DAFTAR LAMPIRAN

Lampiran 1. Daftar Riwayat Hidup
Data Pribadi

Nama	: Alvian Thedy
Tempat, Tanggal Lahir	: Jakarta, 15 Mei 2000
Jenis Kelamin	: Laki-laki
Agama	: Kristen Protestan
Kewarganegaraan	: Indonesia
Alamat	: Jl. Hanoman I No. 31, RT.003 / RW.004, Rawa Buawa, Cengkareng, Jakarta Barat 11740
Nomor Telepon / HP	: 0818-0653-7937
e-mail	: m20180803050@esaunggul.ac.id

Riwayat Pendidikan

Periode (Tahun)	Sekolah / Institusi / Universitas	Jurusan	Jenjang Pendidikan
2006 – 2012	SD Paskalis I	-	SD
2012 – 2015	SMP Paskalis I	-	SMP
2015 – 2018	SMAN 5 Jakarta	MIPA	SMA
2018 – Sekarang	Universitas Esa Unggul	Sistem Informasi	S-1

Lampiran 2. Wawancara

No.	Pertanyaan	Jawaban
1.	Siapa saja yang berhubungan dan bertanggung jawab dengan Sistem Web E-Learning	Yang bertanggung jawab dalam maintenance terhadap e-learning BTIK, namun yang mengelola isi serta merubah mata kuliah adalah BPP dan BPPU, dosen bertugas mengisi kelas yang akan diajar dan juga mahasiswa
2.	Apakah ada aturan tertentu dalam pengadaan hardware dan software serta sistem yang dibuat sebagai pendukung dalam menjalankan web e-learning yang ada ?	Ada, PC dengan Operating sistem Windows serta CPU serta router untuk penghubung jaringan. Serta dalam menjalankan e-learning dibantu dengan MOODLE dan CloudFlare untuk mengamankan jaringan
3.	Perangkat fisik apa saja yang terhubung dengan web e-learning?	Server, komputer dan CPU
4.	Ada berapa jenis web e-learning yang sudah dibuat atau pernah dibuat? Dan tujuan/ target penggunanya siapa?	Sejauh ini sudah ada 3 e-learning yang sudah dibuat, dan yang terakhir ini digunakan untuk semua mahasiswa aktif saat ini
5.	Dimana letak server yang digunakan untuk web e-learning?	Letak server berada di ruang BTIK dan berada diruangan yang sendiri
6.	Bagaimana saat ini dalam penanganan kasus risiko yang sudah terjadi? Apakah ada pelaporan dan tindak lanjut dalam penanganan nya?	Penanganan resiko dilakukan berdasarkan kejadian di saat itu, belum ada tindak lanjut Ketika masalah sudah selesai
7.	Dalam interkoneksi jaringan, web e-learning terhubung dengan web atau sistem apa saja?	Web e-learning terhubung dengan CloudFlare dan siakad dalam mengambil data mahasiswa dan mengintegrasikan nilai dari e-learning ke siakad
8.	Siapa saja yang berhak dalam merubah, menambahkan, serta menghapus akses? Sertakan jabatan di dalam struktural yg dibuat	Yang berhak dalam mengubah serta memberikan akses diawali oleh BTIK kemudian dialihkan ke BPP dan BPPU dalam menangani kegiatan perkuliahan

9.	Kontrol apa saja yang sudah di terapkan dalam menangani keamanan informasi terhadap web e-learning?	Setiap pegawai memiliki akun untuk hak akses, Penggunaan CloudFlare sebagai standar keamanan jaringan, Dilarang membawa makanan dan minuman ke dalam ruang kerja, Maintenance setiap 2 kali dalam setahun, Setiap awal semester seluruh stakeholder disarankan untuk mengubah password akun, Terdapat pelatihan untuk dosen

Lampiran 3. Hasil Kuisioner

Kuisioner mengenai karakteristik sistem dan mengidentifikasi aset

Asset		Keterangan
Data dan Informasi	Data mata kuliah	Data mengenai materi perkuliahan
	Data nilai	Data mengenai nilai-nilai mahasiswa
	Data dosen	Data mengenai dosen yang mengajar berdasarkan kejuruan dan mata kuliah
	Data mahasiswa	Data mengenai mahasiswa yang tergabung dalam kelas
	Data tugas	Data mengenai tugas-tugas mata kuliah
	Data absensi	Data mengenai kehadiran dosen maupun mahasiswa
Software	MOODLE	Sebuah software yang membantu mengoperasikan e-learning
	CloudFlare	Software jaringan yang menjamin keamanan akses
Hardware	Komputer+CPU	Menggunakan OS Linux, Windows 10
	Server	Menjalankan perangkat lunak administratif yang mengontrol akses terhadap jaringan dan sumber daya yang terdapat di dalamnya
	Router	Router adalah sebuah alat jaringan computer yang mengirimkan paket

		data melalui sebuah jaringan
SDM/Karyawan	BTIK	Bagian organisasi yang bertugas mensupport tingkat keamanan dan aksesbilitas sistem
	BPP	Bagian organisasi yang bertugas mengecek materi perkuliahan
	BPPU	Bagian organisasi yang bertugas mendaftarkan kelas kedalam sistem
	Dosen	Bagian organisasi yang bertugas dalam menyerahkan bahan ajar, mengajar serta menilai tugas mahasiswa
	Mahasiswa	Bagian organisasi yang bertugas sebagai peserta didik dalam tingkat Perguruan Tinggi

