langsung terhubung kepada pemadan kebakaran di sekitar Petojo, sehingga mendapatkan pertolongan yang sigap.
- Menambahkan *fire sprinkler* di masing-masing kelas dan ruang guru.

c. *Daily Activity*
- Menyalakan *auto delete file* yang baru saja di*download* oleh siswa (*file* tidak penting) pada masing-masing komputer yang ada di lab Ketika komputer tersebut di *shut down*.
- Membuat sebuah sistem *cloud computing* seperti *google drive* sebagai media untuk siswa-siswi mengumpulkan tugas-tugas yang telah dikerjakan pada saat pembelajaran. *Backup file* juga dapat dilakukan dengan menggunakan *software* yang mengintegrasikan seluruh

komputer (seperti komputer operator warung internet) tertentu untuk bisa mem-*backup file* tersebut dengan menggunakan satu komputer saja.

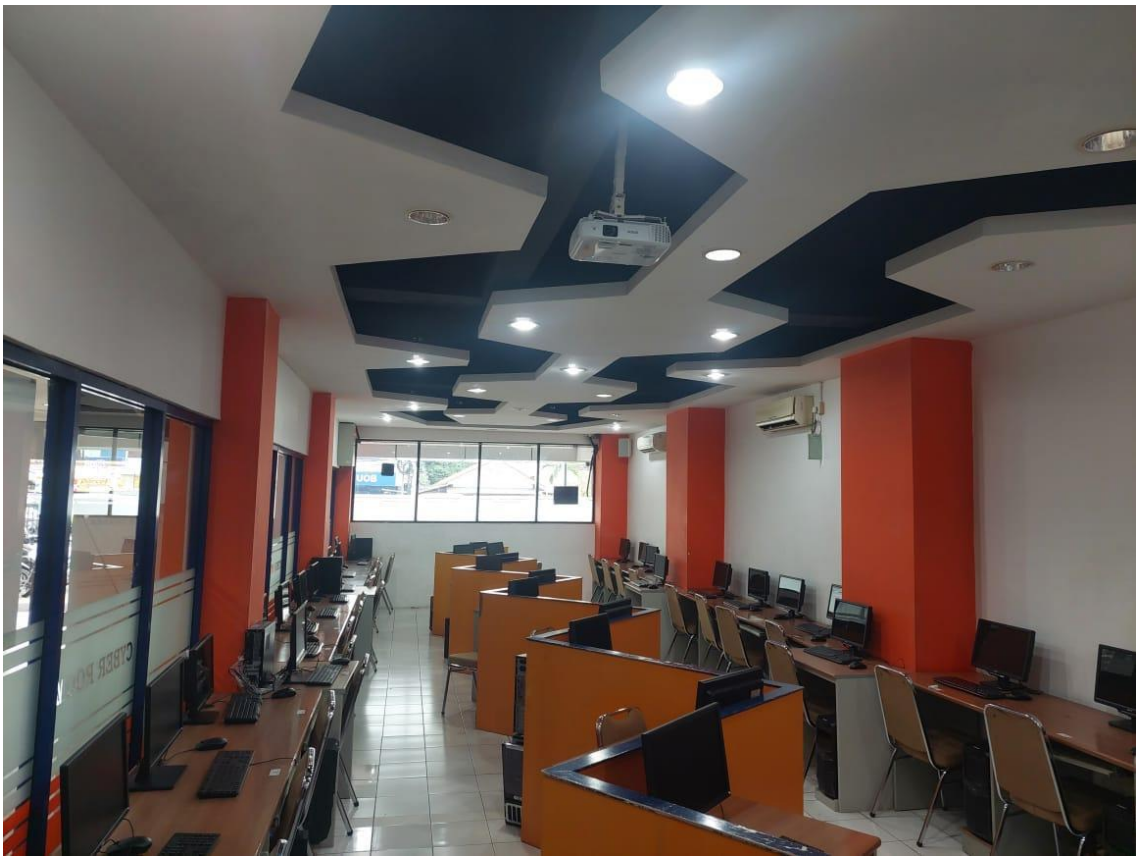
- Memberikan secarik kertas yang berisi *username* kelas kepada siswa-siswi yang akan menggunakan lab komputer tersebut, agar para siswa-siswi tidak akan lupa *username* mereka lagi.
- Tidak memperbolehkan siswa-siswi meninggalkan lab komputer jika belum *logout username* mereka.

