BAB V
KESIMPULAN DAN SARAN

5.1. Kesimpulan

Hasil perolehan dan pengolahan data terkait penelitian evaluasi tingkat keamanan informasi pada kantor Sistem Informasi di Universitas X mendapatkan total skor ketergantungan kategori Sistem Elektronik (SE) yaitu 28 dan tingkat ketergantungan termasuk ke dalam kategori "Tinggi". Hasil pada seluruh area pengamanan Kantor Sistem Informasi di Universitas X mendapatkan Tingkat kelengkapannya sebesar 324 dengan status Pemenuhan Kerangka Kerja Dasar dan Tingkat Kematangan secara keseluruhan di Kantor Sistem Informasi di Universitas X menyentuh level I+ sampai dengan level II. Pada Area Suplemen, bagian pengamanan dengan keterlibatan pihak ketiga mencapai 67%, Pengamanan Layanan Infrastruktur Awan mencapai 67%, dan bagian Perlindungan Data Diri mencapai 33%. Hasil dari evaluasi keamanan informasi yang telah didapatkan menunjukan bahwa Kantor Sistem Informasi di Universitas X masih tergolong "Tidak Layak" dalam pemenuhan standar ISO/IEC 27001.

Dalam rangka memenuhi standar ISO/IEC 27001, semua aspek yang dinilai dalam Indeks KAMI memerlukan perbaikan. Perbaikan yang dilakukan dengan pemberian rekomendasi berdasarkan kekurangan yang telah teridentifikasi di setiap area penilaian. Dengan demikian, Kantor Sistem Informasi di Universitas X dapat meningkatkan keamanan informasinya melalui rekomendasi yang diberikan.

5.2. Saran

Dalam penelitian yang telah dilakukan, berikut ini akan disampaikan beberapa saran untuk penelitian yang lebih lanjut:

1. Penelitian selanjutnya diharapkan menggunakan Indeks KAMI versi terbaru yang disediakan oleh pihak KOMINFO.
2. Melakukan evaluasi keamanan informasi secara teratur (2x setahun) menggunakan Indeks KAMI untuk memantau kesiapan keamanan

informasi dan mengevaluasi keberhasilan perbaikan rekomendasi yang telah diterapkan. Dengan ini, tingkat kematangan dan tingkat kelengkapan dapat mencapai ambang batas minimum ISO/IEC 27001.

DAFTAR PUSTAKA

[1] A. L. Maryanto, M. N. Al Azam, and A. Nugroho, "Evaluasi Manajemen Keamanan Informasi Pada Perusahaan Pemula Berbasis Teknologi Menggunakan Indeks Kami," *J. Simantec*, vol. 11, no. 1, pp. 1–12, 2022, doi: 10.21107/simantec.v11i1.14099.

[2] C. A. Cholik, "PERKEMBANGAN TEKNOLOGI INFORMASI KOMUNIKASI / ICT DALAM BERBAGAI BIDANG," *J. Fak. Tek.*, vol. 2, no. 2, pp. 39–46, 2021.

[3] I. B. A. E. M. Putra, N. Gunantara, and M. Sudarma, "Tata Kelola Teknologi Informasi Dengan Kerangka Kerja COBIT 5 Pada Lembaga Pemerintah Dan Swasta," *Maj. Ilm. Teknol. Elektro*, vol. 20, no. 1, p. 1, 2021, doi: 10.24843/mite.2021.v20i01.p01.

[4] A. Kornelia and D. Irawan, "Analisis Keamanan Informasi Menggunakan Tools Indeks Kami ISO 4.1," *J. Pengemb. Sist. Inf. dan Inform.*, vol. 2, no. 2, pp. 78–86, 2021, doi: 10.47747/jpsii.v2i2.548.

[5] B. Triandi, "Keamanan Informasi secara Aksiologi Dalam Menghadapi Era Revolusi Industri 4.0," *JURIKOM (Jurnal Ris. Komputer)*, vol. 6, no. 5, pp. 477–483, 2019, [Online]. Available: http://ejurnal.stmik-budidarma.ac.id/index.php/jurikom/article/view/1556

[6] Y. Ding, Z. Wu, Z. Tan, and X. Jiang, "Research and application of security baseline in business information system," *Procedia Comput. Sci.*, vol. 183, pp. 630–635, 2021, doi: 10.1016/j.procs.2021.02.107.

