KURAWAL Jurnal Teknologi, Informasi dan Industri *Volume 6 Nomor 1 - Maret 2023*
e-issn : 2615-6474
p-issn : 2620-3804
URL : https://jurnal.machung.ac.id/index.php/kurawal

PERENCANAAN SISTEM MANAJEMEN KEAMANAN INFORMASI BERDASARKAN STANDAR ISO 27001:2013 PADA KOMINFO KABUPATEN MALANG

Anis Setyaningrum [1)], Yudhi Kurniawan [2)], Rudy Setiawan [3)]

[1,2,3)] Program Studi Sistem Informasi, Universitas Ma Chung
Jalan Villa Puncak Tidar N-1 Malang

email : 321810021@student.machung.ac.id[1)], yudhi.kurrniawan@machung.ac.id[2)], rudy.setiawan@machung.ac.id[2)]

Abstrak

Dinas Komunikasi dan Informasi (DISKOMINFO) Kabupaten Malang merupakan Perangkat Daerah (PD) yang memanfaatkan Teknologi Informasi dan Komunikasi (TIK). Terkait dengan pentingnya penerapan Tata Kelola TIK untuk Sistem Manajemen Keamanan Informasi, yang diatur dalam Peraturan Presiden No. 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE) serta Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 4 Tahun 2016, semua lembaga pemerintah diwajibkan melaksanakan manajemen keamanan untuk seluruh informasi yang mereka kelola. Metode yang digunakan dalam penelitian ini untuk mengatasi masalah yang dibahas adalah dengan membuat kebijakan dan prosedur operasional standar (SOP) serta menilai risiko keamanan informasi pada aset organisasi dengan merujuk pada standar ISO/IEC 27001:2013 sebagai standar manajemen keamanan informasi. Alasan penggunaan standar ini adalah karena pemerintah Indonesia melalui Badan Standardisasi Nasional (BSN) telah menetapkan SNI ISO/IEC 27001:2013 sebagai standar nasional (SNI) untuk mengelola keamanan informasi bagi semua organisasi dari berbagai jenis dan ukuran. Hasil penelitian ini adalah penyusunan dokumen kebijakan keamanan informasi dan dokumen SOP untuk meningkatkan kontrol keamanan dalam sistem manajemen keamanan informasi yang berbasis ISO/IEC 27001:2013.

Kata Kunci :

SNI ISO/IEC 27001:2013, Sistem Manajemen Keamanan Informasi (SMKI), Standar Operasional Prosedur (SOP).

Abstract

The Department of Communication and Information (DISKOMINFO) of Malang Regency is a Regional Apparatus (PD) that utilizes Information and Communications Technology (ICT). Regarding the importance of implementing ICT Governance for the Information Security Management System, as stipulated in Presidential Regulation No. 95 of 2018 on Electronic-Based Government Systems (SPBE) and the Regulation of the Minister of Communication and Information of the Republic of Indonesia Number 4 of 2016, all government agencies are required to implement security management for all the information they handle. The method used in this study to address the discussed issues involves developing policies and standard operating procedures (SOPs) and assessing information security risks in organizational assets, referring to the ISO/IEC 27001:2013 standard as a guideline for information security management. The reason for using these standards is that the Indonesian government, through the National Standardization Body (BSN), has designated SNI ISO/IEC 27001:2013 as the national standard (SNI) for managing information security for organizations of all types and sizes. The result of this research is the creation of information security policy documents and SOP documents to enhance security controls within information security management systems based on ISO/IEC 27001:2013.