Gambar 2. Ruang Kelas SMA XYZ

Gambar di atas ini merupakan gambaran salah satu dari seluruh kelas yang berada di SMA(Sekolah Menengah Akhir) XYZ, di dalam kelas tersebut disediakan bangku dan juga meja yang di butuhkan sesuai dengan jumlah murid yang berada di dalam kelasnya. Dan di setiap sudut dari kelas tersebut terdapat satu meja guru beserta dengan bangkunya untuk guru tersebut melakukan pengajaran/pembelajaran di dalam kelas tersebut. Di dalam kelas tersebut juga terdapat dua buah papan tulis beserta dengan spidol dan juga penghapus yang digunakan oleh guru dan siswa/siswi untuk melaksanakan pembelajaran seperti penjelasan materi, tanya jawab murid dan guru, dan juga untuk memberikan informasi penting terkait dalam pembelajaran jika guru yang bersangkutan berhalangan hadir.

Gambar 3. Ruang Guru SMA XYZ

Gambar di atas ini merupakan tempat para guru yang sebelum/sesudah mengajar beristirahat/mengerjakan pekerjaan mereka seperti melakukan penilaian terhadap tugas dan penilaian ulangan pada siswa/siswi SMA XYZ. Tempat ini juga merupakan tempat guru-guru SMA XYZ melakukan rapat penting, seperti rapat jadwal pembagian rapot, menentukan jadwal Ujian Tengah Semester (UTS) dan Ujian Akhir Semester (UAS), Ujian Sekolah, Ujian Prakter (khusus murid SMA kelas 3) dan lainnya.



Gambar 4. Lab komputer SMA XYZ

Gambar di atas ini merupakan tempat di mana para siswa/siswi SMA XYZ melakukan pembelajaran yang bermata pelajaran TIK (Teknologi Informasi dan Komunikasi). Tempat ini merupakan target dari penelitian yang kami lakukan dari segi Keamanan Sistem Informasinya dan mempelejari Keamanan Sistem Informasi yang di ajarkan.

Gambar 5. Tata Usaha SMA XYZ

Gambar di atas adalah tempat dimana para guru melakukan pengumuman/memberikan informasi jika ada pergantian pada pembelajaran, istirahat, memanggil murid jika ada keperluanpenting dengan salah satu guru. Dan juga setiap pagi sebelum memulai pembelajaran para murid diwajibkan bergantian untuk melakukan renungan pagi dan doa pagi lalu renungan pagi yang dilakukan oleh para siswa/siswi tersebut disiarkan melalui alat pengumuman yang disediakan di dalam ruangan tata usaha tersebut. Lalu jika ada informasi/pengumuman penting akan disiarkan ke setiap kelas, agar para murid yang berada di masing-masing kelas bisa mengetahui informasi/pengumuman yang di berikan.

Gambar 6. Lapangan Basket

Gambar di atas merupakan lapangan di Sekolah XYZ yang memiliki akses melalui Tangga SMA (Sekolah Menengah Atas) dan SMP(Sekolah Menengah Pertama) dan juga memiliki 2 jenis lapangan, yaitu lapangan *futsal* dan lapangan basket, gambar di atas ini merupakan lapangan basket. Sesuai namanya lapangan ini dipakai oleh SMP dan juga SMA XYZ untuk bermain basket pada saat jam olahraga berlangsung/diadakan. Lapangan basket ini juga bisa digunakan sebagai tempat upacara bendera untuk seluruh murid Sekolah XYZ dari SD (Sekolah Dasar), SMP (Sekolah Menengah Pertama),SMA (Sekolah Menengah Atas), dan SMK (Sekolah Menengah Kejuruan), dan jika di salah satu mata pelajaran memiliki materi bola voli, lapangan basket inilah yang akan dijadikan lapangan bola voli, dengan menggunakan *net* tambahan untuk menjadi pemisah antara 2 kelompok voli murid – murid yang sedang menggunakan lapangan.