[7] S. F. Rahayu *et al.*, "PENGUKURAN TINGKAT KEAMANAN INFORMASI MENGGUNAKAN METODE INDEKS KAMI (Studi Kasus: Dinas Komunikasi dan Informatika Kota Pontianak)," *Coding J. Komput. dan Apl.*, vol. 09, no. 03, pp. 468–477, 2021.

[8] G. Prasetyaningrum, Finda Nurmayanti, and Fallya Azahra, "Faktor-Faktor Yang Mempengaruhi Etika Sistem Informasi: Moral, Isu Sosial Dan Etika Masyarakat (Literature Review Sim)," *J. Manaj. Pendidik. Dan Ilmu Sos.*, vol. 3, no. 2, pp. 520–529, 2022, doi: 10.38035/jmpis.v3i2.1115.

[9] J. Fasilkom, "Tanggamus Menggunakan Indeks Kami Versi 4 . 2," vol. 13, no. 2, pp. 181–187, 2023.

[10] Badan Siber dan Sandi Negara, "Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2020 Tentang Sistem Pengamanan Dalam Penyelenggaraan Sistem Elektronik," p. 20, 2020.

[11] A. Wicaksana and T. Rachman, "Peraturan Menteri Komunikasi dan Informatika Republik Indonesia No. 4 Tahun 2016," *Angew. Chemie Int. Ed. 6(11), 951–952.*, vol. 3, no. 1, pp. 10–27, 2018, [Online]. Available: https://medium.com/@arifwicaksanaa/pengertian-use-case-a7e576e1b6bf

[12] I. Kami, P. Politeknik, and N. Ketapang, "Analisis Tingkat Kesiapan Keamanan Informasi Menggunakan," vol. 9, no. 1, pp. 1–9, 2024.

[13] B. Penilaian, I. Kami, and D. Xyz, "EVALUASI SISTEM MANAJEMEN KEAMANAN INFORMASI BERDASARKAN PENILAIAN INDEKS KAMI v.4.2 PADA DINAS XYZ PROVINSI JAWA TENGAH".

[14] P. Kantor, W. Kementerian, H. Dan, and H. A. M. Diy, "Evaluasi Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Information Security Evaluation Using Information Security Index (KAMI) In The Ministry Of

Law And Ham DIY," vol. 3, no. 1, pp. 1–6, 2020.
[15] A. Firdani, Suprapto, and A. R. Perdanakusuma, "Perencanaan Pengelolaan Keamanan Informasi Berbasis ISO 27001 Menggunakan Indeks KAMI (Studi Kasus: Dinas Komunikasi dan Informatika Kabupaten Rembang)," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 3, no. 6, pp. 6009–6015, 2019, [Online]. Available: http://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/5617
[16] S. Yuliani, N. T. Ramadhini, A. I. Gustisyaf, and A. Wahyudin, "Asesmen Keamanan Informasi Menggunakan Indeks Kami," *Naratif J. Nas. Riset, Apl. dan Tek. Inform.*, vol. 2, no. 1, pp. 1–5, 2020, doi: 10.53580/naratif.v2i1.76.
[17] D. Saputra, R. Y. Rahman, M. S. Hasibuan, and G. J. H Aziz, "Penilaian Tingkat Kesiapan Keamanan Informasi Pada Dinas Kominfo Kabupaten Xyz Dengan INDEKS Kami Ver 42," *J. Ilmu Komputer, Sist. Informasi, Tek. Inform.*, vol. 2, no. 2, 2023.
[18] D. Rutanaji, S. S. Kusumawardani, and W. W. Winarno, "ISO 27001 sebagai Metode Alternatif bagi Perancangan Tata Kelola Keamanan Informasi (Sebuah Usulan untuk Diterapkan di Arsip Nasional RI)," *Pros. Semin. Nas. ReTII ke-12 2017*, pp. 168–173, 2017, [Online]. Available: https://journal.itny.ac.id/index.php/ReTII/article/view/604
[19] H. A. Pratiwi and L. Wulandari, "Evaluasi Tingkat Kesiapan Keamanan Informasi Menggunakan Indeks Keamanan Informasi (Indeks KAMI) Versi 4.0 pada Dinas Komunikasi dan Informatika Kota Bogor," *J. Ind. Eng. Manag. Res.*, vol. 2, no. 5, pp. 146–163, 2021.
[20] M. F. Husin, H. . Wowor, and S. D. . Karouw, "Implementasi Indeks Kami Di Universitas Sam Ratulangi," *J. Tek. Inform.*, vol. 12, no. 1, 2017.
[21] J. A. dan C. M. Karyati, "perancangan sistem manajemen keamanan informasi (SMKI) berdasarkan ISO 27001:2022 (studi kasus data center dinas komunikasi dan informatika kota Tangerang selatan)," *Ilm. KOMPUTASI*, vol. 4, no. 1, pp. 88–100, 2023.

