DAFTAR LAMPIRAN

Lampiran 1. Riwayat Hidup

Data Pribadi

Nama : Fakhirah Din Mohamad

Tempat, Tanggal Lahir: Jakarta, 28 Mei 2001

Jenis Kelamin : Perempuan

Agama : Islam

Alamat : Jl. H. Alimin No.10EF RT01/01, Kel Kedoya Selatan, Kec Kebon jeruk, Kota Jakarta Barat, Kode Pos 11520

No Telepon : 087883934472

Email : irafakhirah838@gmail.com

Riwayat Pendidikan

Periode (Tahun)	Sekolah/Institusi/Universitas	Jurusan	Jenjang Pendidikan
2007 - 2013	SDN 04 Pagi Kedoya Selatan	-	SD
2013 - 2016	SMP Al-Kamal Jakarta Barat	-	SMP
2016 - 2019	SMK Multi Media Mandiri Jakarta Barat	TKJ	SMK
2019 - 2023	Universitas Esa Unggul	Sistem Informasi	S1

Lampiran 2. Wawancara

No.	Pertanyaan	Jawaban
1.	Interkoneksi jaringan pada Website SIAKAD terhubung dengan sistem apa?	Website SIAKAD terhubung dengan On premise
2.	Apa saja perangkat fisik yang telah terhubung dengan Website SIAKAD?	Server, Router, komputer beserta CPU
3.	Siapa saja yang bertanggung jawab dan bersangkutan dengan Website SIAKAD?	Yang bertanggung jawab dalam melakukan maintenance terhadap website SIAKAD ialah BTIK.
4.	Adakah peraturan tertentu dalam melaksanakan pengadaan hardware dan software. Kemudian sistem apa yang digunakan sebagai pendukung dalam menjalankan website SIAKAD?	Dalam pengadaan disesuaikan dengan kebutuhan padaa saat itu juga. Sistem yang digunakan sebagai pendukungnya ialah server on premise
5.	Pengendalian apa saja yang telah diterapkan dalam menangani keamanan informasi terhadap website SIAKAD?	Penggunaan Firewall sebagai standar keamanan sistem informasi
6.	Frekuensi dalam melakukan maintenance dilakukan berapa kali?	1 Tahun 2x (Tiap semester). Namun untuk maintenance infrastruktur dilakukan pada saat ada kebutuhan patch system (OS Upgrade, Service Upgrade, Resource Upgrade dan security patch). Jadi menentukannya tidak berdasarkan adanya perubahan system, begitupun dari sisi network.
7.	Apa yang dilakukan saat ini dalam melakukan penanganan jika terjadi kasus risiko yang sudah terjadi?	Penanganan risiko dilakukan pada saat kejadian tersebut terjadi di saat itu juga
8.	Berapakah jenis website SIAKAD yang sudah dibuat atau pernah dibuat? Kemudian untuk target penggunannya siapa saja?	Tidak Ada
9.	Siapa saja yang memiliki hak dalam menambahkan, merubah dan menghapus akses?	Yang memiliki hak dalam mengubah, menambahkan dan menghapus akses ialah BTIK.

10.	Berada dimanakah penempatan lokasi server yang digunakan untuk website SIAKAD?	Lokasi server berada di ruang BTIK (Biro Teknologi Informasi dan Komunikasi) kebon jeruk dan penempatan server berada di ruangan tersendiri.

Lampiran 3. Kuesioner

Kuesioner mengenai sumber ancaman berdasarkan asal aset

Tingkat Kerentanan	Penjelasan
High	Sumber ancaman yang memiliki motivasi tinggi dapat merugikan organisasi, hal ini terjadi karena pengendalian untuk mencegah kerentanan dilakukan tidak efektif.
Medium	Sumber ancaman memiliki motivasi yang mampu merugikan organisasi, namun organisasi masih dapat melakukan kontrol yang mana mampu menghambat keberhasilan dari kerentanan yang ada.
Low	Sumber ancaman yang memiliki motivasi kurang atau rendah, kontrol digunakan untuk mencegah atau mengurangi suatu kerentanan yang akan terjadi pada organisasi.