Gambar 7. Lapangan *Futsal*

Gambar di atas ini merupakan lapangan *futsal* yang disebutkan sebelumnya. Sesuai namanya lapangan ini digunakan oleh SMP (Sekolah Menengah Pertama) dan SMA (Sekolah Menengah Atas) XYZ untuk bermain *futsal* jika terdapat materi *futsal*/sepak bola di pembelajaran olahraga, dan juga seperti lapangan basket, tempat ini bisa dijadikan sebagai tempat upacara, karena jika hanya menggunakan 1 lapangan saja, makalapangan basket di atas tadi tidak akan mencukupi seluruh murid Sekolah XYZ yang jumlah murid di satu sekolah sampai ratusan murid. Kedua lapangan ini juga sering dipakai pada akhir – akhir semester untuk melakukan pertandingan *class meetin*g (pertandingan antar kelas) dari *futsal*, basket, dan voli. Bahkan jika ada acara Kemerdekaan Indonesia kedua lapangan tersebut digunakan untuk melakukan lomba– lomba yang di adakan.

Gambar 8. Tim PKM berfoto bersama narasumber

Gambar diatas merupakan foto tim PKM pada saat berkunjung dan melakukan wawancara ke Sekolah XYZ dan melakukan wawancara bersama narasumber yakni dengan Pak Sumitro Siahaan selaku guru Sekolah XYZ dari pelajaran TIK (Teknologi Informasi dan Komunikasi). Proses wawancara ini dilakukan pada tanggal 13 Februari 2023 dan sebelum melakukan wawancara ini kami melakukan pendiskusian dengan kepala sekolah yaitu Ibu Anastasia Sri Prihartini pada tanggal 9 Februari 2023 untuk mendapatkan izin dalam melakukan wawancara terhadap Keamanan Jaringan Informasi terhadap bencana alam yang terjadi pada Sekolah XYZ .

Simpulan

Berdasarkan hasil analisis yang di dapatkan disimpulkan bahwa:

1. Menurut kami tim penulis, Security Policy yang terdapat di dalam lab komputer SMA XYZ sudah bagus, tetapi masih ada Security Policy yang masih kurang tepat, seperti untuk pengawasan murid yang dikarenakan hanya mempunyai 1 guru dan 1 CCTV bisa menyulitkan guru tersebut untuk memperhatikan para murid mengikuti pelajaran dengan baik atau hanya bermain game.
2. Menurut kami, SOP menghadapi bencana alam yang terdapat di SMA XYZ sebagian besar sudah mengikuti standar SOP sekolah lainnya. SOP yang ada di SMA XYZ ini masih banyak kekurangannya, seperti sebagian murid yang masih belum mengetahui cara menyelamatkan diri di lingkungan sekolah, karena jarang melakukan demonstrasi bencana alam.
3. Menurut kami, Daily Activity yang dilakukan oleh petugas lab komputer masih kurang tepat yang di mana pada saat di luar jam pelajaran pintu lab komputer masih dalam keadaan terbuka, sehingga ada kemungkinan besar orang yang tidak berkepentingan dan orang yang tidak berhak melakukan aksi pencurian data.

Kemudian adapun saran yang dapat kami berikan untuk SMA XYZ selain rekomendasi atas beberapa hal untuk keamanan sistem informasinya:

1. Keamanan sistem informasi yang terdapat di SMA XYZ masih banyak kekurangannya, seperti jika ada kendala sistem, tim bagian TI harus datang terlebih dahulu ke Sekolah XYZ karena tempat tim bagian memiliki kantor di luar Sekolah XYZ. Di perjalanan tersebut memiliki resiko bagi sistem yang sedang diretas, maka alangkah baiknya ada sebagian tim TI yang menetap di Sekolah XYZ, sehingga ketika sedang terjadi peretasan, tim TI bisa dengan sigap mengatasi masalah tersebut.
2. Karena guru TIK SMA XYZ hanya ada seorang, pada pengawasan pembelajaran akan ada kendala untuk mengawasi siswa-siswi dan menjelaskan materi secara bersamaan, alangkah

baiknya SMA XYZ bisa menambahkan guru TIK untuk melakukan proses pembelajaran yang lebih baik.

Daftar Pustaka

Andry, J. F., & Loisa, J. (2016). *The E-Commerce Potential For Home-Based Business : A Case Study*. *Jurnal Ilmiah Fifo*, 139.

Abdul, D. F., Budiman, M. I., & Kurniawan, T. (2019). Analisis Sistem Keamanan Sistem Operasi (Windows , Linux , MacOS). *Computers & Security*, *March*.