Lampiran 1 Wawancara dengan Kepala Kantor Sistem Informasi di Universitas X

Tempat: Kantor Sistem Informasi di Universitas X Tanggal: Selasa, 7 Mei 2024 Waktu : 10.12 WIB		
No	**Pertanyaan**	**Jawaban**
1.	apakah pernah ada peneliti yg mengunakan KSI sebelumnya? klo ada apakah menggunakan Index KAMI versi berapa?	Belum ada penelitian yang menggunakan Indeks Kami. Dulu untuk menilai tingkat maturitinya menggunakan COBIT, CMM, model model seperti itu.
2.	Seberapa sering penilaian resiko keamanan informasi dilakukan, dan bagaimana penilain tersebut dilakukan? apakah sudah baik atau belum?	Selama ini di KSI seringnya berdasarkan *based on incident*. Jadi kalo ada insiden nanti dianalisis terlebih dahulu baru diperbaiki. Lalu direncanakan kira-kira seperti apa atau di *budgeting*, nanti proses pengamanannya seperti apa, selama pengamanannya menggunakan firewall, lalu dari sisi software bagaimana. Jadi seperti itu.
3.	apakah metode yang terakhir kali digunakan dalam penilaian risiko keamanan informasi	Dari pihak kami tidak memakai metode khusus atau belum, seperti ISO 27001. Yaudah berdasarkan *based on incident* dan dengan cara kerja internal di KSI dianalisis dan penanganannya bagaimana
4.	apakah ada permasalahan yang pernah terjadi disini, seperti data bocor, atau ada kendala dalam penginputan data? selain dari itu apakah ada juga serangan dari luar seperti retasnya website?	Yang sering itu retasan website. Pihak luar yang mencoba menyerah website website yang dimiliki oleh KSI untuk memasukkan iklan judi slot.
5.	Untuk website dan maraknya peretasan website seperti masuknya judi slot, dan lain-lain, dan itu terjadi karena apa ya pak?	Ya bisa jadi si pengelolanya tidak mengupdate versinya. Verisnya itu kan versi yang lama lalu ada bugs-nya atau bisa jadi kejadian usernya yang nggak *aware* sehingga akunya yang punya kases lebih ke *detected* atau keambil sama *lockstealer* atau *malware* sehingga, lalu bisa dipake orang untuk masuk kayak gitu kan padahal punya admin gitu dan kejadiannya seperti itu yaa
6.	Apa saja teknologi yang digunakan KSI untuk mengamankan data dan sistem informasi?	Kita ada firewall dan berbagai perlengkapannya. Firewall kan ada *hardware*, *software*, dan sistem. Lalu kita menggunakan *framework* Ketika membuat sistem seperti autentikasinya nanti seperti apa, lalu beberapa data yang sesintif dienkripsi. Untuk *update patch* ke sistem yang terbaru, dan ada