Keywords :

SNI ISO/IEC 27001:2013, Information Security Management System (SMKI), Standard Operating Procedure (SOP).

e-issn : 2615-6474
p-issn : 2620-3804
URL : https://jurnal.machung.ac.id/index.php/kurawal

1. PENDAHULUAN

Dinas Komunikasi dan Informatika (DISKOMINFO) Kabupaten Malang adalah Perangkat Daerah (PD) yang memanfaatkan TIK (*Information and Communications Technology*). Terkait dengan pentingnya penerapan Tata Kelola TIK tentang Sistem Manajemen Pengamanan Informasi yang terlampir pada Peraturan Presiden No. 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE) dan Peraturan Menteri Komunikasi dan Informatika Republik Indonesia pada Nomor 4 Tahun 2016 [1], [2]. Belum adanya standar manajemen keamanan informasi sebagai salah satu indikasi dan syarat dalam implementasi Sistem Pemerintahan Berbasis Elektronik (SPBE) pada domain keamanan informasi. Dengan pelaksanaan penelitian ini dapat membantu dalam pengelolaan risiko keamanan informasi dan pembuatan kebijakan yang mengarah ke dalam standar internasional ISO 27001:2013 pada Bidang Persandian dan Aplikasi Informatika Kominfo Kab. Malang.

Hasil dari penelitian ini mencakup 2 dokumen yaitu dokumen pengelolaan risiko terkait keamanan informasi meliputi identifikasi risiko, penilaian risiko dan analisa dan evaluasi risiko. Selanjutnya dokumen Sistem Manajemen Keamanan Informasi (SMKI) yang meliputi control objektif dan kontrol keamanan, kebijakan keamanan informasi dan standar operasional prosedur (SOP).

2. METODE / ALGORITMA

Dalam pengerjaan penelitian ini, metode yang digunakan yaitu dengan mengimplementasikan dokumen ISO:IEC 27001:2013 yang meliputi menentukan kebijakan, prosedur, sasaran keamanan informasi dan proses dalam SMKI yang bersangkutan untuk dalam menangani risiko dan meningkatkan keamanan informasi agar dapat memerikan hasil yang sesuai keseluruhan kebijakan dalam sasaran yang direncanakan [3]. Menerapkan dan mengoperasikan kebijakan, prosedur, kontrol keamanan dan proses SMKI. Memberikan penilaian dan mengukur kinerja atas proses kebijakan, sasaran keamanan informasi, praktik SMKI dan melaporkannya kepada pihak manajemen untuk dapat dilakukan peninjauan. Melaksanakan Tindakan perbaikan berdasar pada hasil audit dan tinjauan dari pihak manajemen atau informasi terkait lainnya agar dapat mencapai peningkatan yang berkelanjutan [4]. Alur penelitian dalam penelitian ini adalah dimulai dari tahap awal yaitu studi literatur dan identifikasi dan analisa masalah. Pengumulan data dilakukan dengan cara wawancara dan observasi. Selanjutnya tahap pengembangan yaitu menentukan ruang lingkup SMKI, melakukan penilaian risiko, identifikasi risiko, analisis risiko, evaluasi risiko, memilih control objektif dan control keamanan dan pembuatan kebijakan keamanan informasi [5].

3. HASIL DAN PEMBAHASAN

Sasaran atas penerapan SMKI adalah melindungi aset organisasi yang dimiliki dan dikelola oleh Kominfo Kabupaten Malang dari segala risiko yang berkaitan dengan keamanan informasi yang mendukung proses bisnis di Kominfo Kabupaten Malang.

3.1 Penilaian Resiko

Identifikasi terhadap aset yang dimiliki oleh Kominfo Kabupaten Malang yang memiliki fungsi untuk mendukung proses bisnis yang ada di dalam organisasi. Beberapa hasil yang didapatkan pada proses observasi dilakukan yaitu ditemukannya beberapa kemungkinan risiko yang dapat terjadi di Kominfo Kabupaten Malang.

e-issn : 2615-6474
p-issn : 2620-3804
URL : https://jurnal.machung.ac.id/index.php/kurawal