Kuisioner mengenai sumber ancaman berdasarkan asal aset

Sumber Ancaman/aset/	Capabilitas aset				Target/ Tujuan serangan	Tingkat kerentanan					Dampak yang dialami
	Ubah	Input	Hapus	Backup		Very High	High	Moderate	Low	Very Low	
Dalam BTIK	X		X	X	*blank*					X	*blank*
Dosen		X	X		*blank*					X	Data nilai dan tugas

											berubah
Luar BTIK	X	X	X		Mengubah data		X				Ada data yang berubah serta information exposure
Mahasiswa		X			*blank*				X		Data tugas dan nilai kosong
Server crash/down /bermasalah	*blank*										Sistem tidak dapat diakses
Pemadaman listrik	*blank*										Perangkat menjadi tidak berfungsi

Kuisioner untuk mengidentifikasi kejadian ancaman dan mencari sumber ancaman berdasarkan tingkat kemampuan dari pihak external

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.

Keterangan:

- Pada sumber ancaman dapat dituliskan menjadi: eksternal, internal, personal
    - Ekternal: pihak diluar Univesitas Esa Unggul yang melakukan serangan
    - Internal: pihak dalam Univesitas Esa Unggul yang dapat melakukan kesalahan
    - Personal: adalah pihak yang mengekspos atau melakukan kesalahan pribadi yang dapat mengancam informasi pribadi
- Pada tabel relevance, jika tidak terjadi atau belum terjadi dapat dikosongkan (N/A)
- Pada bagian tabel dampak, diperbolehkan kosong apabila relevansi tidak pernah terjadi

Sumber atau Informasi dari Sumber ancaman	Sumber ancaman	*Relevance*					*Dampak*
		Confirmed	*Expected*	*Anticipated*	*Predicted*	*Possible*	
Kumpulkan informasi menggunakan penemuan sumber terbuka informasi organisasi.	Eksternal					X	Information Exposure
Mengirimkan malware yang dimodifikasi ke sistem informasi internal organisasi.	Eksternal				X		Information Exposure
Mengirimkan malware yang ditargetkan untuk mengontrol sistem internal dan	Eksternal	N/A					Information Exposure dan pengubahan data secara paksa

Sumber atau Informasi dari Sumber ancaman	Sumber ancaman	*Relevance*					*Dampak*
		Confirmed	*Expected*	*Anticipated*	*Predicted*	*Possible*	
pemusnahan data.							
Memanfaatkan akses fisik staf yang berwenang untuk mendapatkan akses ke fasilitas organisasi.	Eksternal Internal	n/a					pencurian
Kompromi perangkat lunak sistem informasi penting organisasi.	Internal						
Melakukan serangan intersepsi komunikasi.	Eksternal	N/A					*blank*
Melakukan serangan gangguan nirkabel.	Eksternal	N/A					*blank*
Melakukan serangan menggunakan port, protokol, dan layanan yang tidak sah.	Eksternal				X		Sistem sulit diakses

Sumber atau Informasi dari Sumber ancaman	Sumber ancaman	*Relevance*					*Dampak*
		Confirmed	*Expected*	*Anticipated*	*Predicted*	*Possible*	
Melakukan serangan Denial of Service (DoS) yang ditargetkan.	Eksternal			X			Sistem sulit diakses
Melakukan serangan fisik terhadap infrastruktur pendukung fasilitas organisasi.	Ekternal/ Internal	N/A					*blank
Melakukan upaya login brute force/serangan menebak kata sandi.	Internal dan Personal						
Menyebabkan hilangnya integritas dengan membuat, menghapus, dan/atau memodifikasi data pada sistem informasi yang dapat diakses publik	Eksternal	X					Data orisinil diubah/ dihapus

Sumber atau Informasi dari Sumber ancaman	Sumber ancaman	*Relevance*					*Dampak*
		Confirmed	*Expected*	*Anticipated*	*Predicted*	*Possible*	
(misalnya, perusakan web).							
Menyebabkan hilangnya integritas dengan mencemari atau merusak data penting.	Eksternal / Internal				X		Data yang diinput mengandung virus
Menyebabkan hilangnya integritas dengan menyuntikkan data palsu tetapi dapat dipercaya ke dalam sistem informasi organisasi.	Eksternal			X			Data yang mengandung virus
Mendapatkan akses yang tidak sah.	Personal /Eksternal					X	Password yang lemah
Memperoleh data/informasi sensitif	Personal / Eksternal				X		Information Exposure

Sumber atau Informasi dari Sumber ancaman	Sumber ancaman	*Relevance*					*Dampak*
		Confirmed	*Expected*	*Anticipated*	*Predicted*	*Possible*	
dari sistem informasi yang dapat diakses publik.							