		beberapakan yang websitenya itu makai *open source*.
7.	Bagaimana KSI mengelola akses pengguna dan mengontrol privasi data dalam organisasi?	Kalo di Universitas X itu kan *by role*. Jadi sesuai dengan jabatannya atau perannya. Misalnya jadi Kepala departemen nanti disistem apa ya tentu menu-menunya lebih banyak dibandingkan dengan dosen biasa
8.	Bagaimana struktur keamanan informasi di KSI ini dirancang dan diimplementasikan?	Kalo kebijakan terkait dengan data *government* dimana didalamnya terhadap *security* belum ada tapi akan disusun.
9.	apakah disini sudah mengupayakan keamana informasi dengan baik? Upaya apa yang dilakukan?	Ya sudah, salah satunya tadi data sensitive dienkripsi, kemudian hak akses sesuai peran. Nah tinggal nantikan yang mau diini kan dari level kebijakan. Kalo tadi level operasional. Baru mau dibuat kebijakan
10.	Bagaimana proses identifikasi dan penanganan pelanggaran keamanan dilakukan di KSI?	Ya itu tadi, sama seperti yang tadi hanya berdasarkan *based on incident*. Ada insiden baru diidentifikasi. Jadi beberapa sudah memanfaatkan aturan-aturan yang ada di piranti firewallnya
11.	Bagaimana kebijakan KSI terkait dengan penggunaan perangkat dan aplikasi pihak ketiga yang memengaruhi keamanan informasi?	Untuk kebijakannya memang belum ada, tapi ada beberapa di Universitas X misalnya semua sistemnya harus dikembangkan sendiri, lalu kita menggunakan .net, lalu kalo mereka memakai *open source* lalu dulu pernah ke pengelola-pengelolanya untuk rajin diupdate. Misalnya *worldpress*, ojs untuk jurnal. jadi seperti itu si, tapi kalo ketentuan bahwa tidak boleh *install* macem-macem itu memang belum, hanya kemarin kan lalu ada edaran bahwa jangan menginstall *software* bajakan, kayak gitu.
12.	Apakah KSI telah melaksanakan pelatihan keamanan informasi untuk karyawan? Bagaimana efektivitasnya dievaluasi?	Belum, untuk keseluruh karyawan belum. Tapi ada beberapa karyawan yang kemarin kami ikutkan pelatihannya *ec-council cscu (certified srcure computer user)* bareng dengan mahasiswa Informatika. Nah untuk keamanan secara umum seperti itu si. Dan yang lainnya masih hanya awareness lewat *broadcast* lewat *message* di email, atau lewat banner-banner dan kalo anda perhatikan sekarang fokusnya ke *security*.
13.	sebarapa sering melaksanakan evaluasi terkait dengan keamanan informasi?	Biasanya ya, ya tadi karena belum terjadwal ya itu tadi saat *based on*

	apakah 1 bulan sekali atau hanya saat penilaiaan?	*incident*

Lampiran 2 Wawancara dengan Kepala Kantor Keamanan Informasi di Universitas X

Tempat: Kantor Sistem Informasi di Universitas X Tanggal: Kamis, 20 Juni 2024 Waktu : 15.57 WIB		
Area Tata Kelola		
No	**Pertanyaan**	**Jawaban**
2.12	Apakah tanggung jawab pengelolaan keamanan informasi mencakup koordinasi dengan pihak pengelola/pengguna aset informasi internal dan eksternal maupun pihak lain yang berkepentingan, untuk mengidentifikasikan persyaratan /kebutuhan pengamanan (misal: pertukaran informasi atau kerjasama yang melibatkan informasi penting) dan menyelesaikan permasalahan yang ada?	Kalo salama ini, kami kan pengelolaan keamanan informasinya ya, misalnya kalo ada insiden langsung ini siapa ya yang PIC yang terkait dengan insiden ini, misalnya ngga bisa di handle kek misalnya ada brich kok situs kuliahnya kebobol kedeteksi sama username nya ini. Nah nanti dikoordinasikan dengan bidang yang ngurusin itu. Lalu ya bidang yang ngurusin itu menghubungi user untuk mengganti passwordnya. Untuk proses alurnya seperti itu. Ada ni bidang infrastruktur jaringan mendeteksi adanya serangan judi online lagi, nah ini kan perlu dihubungkan lagi ke bidang-bidang yang mengurus seperti situs kuliah, e-jurnal.
2.21	Apakah Kantor Sistem Informasi di universitas X sudah mengidentifikasi legislasi, perangkat hukum dan standar lainnya terkait keamanan informasi yang harus dipatuhi dan menganalisa tingkat kepatuhannya?	Belum, dari pihak kampus belum ada legal atau apa. Dan UUPDP belum di sahkan perlindungan data pribadi jadikan kita haru melindungi data pribadi seperti apa juga ada. Peraturan dari universitas juga belum ada. Nah seprti yang saya bilang tadi bahwa kebijakan terkait data government dan securitynya belum. Mungkin kalo dari kami itu seperti instruksi kerjanya bahwa password harus di enkripsi. Dan untuk bentuk dokumen seperti hukum atau standar
Area Risiko Keamanan Informasi		
No	**Pertanyaan**	**Jawaban**
3.3	Apakah Kantor Sistem Informasi di universitas X mempunyai kerangka kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?	Kalo kami sekedar password harus di enkripsi, terus kami mengirim edaran jangan gunakan software bajakan. Kebijakan seperti password harus ada gabungan angka, huruf besar, kecil yang mudah-mudah seperti itu aja. Untuk instruksi kerjanya ada bahwa ini harus ada enkripis dengan algoritma ini
Area Kerangka Kerja		
No	**Pertanyaan**	**Jawaban**