Tabel 1 Kemungkinan Risiko dan Dampak

No.	Risiko	Dampak
R1	Kebakaran	Kehilangan aset-aset dan mengganggu proses bisnis instansi tersebut.
R2	Petir	Alat rusak, ketersediaan data terhambat, instansi mengalami kerugian secara finansial, proses bisnis terganggu.
R3	Gempa Bumi	Alat rusak, ketersediaan data terhambat, instansi mengalami kerugian secara finansial, proses bisnis terganggu.
R4	Banjir	Kehilangan aset-aset dan mengganggu proses bisnis instansi tersebut.
R5	*Human Error*	Aset-aset IT tidak beroperasi dengan baik, data sulit untuk diakses, mengganggu proses bisnis.
R6	Kegagalan Proyek IT	Rencana yang sudah dibuat tidak berjalan.
R7	Anggaran yang tidak tercukupi	Teknologi yang usang sehingga menimbulkan banyak celah pada sistem.
R8	Regulasi /SOTK (Struktur Organisasi dan Tata Kerja)	Terhentinya program belum berjalan dan program yang sudah berjalan.
R9	*Service Level Agreement* (SLA)	Tidak adanya kontrak kerja yang mengikat .
R10	Buku petunjuk yang kurang memadai	Pedoman tidak jelas dan tidak terukur yang mengakibatkan kewajiban dan tanggung jawab tidak terpenuhi.
R11	Penyalahgunaan hak akses/*user* ID	Manipulasi data, kebocoran informasi atau data penting.
R12	Pencurian Perangkat	Kehilangan perangkat, kehilangan data, kerugian finansial dan proses bisnis terganggu.
R13	Data dan Informasi yang tidak sesuai dengan fakta	Manipulasi data, proses bisnis terganggu.
R14	*Maintenance* tidak terjadwal	Melemahnya kapasitas personal komputer dan mal fungsi.
R15	Dokumentasi tidak lengkap	Menyulitkan programmer dalam pengembangan program dan kesalahan pembuatan fungsi pada program.
R16	*Cybercrime*	Manipulasi data, pencurian data.
R17	Mutasi pegawai fungsional	Banyak aset organisasi tidak berjalan dengan maksimal.
R18	Tidak adanya SDM yang ahli dalam bidangnya	Program yang sedang berjalan dapat terhenti, pegawai baru butuh beberapa waktu untuk menyesuaikan diri sehingga hal ini dapat mengganggu proses bisnis organisasi.
R19	Kesalahan teknis	Pekerjaan terhambat, alat rusak, proses bisnis terganggu
R20	Pengunduran diri	Sulit mencari pengganti staf yang ahli dan berpengalaman dibidang pekerjaan, proses bisnis terganggu.
R21	Pegawai yang sakit atau cedera	Sulit mencari pengganti staf yang ahli dan berpengalaman dibidang pekerjaan.
R22	Petugas tidak mengikuti keseluruhan SOP	Alat rusak, kerja tidak optimal.
R23	Kegagalan sistem jaringan/jaringan terputus	Gagal *update* data, kehilangan data, pekerjaan terganggu.

No.	Risiko	Dampak
R24	Listrik padam	Mengganggu proses kerja, performa server menurun, kerusakan *hardware.*
R25	Kegagalan/rusaknya *Software*	Kehilangan data, proses bisnis sangat terganggu, kerugian secara finansial.
R26	Kegagalan / rusaknya *Hardware*	Kehilangan data, proses bisnis sangat terganggu, kerugian finansial.
R27	Gagal melakukan fungsi media penyimpanan seperti *disk error, disk full*	Gagal menyimpan data, kehilangan data, proses bisnis terganggu.
R28	Data *corrupt*/Rusak	Data rusak, kehilangan data, proses bisnis terganggu
R29	*Overload Database*	Kehilangan data, lambat *loading.*
R30	*Server down*	Kehilangan data, proses bisnis terhenti, kerugian besar.
R31	Kegagalan *recovery data* data	Kegiatan bisnis terhambat.
R32	Genset tidak berfungsi	Mengganggu proses bisnis organisasi.
R33	Program *crash*	Data hilang dan rusak serta SOP yang ada tidak dapat berjalan dengan baik.
R34	Kegagalan *backup* data/ *generate* data	Kehilangan data-data sebelumnya dan tidak adanya pembaharuan data.
R35	*Web service* mati tiba-tiba	Gagal melakukan akses ke program dan data base utama.
R36	Overheat Perangkat Komputer	Alat mengalami kerusakan, *loading* lambat proses bisnis terganggu.
R37	Serangan Virus, *Malware, Malicious Program*	Kehilangan data, proses bisnis terganggu, data *corrupt.*