Kuisioner untuk mengidentifikasi kejadian ancaman dan mencari sumber ancaman berdasarkan serangan dari non-musuh/non eksternal

Keterangan:

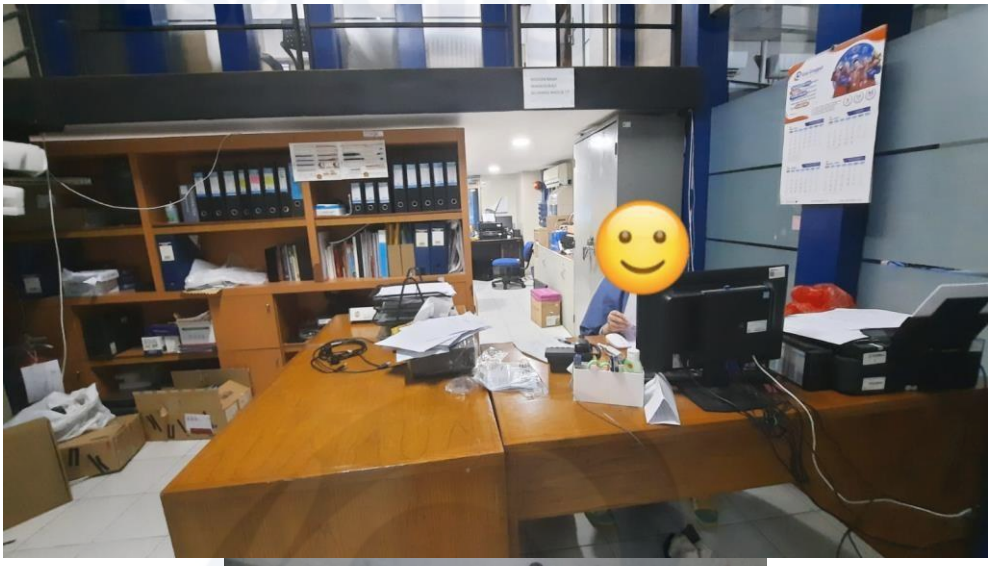
- Tingkat kemungkinan:
  - Very High = Terjadi hamper setiap saat
  - High = Terjadi 5x dalam setahun
  - Medium = Terjadi hampir 3x setahun
  - Low = Terjadi hamper 2x setahun
  - Very Low = Terjadi hamper 1x setahun atau hamper tidak pernah

Sumber atau Informasi dari Sumber ancaman	Sumber ancaman	Tingkat Kemungkinan					Tingkat Dampak	Dampak Yang dialami
		Very High	*High*	*Medium*	*Low*	*Very Low*		

Tumpahan/keluarnya informasi sensitif	Ekternal			x			High	Information Exposure
Kesalahan penanganan kritis dan/atau sensitif informasi oleh pengguna yang berwenang	Internal					x		Kerusakan perangkat Data lost
Pengaturan hak istimewa yang salah	Internal		x					Information Exposure Data lost
Tampilan tidak terbaca, karena UI/hardware	Aset					x		
Gempa di fasilitas utama	Lingkungan					x		
Kebakaran di fasilitas utama	Internal					X		
Banjir di fasilitas utama	Lingkungan					X	Low	
Badai di fasilitas utama	Lingkungan			X			Very High	Korsleting listrik
kesalahan disk	Aset							Data mengandung virus
Kesalahan disk yang meluas	Internal/ aset					X	Very High	Data yang *corrupt*
Jaringan router yang bermasalah	aset			X			Low	Keterlambatan akses dan input data

Lampiran 4. Tempat penelitian

Berikut adalah tampak dalam dan luar dari ruang BTIK, didalam ruang BTIK terdapat ruangan server, namun penulis tidak diizinkan untuk mendokumentasikannya



Lampiran 5. Surat Izin Penelitian

Universitas Esa Unggul
Fakultas Ilmu Komputer

Jakarta, 25 Juli 2022

Nomor : 83-016/SP/KAPRODI-SI/FASILKOM/EXT/VII/2022
Lampiran : -
Perihal : ***Surat Permohonan Izin Untuk Penelitian***

Kepada Yth. Kepala BTIK Universitas Esa Unggul
RT.1/RW.2, Duri Kepa, Kec. Kb. Jeruk,
Kota Jakarta Barat,

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 :

Nama : Alvian Thedy
NIM : 20180803050
Judul TA/Skripsi: Analisis Manajemen Risiko Terhadap Sistem E-learning Dengan Metode NIST SP 800-30 (Studi kasus: Universitas Esa Unggul)

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 dan pengecekan 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. 206, 207 (021) 567 4248
www.esaunggul.ac.id