Sumber Ancaman	Hak Akses				Tujuan Serangan	Tingkat Kerentanan			Dampak yang terjadi
	Input	Ubah	Hapus	Backup		High	Medium	Low	
Dosen	✓	✓	✓	✓	*blank*			✓	Data nilai dan tugas menjadi berubah
Mahasiswa	✓	✓	✓		Mencoba login dengan user yang memiliki hak akses lebih tinggi		✓		Data akan lebih mudah dimanipulasi dan dicuri
Dalam BTIK	✓	✓	✓	✓	*blank*			✓	*blank*
Luar BTIK	✓	✓	✓	✓	Melakukan perubahan data			✓	Mengalami information exposure dan ada beberapa data berubah
Pemadaman Listrik	*blank*						✓		Dapat menyebabkan

					perangkat tidak berfungsi dengan baik
Server down/bermasalah	*blank*		✓		Sistem tidak dapat melakukan pengaksesan

Kuesioner ini bertujuan untuk melakukan identifikasi kejadian ancaman dan mencari sumber ancaman berdasarkan tingkat kemampuan dari pihak luar (*Eksternal)*.

TABLE E-4: RELEVANCE OF THREAT EVENTS

Value	Description
Confirmed	The threat event or TTP has been seen by the organization.
Expected	The threat event or TTP has been seen by the organization's peers or partners.
Anticipated	The threat event or TTP has been reported by a trusted source.
Predicted	The threat event or TTP has been predicted by a trusted source.
Possible	The threat event or TTP has been described by a somewhat credible source.
N/A	The threat event or TTP is not currently applicable. For example, a threat event or TTP could assume specific technologies, architectures, or processes that are not present in the organization, mission/business process, EA segment, or information system; or predisposing conditions that are not present (e.g., location in a flood plain). Alternately, if the organization is using detailed or specific threat information, a threat event or TTP could be deemed inapplicable because information indicates that no adversary is expected to initiate the threat event or use the TTP.

Nilai	Keterangan
Dikonfirmasi	Ancaman peristiwa atau TTP telah dilihat oleh organisasi.
[illegible]	Peristiwa ancaman atau TTP telah dilihat oleh rekan atau mitra organisasi.
Diantisipasi	Peristiwa ancaman atau TTP telah dilaporkan oleh sumber tepercaya.
Diprediksi	Peristiwa ancaman atau TTP telah diprediksi oleh sumber tepercaya.
Mungkin	Peristiwa ancaman atau TTP telah dijelaskan oleh sumber yang cukup kredibel.
T/A	Peristiwa ancaman atau TTP saat ini tidak berlaku. Misalnya, peristiwa ancaman atau TTP dapat mengasumsikan teknologi, arsitektur, atau proses tertentu yang tidak ada dalam organisasi, misi/proses bisnis, segmen EA, atau sistem informasi; atau kondisi predisposisi yang tidak ada (misalnya, lokasi di dataran banjir). Bergantian, jika organisasi menggunakan informasi ancaman yang terperinci atau spesifik, peristiwa ancaman atau TTP dapat dianggap tidak dapat diterapkan karena informasi menunjukkan bahwa tidak ada musuh yang diharapkan memulai peristiwa ancaman atau menggunakan TTP.

Keterangan:

- Pada kolom sumber ancaman, responden bisa menuliskan yang dimana dari pihak *Eksternal, Internal, Personal.*
  - *Eksternal* ialah pihak yang berasal dari luar Universitas Esa Unggul yang berusaha melakukan serangan.

- *Internal* ialah pihak yang berasal dari dalam Universitas Esa Unggul dapat melakukan kesalahan
- *Personal* ialah pihak yang melakukan kesalahan pribadi yang dapat mengacam informasi pribadi.

- Pada tabel relevance, apabila belum terjadi/tidak terjadi dapat dikosongkan (N/A)
- Pada bagian tabel dampak, dipersilahkan atau diperbolehkan kosong apabila *Relevance* tidak pernah terjadi