Ismawati, & Kuswanto, J. (2020). Sistem Pakar Kerusakan Hardware Komputer. *INTECH Informatika Dan Teknologi*, *1*(1), 17–23. http://journal.unbara.ac.id/index.php/INTECH.

Johnson, R., & Easttom, C. (2020). *Security Policies and Implementation Issues, 3rd Edition by Robert Johnson Chuck Easttom (z-lib.org)*. https://www.jblearning.com/catalog/productdetails/9781284199840.

Nurul, S., Anggrainy, S., & Aprelyani, S. (2022). Faktor-Faktor Yang Mempengaruhi Keamanan Sistem Informasi: Keamanan Informasi, Teknologi Informasi Dan Network (Literature Review Sim). *Ekonomi Manajemen Sistem Informas*, *3*(5). https://doi.org/10.31933/jemsi.v3i5.

Simanullang, P. M. (2021). *PENGARUH PERANGKAT KERAS KOMPUTER DALAM SISTEM INFORMASI MANAJEMEN The Effect Of Computer Hardware In Management Information Systems*. 10.31219/osf.io/c43en

Anggara, S. D. (2022). Praktik Pengendalian Internal pada Pengelolaan Keuangan di Lembaga Kemahasiswaan. *Perspektif Akuntansi*, *5*(2), 063–081. https://doi.org/10.24246/persi.v5i2.p063-081

Fathul, A. (2021). *Analisis Tingkat Keamanan Sistem Informasi Akademik (SIAKAD) UIN Ar-Raniry Menggunakan Standar ISO 27001;2013 dengan Klausul 11 dan 14*.

Johnson, R., & Easttom, C. (2020). *Security Policies and Implementation Issues* (3rd ed.).

Kurniawan, E. (2018). *Analisis Tingkat Keamanan Sistem Informasi Akademik Berdasarkan Standard ISO/IEC 27002:2013 Menggunakan SSE-CMM*.

Miftahurrizqi, Windiarti, I. S., & Prabowo, A. (2021). *Analisis Keamanan Sistem pada Sistem Informasi Akademik menggunakan COBIT 5 Framework pada Sub Domain DSS05*. 1–6.

Muhammad, F., Hadi, A., & Irfan, D. (2018). Pengembangan Sistem Informasi Panduan Mitigasi Bencana Alam Provinsi Sumatera Barat. *Jurnal Teknologi Informasi & Pendidikan*, *11*, 1–16.

Nurul, S., Anggrainy, S., & Aprelyani, S. (2022). *Faktor-Faktor yang Mempengaruhi Keamanan Sistem Informasi: Keamanan Informasi, Teknologi Informasi dan Network (Literature Review SIM)*. *3*(5). https://doi.org/10.31933/jemsi.v3i5

Oktafiani, C. (2020). *Keamanan Informasi Dalam Pemanfaatan Teknologi Informasi Pada PT. X*. 1–24.

Perdana, R. S. (2018). Audit Keamanan Sistem Informasi Akademik Menggunakan Framework Nist Sp 800-26 (Studi Kasus : Universitas Sangga Buana YPKP Bandung). *Jurnal Infotronik*, *3*(1).

Rendro, D. B., Ngantono, & Aji, W. N. (2020). Analisis Monitoring Sistem Keamanan Jaringan Komputer Menggunakan Software NMAP (Studi Kasus di SMK Negeri 1 Kota Serang). *PROSISKO*, *7*(2).

Sayuthi. (2021). *Konsep Pengendalian Intern Untuk Keamanan Sistem Informasi*. *17*, 290–308.

Wahyudi, H., Zulianto, A., Maulana, A., Mardira Indonesia, S., & Langlangbuana, U. (2020). Studi Kasus STMIK Mardira Indonesia. *Jurnal Computech & Bisnis*, *14*(1), 40–46.

Winanti, M. B., & Dzulhan, I. (2018). *Audit Keamanan Sistem Informasi Akademik Dengan Kerangka Kerja ISO 27001 di Program Studi Sistem Informasi Unikom*. 121–132.

Zulkarnain. (2020). Analisis Implementasi Keamanan Sistem Informasi pada Perusahaan Perakitan Elektronik. *Journal of Information System and Technology*, *01*.