3.2 Analisis Risiko

Pada proses analisis risiko upaya untuk memahami risiko yang lebih mendalam dilakukannya proses penilaian terhadap kemungkinan risiko yang telah diidentifikasi sebelumnya. Selain itu, proses ini juga digunakan sebagai masukan terhadap risiko serta strategi dalam pengambilan keputusan bagi risiko tersebut [6]. Di dalam Kominfo Kabupaten Malang sendiri terdapat beberapa penemuan risiko yang didapati sering muncul hingga mengganggu proses berjalannya operasional IT mereka.

Tabel 2 Penilaian Kemungkinan Risiko dengan *Likelihood* dan *Impact*

No.	Kemungkinan risiko	*Likelihood*	*Impact*
R1	Kebakaran	*Rare*	*Major*
R2	Petir	*Rare*	*Moderate*
R3	Gempa Bumi	*Rare*	*Moderate*
R4	Banjir	*Rare*	*Major*
R5	*Human Error*	*Possible*	*Moderate*
R6	Kegagalan Proyek IT	*Unlikely*	*Moderate*
R7	Anggaran yang tidak tercukupi	*Possible*	*Major*
R8	Regulasi /SOTK (Struktur Organisasi dan Tata Kerja)	*Possible*	*Moderate*
R9	*Service Level Agreement* (SLA)	*Likely*	*Major*
R10	Buku petunjuk yang kurang memadai	*Possible*	*Moderate*
R11	Penyalahgunaan hak akses/*user* ID	*Rare*	*Major*
R12	Pencurian Perangkat	*Rare*	*Moderate*
R13	Data dan Informasi yang tidak sesuai dengan fakta	*Unlikely*	*Major*
R14	*Maintenance* tidak terjadwal	*Possible*	*Moderate*
R15	Dokumentasi tidak lengkap	*Likely*	*Major*

No.	Kemungkinan risiko	*Likelihood*	*Impact*
R16	*Cybercrime*	*Likely*	*Major*
R17	Tidak adanya SDM yang ahli dalam bidangnya	*Likely*	*Major*
R18	Mutasi pegawai fungsional	*Unlikely*	*Moderate*
R19	Kesalahan teknis	*Unlikely*	*Major*
R20	Pengunduran diri	*Possible*	*Major*
R21	Pegawai yang sakit atau cedera	*Possible*	*Moderate*
R22	Petugas tidak mengikuti keseluruhan SOP	*Possible*	*Moderate*
R23	Kegagalan sistem jaringan/jaringan terputus	*Unlikely*	*Major*
R24	Listrik padam	*Possible*	*Moderate*
R25	Kegagalan/rusaknya *Software*	*Possible*	*Major*
R26	Kegagalan / rusaknya *Hardware*	*Possible*	*Major*
R27	Gagal melakukan fungsi media penyimpanan seperti *disk error, disk full*	*Possible*	*Major*
R28	Data *corrupt*/Rusak	*Possible*	*Moderate*
R29	*Overload Database*	*Likely*	*Moderate*
R30	*Server down*	*Unlikely*	*Major*
R31	Kegagalan *recovery data* data	*Unlikely*	*Major*
R32	Genset tidak berfungsi	*Unlikely*	*Moderate*
R33	Program *crash*	*Possible*	*Moderate*
R34	Kegagalan backup data/*generate* data	*Possible*	*Major*
R35	*Web service* mati tiba-tiba	*Possible*	*Major*
R36	*Overheat* Perangkat Komputer	*Unlikely*	*Moderate*
R37	Serangan Virus, *Malware, Malicious Program*	*Likely*	*Major*

3.3 Evaluasi Risiko

Proses terakhir dalam *risk assessment* adalah melakukan evaluasi risiko. Pada tahapan ini menggunakan rujukan berupa matriks risiko, terbagi menjadi tiga *risk level* dalam matriks tersebut di antaranya *low, medium dan high.* Nilai dari *likelihood* dan *impact* yang telah ditemukan pada kemungkinan risiko di tahapan proses sebelumnya akan dibedakan kembali menyesuaikan matriks yang ada.