Sumber/informasi yang berasal dari sumber ancaman	**Sumber ancaman**	***Relevance***						**Dampak**
		Confirmed	***Expected***	***Antipated***	***Predicted***	***Possible***	***N/A***	
Melakukan upaya login paksa atau serangan menebak kata sandi.	*Internal* dan *Personal*	✓						Mengalami eksploitasi data pribadi
Melakukan serangan gangguan nirkabel.	*Internal*	✓						*blank*
Merusak atau mencemari data yang penting dapat menyebabkan hilangnya integritas.	*Eksternal* dan *Internal*			✓				Data yang telah diinput mengandung virus
Terjadinya serangan fisik terhadap infrastruktur pendukung pada fasilitas organisasi.	*Eksternal* dan *Internal*			✓				Perangkat mengalami kerusakan
Mengirimkan malware yang dimodifikasi ke sistem	*Eksternal* dan *Internal*			✓				Information exposure

Sumber/informasi yang berasal dari sumber ancaman	**Sumber ancaman**	***Relevance***						**Dampak**
		Confirmed	***Expected***	***Antipated***	***Predicted***	***Possible***	***N/A***	
informasi internal organisasi.								
Kumpulkan informasi menggunakan penemuan sumber terbuka informasi organisasi.	*Eksternal* dan *Internal*			✓				Information exposure
Mengeksploitasi sistem informasi yang terkonfigurasi dengan buruk atau tidak sah yang terpapar ke Internet.	*Eksternal* dan *Internal*			✓				Mengalami pencurian data
Melakukan serangan Denial of Service (DoS) yang ditargetkan.	*Eksternal*			✓				Sistem akan kesulitan diakses
Melakukan serangan menggunakan port, protokol dan tidak diizinkan untuk digunakan oleh organisasi.	*Eksternal* dan *Internal*			✓				Sistem akan kesulitan diakses
Melakukan serangan penyadapan komunikasi	*Eksternal*						✓	*blank*

Sumber/informasi yang berasal dari sumber ancaman	**Sumber ancaman**	***Relevance***						**Dampak**
		Confirmed	***Expected***	***Antipated***	***Predicted***	***Possible***	***N/A***	
Menyebabkan hilangnya integritas dengan membuat, Menghapus dan/atau memodifikasi data pada sistem informasi yang dapat diakses publik (misalnya, perusakan web).	*Eksternal*	✓						Data original diubah/dihapus
Menyebabkan pengungkapan yang tidak sah atau ketidaktersediaan dengan menumpahkan informasi sensitif.	*Eksternal* dan *Internal*	✓						Information exposure
Memperoleh data/informasi sensitif dari sistem informasi yang dapat diakses publik.	*Eksternal* dan *Internal*			✓				Information exposure
Melakukan perusakan/kehancuran pada komponen sistem Informasi.	*Eksternal* dan *Internal*			✓				Dapat menghambat atau menghilangkan kemampuan organisasi untuk menjalankan

Sumber/informasi yang berasal dari sumber ancaman	**Sumber ancaman**	***Relevance***						**Dampak**
		Confirmed	***Expected***	***Antipated***	***Predicted***	***Possible***	***N/A***	
								misi atau fungsi bisnis
Menyebabkan hilangnya integritas dengan menyuntikkan data palsu tetapi dapat dipercaya ke dalam sistem informasi organisasi.	*Eksternal*				✓			Data mengandung virus
Eksploitasi akses fisik staf yang berwenang untuk mendapatkan akses ke fasilitas organisasi.	*Eksternal* dan *Internal*			✓				*blank

Kuesioner ini bertujuan untuk identifikasi kejadian ancaman dan mencari sumber ancaman berdasarkan serangan dari non musuh/non eskternal.

Keterangan:

- Tingkat Kerentanan:
  - High: Sumber ancaman yang memiliki motivasi tinggi dapat merugikan organisasi, hal ini terjadi karena pengendalian untuk mencegah kerentanan dilakukan tidak efektif.
  - Medium: Sumber ancaman memiliki motivasi yang mampu merugikan organisasi, namun organisasi masih dapat melakukan kontrol yang mana mampu menghambat keberhasilan dari kerentanan yang ada.
  - Low: Sumber ancaman yang memiliki motivasi kurang atau rendah, kontrol digunakan untuk mencegah atau mengurangi suatu kerentanan yang akan terjadi pada organisasi.