4.3	Apakah tersedia mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpanannya?	Prosedur umum saja. Jadi misalnya data ini nanti harus disimpan berapa lama, kalo data-data mahasiswa yang sudah lulus dihapus atau disimpan belum ada. Kalo yang sudah ada yaa itu ya tadi oke udah disimpan, disini, terus kalo ada insiden lalu harus gimana dan mana yang harus di proteksi oh ya sperti password algorritamnay apa.
4.8	Apakah konsekuensi dari pelanggaran kebijakan keamanan informasi sudah didefinisikan, dikomunikasikan dan ditegakkan?	Belum, ya itu di level universitas missal ada kebocoran data harus gimana, belum ada. Dan prosedur serta kebijakan seperti yang sudah dibilang data government belum ada.
4.15	Apakah tersedia kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (business continuity planning) yang mendefinisikan persyaratan/konsiderans keamanan informasi, termasuk penjadwalan uji cobanya?	Kami cuman ada prosedur back-up data saja secara rutin. Terus nanti ada maintenance macem-macem juga ada. Dan untuk dokumennya sekarang lebih ke otomatis ke sistemnya. Yaa tinggal ditentukan saja mau back-upnya seminggi 1x atau tiap malam.
4.16	Apakah perencanaan pemulihan bencana terhadap layanan TIK (disaster recovery plan) sudah mendefinisikan komposisi, peran, wewenang dan tanggung jawab tim yang ditunjuk?	Karena selama ini yang mengelola cuman 1. Jadi kami punya bidang infrastruktur jaringan ya mereka yang ngeprint arsinya. Termasuk back-up nya nyimpan dimana, dan upsnya seperti apa. Tapi karena keterbatasan staff disini yaa orang itu yang mengelola itu. Dan untuk bagian itu kan hanya 2 orang jadi ya dibantu untuk sistem back-upnya dengan sistem
4.23	Apakah Kantor Sistem Informasi di universitas X memiliki dan melaksanakan program audit internal yang dilakukan oleh pihak independen dengan cakupan keseluruhan aset informasi, kebijakan dan prosedur keamanan yang ada (atau sesuai dengan standar yang berlaku)?	Kami kan di universitas ini ada ISO tapi 21001 bukan ISO yang terkait keamanan 2700. Itu rutin, ada. Dan nanti yang via independent biasanya 1 tahun 2x atau 1x, saya lupa tapi nanti juga ada audit internal sendiri yang auditnya di luar KSI. Tapi itu tidak focus ke keamanan ya, itu audit untuk semua proses di KSI, dan itu juga di semua universitas dan termasuk KSI. Ya meskipun bisa jadi salah satunya kemarin di audit prosedur back-upnya, ada yang nyambung ke keamanan informasi, tapi ada juga yang nggak.
Area Pengelolaan Aset		
No	**Pertanyaan**	**Jawaban**
5.2	Apakah tersedia definisi klasifikasi aset informasi yang sesuai dengan peraturan perundangan yang berlaku?	Belum ada