LIKELIHOOD						
	Certain / Pasti terjadi (5)	*Medium*	*Medium*	*High*	*High*	*High*
	Likely / Sering (4)	*Low*	*Medium*	R27	R7, R13, R14, R15, R35	*High*
	Possible / Kadang (3)	*Low*	*Low*	R3, R6, R8, R12, R19, R20, R22, R26, R31	R5, R17, R23, R24, R25, R32, R33	*High*
	Unlikely / Jarang	*Low*	*Low*	R4, R16, R30, R34	R11, R18, R21, R28, R29	*High*
	Rare / Hampir Tidak Pernah (1)	*Low*	*Low*	R2, R3, R10	R1, R4, R9	*Medium*
		Insignificant / Sangat Kecil (1)	*Minor*/ Kecil (2)	*Moderate* / Biasa (3)	*Major* / Besar (4)	*Catastrophic* / Sangat Besar (5)
IMPACT						

Gambar 1 Matriks Evaluasi Risiko

3.4 Memilih Kontrol Objektif dan Kontrol Keamanan

Langkah selanjutnya setelah menetapkan pilihan penanganan risiko yaitu, menentukan kontrol keamanan yang sesuai dengan kemungkinan risiko pada aset milik Kominfo Kabupaten Malang. Penetapan kontrol objektif dan kontrol keamanan disesuaikan dengan dampak dari ancaman kemungkinan risiko yang telah di analisa sebelumnya [7]. Pada tabel 3 berikut ini merupakan pemetaan hasil rekomendasi klasifikasi risiko dengan identifikasi risikonya.

Tabel 3 Pemetaan Klasifikasi Risiko dengan Identifikasi Risiko

No.	Klasifikasi Risiko	Identifikasi Risiko
KR1	Risiko Bencana Alam	Kebakaran
		Petir
		Gempa bumi
		Banjir
		Listrik padam
KR2	Risiko *Human Error*	*Human error*
		Kegagalan proyek IT
		Anggaran yang tidak tercukupi
		Buku petunjuk yang kurang memadai
		Tidak adanya SDM yang ahli dalam bidangnya
		Kegagalan *restore data*
		Kegagalan *backup data/generate data*
		Maintenance tidak terjadwal
KR3	Risiko Hukum dan Peraturan	Regulasi /SOTK
		Service Level Agreement
		Dokumentasi tidak lengkap
		Mutasi pegawai fungsional

No.	Klasifikasi Risiko	Identifikasi Risiko
		Pengunduran diri
		Pegawai yang sakit atau cedera
		Petugas tidak mengikuti keseluruhan SOP
KR4	Risiko Penyalahgunaan wewenang	Penyalahgunaan hak akses/*user id*
KR5	Risiko Kriminal	Pencurian perangkat
		Cybercrime
KR6	Risiko Keutuhan Data	Data dan informasi yang tidak sesuai dengan fakta
KR7	Risiko Kegagalan IT	Kesalahan Teknis
		Kegagalan sistem jaringan/jaringan terputus
		Kegagalan/rusaknya *software*
		Kegagalan/rusaknya *hardware*
		Gagal melakukan fungsi media penyimpanan seperti *disk error, disk full*
		Data corrupt/rusak
		Overload database
		Server down
		Genset tidak berfungsi
		Program crash
		Web service mati tiba-tiba
		Overheat perangkat komputer
KR8	Risiko Virus	Serangan virus, *malware, malicious program*

3.5 Dokumen Kebijakan Keamanan Informasi yang Diberikan

Di mana kebijakan ini sebagai arahan dalam melakukan proses-proses kerja berdasarkan keamanan informasi ISO 27001:2013. Dengan harapan dokumen kebijakan yang telah disusun dapat dijalankan dengan baik dalam manajemen keamanan informasi. Berikut ini merupakan hasil dari pemetaan risiko dengan klausul dan kategori kebutuhan keamanan informasi dapat dilihat pada tabel 4.