- Tingkat Dampak:
  - High: Memberikan pengaruh yang besar terhadap organisasi
  - Medium: Memiliki pengaruh besar namun organisasi tidak terancam
  - Low: Dampak tidak berpengaruh signifikan terhadap organisasi

Sumber/informasi yang berasal dari sumber ancaman	Sumber ancaman	Tingkat Kerentanan			Tingkat Dampak	Dampak yang terjadi
		High	Medium	Low		
Jaringan router bermasalah.	*Eksternal* *Internal*			✓	High	Terlambatnya pengaksesan dan pada proses input data
Pemadaman listrik di fasilitas utama.	*Eksternal* *Internal*		✓		High	Aktivitas terhenti
Kesalahan penanganan informasi penting atau sensitif oleh pengguna yang berwenang.	*Internal*		✓		High	Data lost Data tidak sinkron
Keluarnya informasi yang sensitif.	*Eksternal* *Internal*			✓	Medium	Information exposure
Terjadinya kesalahan disk yang meluas.	*Internal*			✓	Low	Data *corrupt*/ data mengalami kerusakan
Kebakaran di fasilitas utama.	*Internal*		✓		High	Kerusakan pada perangkat fisik
Banjir di fasilitas utama	*Lingkungan*		✓		High	Kerusakan pada perangkat fisik

Sumber/informasi yang berasal dari sumber ancaman	Sumber ancaman	Tingkat Kerentanan			Tingkat Dampak	Dampak yang terjadi
Gempa bumi fasilitas utama.	*Lingkungan*			✓	Low	Aktivitas sementara waktu terhenti dan terjadi kerusakan perangkat
Badai difasilitas utama.	*Lingkungan*			✓	High	Terjadinya korsleting listrik
Terjadi kesalahan disk.	Aset			✓	Low	Data mengandung virus
Pengaturan hak istimewa yang Salah.	*Internal*		✓		High	Data lost dan terjadi information exposure
Tampilan tidak terbaca karena peralatan yang menua.	Aset		✓		Low	*blank
Adanya serangan sistem komputer	*Ekternal*		✓		Medium	Mengalami Down
Pencurian aset	*Eksternal* dan Intermal			✓	Medium	Hilangnya aset-aset penting

Lampiran 4. Surat Permohonan Izin Penelitian

Universitas Esa Unggul
Fakultas Ilmu Komputer

Jakarta, 14 November 2022

Nomor : 83-048/SP/KAPRODI-SI/FASILKOM/UEU/EXT/XI/2022
Lampiran : -
Perihal : ***Surat Permohonan Izin Untuk Penelitian***

Kepada Universitas Esa Unggul
Jl. Arjuna Utara No.9, Duri Kepa, Kec. Kb. Jeruk,
Kota Jakarta Barat
Kepala BTIK Universitas Esa Unggul,
Jakarta

Dengan hormat,

Sehubungan dengan mata kuliah Tugas Akhir (Skripsi) yang memerlukan data dan informasi bagi mahasiswa Fakultas Ilmu Komputer Program Studi Sistem Informasi, bersama ini kami sampaikan bahwa mahasiswa kami bermaksud untuk mencari beberapa data / informasi. Adapun nama mahasiswa tersebut adalah :

No	NIM	Nama	No HP	Judul Skripsi
1	20190803034	Fakhirah Din Mohamad	087883934472	ANALISIS RISIKO PADA SISTEM INFORMASI AKADEMIK DI UNIVERSITAS ESA UNGGUL DENGAN MENGGUNAKAN METODE NIST SP 800-30

Kami berharap Bapak/Ibu memberikan izin penelitian untuk Mahasiswa tersebut.

Demikianlah atas perhatian dan kerjasamanya, kami ucapkan terima kasih.

Hormat kami,
Ketua Program Studi Sistem Informasi

Universitas Esa Unggul
FAKULTAS ILMU KOMPUTER
SISTEM INFORMASI

Anik Hanifatul Azizah, S.Kom, M.IM

C.c : 1. Arsip
Note : pada saat pengambilan data bisa mengikuti protokol covid (memakai masker, handsanitizer danpengecekan suhu tubuh, dan sangat disarankan untuk mengambil data secara online).

Jl. Arjuna Utara 9, Tol Tomang, Kebon Jeruk, Jakarta 11510, Indonesia
(021) 567 4223 ext. 207 (021) 567 4248
www.esaunggul.ac.id

Lampiran 5. Dokumentasi


RUANG
SERVER
BATAS SUCI
ALAS KAKI HARUS DILEPAS
Nov 25, 2022, 11:17