5.6	Apakah tersedia proses pengelolaan konfigurasi yang diterapkan secara konsisten?	Ada, kalo misalnya kaitannya dengan konfigurasi dengan deployment sistemnya. Kitakan punya untuk membuat sistemnya makai .net nah nanti oh ini harus ke dev nya dulu, baru ke productionnya, macem-macem itu konfigurasinya ada. Dan ada prosedurnya
5.32	Apakah tersedia proses pengelolaan konfigurasi yang diterapkan secara konsisten?	Nggak ada, ya cuman pake VPN saja bahwa mau akses jaringan internal misalnya laptopnya KSI dibawa keluarkan mau akses jaringan ini, ada VPN. Pegawai juga mau akses jaringan di universitas juga pakai VPN. Dan surat tugas seperti workshop, dll itu ada.
5.33	Apakah tersedia proses untuk memindahkan aset TIK (piranti lunak, perangkat keras, data/informasi dll) dari lokasi yang sudah ditetapkan (termasuk pemutakhiran lokasinya dalam daftar inventaris)?	Itu kan ada di sistemnya, di aset management macem-macem. Yaa itu bukan KSI yang mengelola tetapi ada kantor sendiri, kantor prasarana dan sarana kan yang segala mencatat mutasi barang, macem-macem. Tapi kalo KSI misalnya, oh ada alat yang sudah nggak dipakai kita kembalikan yaa ada.
Area Teknologi dan Keamanan Informasi		
No	**Pertanyaan**	**Jawaban**
6.1	Apakah layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan?	Kita kan ada firewall, lalu ada SSO. Untuk mengakses insternet, dll kan harus login dulu.
6.7	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada?	Ada, semua akses point dapat di monitor. Kalo ada jaringan yang putus atau nggak switch-switchnya itu ada. Dan semuanya dalam bentuk laporan sudah by sistem
6.10	Apakah semua log dianalisa secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik)?	Kita tidak menganalisa tetapi kami sudah by sistem. Nah kalo baru ada insiden baru kita analisis dan itu sudah ada sistemnya. Memanfaatkan firewall, semua log sudah disimpan dengan masing-masing sistemnya. Lebih mengandalkan ke sistemnya
6.16	Apakah sistem dan aplikasi yang digunakan sudah menerapkan pembatasan waktu akses termasuk otomatisasi proses timeouts, lockout setelah kegagalan login, dan penarikan akses?	Beberapa ada,karena sistemnya banyak. Kaya situs kuliah itu otomatis nantikan timeouts, terus beberapa sistem juga timeout.
Area Suplemen		
No	**Pertanyaan**	**Jawaban**

7.1.1.7	Apakah hak audit TI secara berkala ke pihak ketiga/pihak ketiga telah ditetapkan sebagai bagian dan persyaratan kontrak, dikomunikasikan dan disetujui pihak ketiga? Termasuk di dalamnya akses terhadap laporan audit internal / eksternal tentang kondisi kontrol keamanan informasi pihak ketiga/pihak ketiga?	Ya itu tadi, audit secara umum saja. Tidak fokus dengan keamanan informasinya.
7.1.3.8	Apakah kondisi terkait denda / penalti karena ketidakpatuhan pihak ketiga terhadap persyaratan dan / atau tingkat layanan telah didokumentasikan, dikomunikasikan, dipahami dan diterapkan?	Itu biasanya vendor, contoh misalnya udah dibagian kontraknya misalnya, kami bekerja sama dengan salah satu profider untuk benwit, nanh nanti mereka perfomennya tidak sesuai ya mereka sendiri yang sudah punya aturan, berarti harus beri konpensasi ke universitas seperti ini, lalu nantinya mungkin untuk tagihan bulan ini oh kami otomatis ke diskon karena mereka sempat down atau apa. Nah itu sudah bagian dari kontrak dan biasanya di benwit aja.
7.3.3	Apakah proses terkait penyimpanan, pengolahan dan pertukaran data pribadi di Kantor Sistem Informasi di universitas X sudah didokumentasikan?	Ya semuanya melalui sistem dan by sistem
7.3.5	Apakah Kantor Sistem Informasi di universitas X sudah menunjuk pejabat-pejabat (Data Protection Officer, Data Controller, Data Processor) yang bertanggung-jawab dan berwenang dalam penerapan kebijakan dan proses Perlindungan Data Pribadi?	Belum ada. Karena staffnya juga terbatas
7.3.9	Apakah Kantor Sistem Informasi di universitas X sudah menjalankan program peningkatan pemahaman/kepedulian kepada seluruh pegawai terkait Perlindungan Data Pribadi, termasuk hal-hal terkait Peraturan Perundangan yang berlaku?	Ya kalo PDP nya atau peraturanya belum di sahkan ya kami hanya awareness saja bahwa ganti password rutin biar nanti data mereka keretas, jangan ngeklik phising sembarangan, jangan menggunakan software bajakan. Jadi ya lebih kesitu saja. Untuk memberitahukan awareness itu biasanya kami broadcast, seperti pengumuman-pengumuman ke mahasiwa.