Tabel 4. Daftar Kebijakan Keamanan Informasi

Aspek	Kebijakan
A.5 Kebijakan Keamanan Informasi	Kebijakan *Backup* dan R*estore*
	Kebijakan Penggunaan Layanan
	Kebijakan Pengelolaan Hak Akses
	Kebijakan Penggunaan *Password*
	Kebijakan Klasifikasi Data
	Kebijakan Virus Komputer dan *Malware*
	Kebijakan Audit Sistem Informasi
A.6 Organisasi Keamanan Informasi	Kebijakan Peran dan Tanggung Jawab Kepegawaian
	Kebijakan Keamanan Informasi Pihak Eksternal
	Kebijakan Manajemen Proyek IT
	Kebijakan Akses Jarak Jauh
A.7 Keamanan SDM	Kebijakan Pengecekan Latar Belakang
	Kebijakan Pelatihan dan Pengembangan SDM
	Kebijakan Penegakan (*Enforcement Policy*)
	Kebijakan Perubahan Tanggung jawab
A.8 Manajemen Aset	Kebijakan Manajemen Aset IT
	Kebijakan Penggunaan yang dapat Diterima (*Acceptable Use Policy*)
	Kebijakan Pengembalian Aset
	Kebijakan Penyimpanan Data

e-issn : 2615-6474
p-issn : 2620-3804
URL : https://jurnal.machung.ac.id/index.php/kurawal

Aspek	Kebijakan
A.9 Kendali Akses	Kebijakan Informasi Sensitif
	Kebijakan Akses USB
	Kebijakan Pembuangan Media
	Kebijakan Pengelolaan Hak Akses
	Kebijakan Akses Jaringan (*Network Access*)
	Kebijakan *Logging* Sistem Dan Komputer
	Kebijakan Hak Akses Istimewa
	Kebijakan Manajemen Otentikasi
	Kebijakan Audit Akses Pengguna
	Kebijakan Pengelolaan Akun
	Kebijakan Manajemen Akses dan Keamanan Data
	Kebijakan Pengelolaan *Password*
	Kebijakan Pembatasan Akses Program Utilitas
	Kebijakan Pembatasan Akses Kode Sumber Program
A.10 Kriptografi	Kebijakan Enkripsi dan Manajemen Kunci
A.11 Keamanan Fisik Dan Lingkungan	Kebijakan Klasifikasi Area Kerja
	Kebijakan Area Terbatas
	Kebijakan Keamanan Fisik
	Kebijakan Penggunaan Fasilitas IT
	Kebijakan Penggunaan IT oleh *Visitor/Guest*
	Kebijakan Perawatan *Hardware*
	Kebijakan Perawatan Kabel Jaringan Telekomunikasi
	Kebijakan Konfigurasi Peralatan
	Kebijakan Manajemen Aset IT
	Kebijakan Pemusnahan Perangkat IT
	Kebijakan Pengosongan Meja dan Layar
A.12 Keamanan Operasi	Kebijakan Instalasi *Software*
	Kebijakan Pengendalian Akses Sistem dan Aplikasi
	Kebijakan Spesifikasi Perangkat PC Dan Laptop
	Kebijakan Manajemen Proyek IT
	Kebijakan Penggunaan Internet
	Kebijakan *Backup* dan *Restore* Data
	Kebijakan Manajemen Risiko
	Kebijakan Manajemen Akses dan Keamanan Data
	Kebijakan Audit dan *Logging*
	Kebijakan Respons Insiden
	Kebijakan Audit Sistem Informasi
A.13 Keamanan Komunikasi	Kebijakan Penggunaan Internet
	Kebijakan Komunikasi Nirkabel
	Kebijakan *Sharing File*
	Kebijakan Penggunaan Email
	Kebijakan Tentang NDA
A.14 Akuisisi, Pengembangan Dan Perawatan Sistem	Kebijakan Pengembangan Sistem
	Kebijakan Keamanan Jaringan Internet dan *Firewall*
	Kebijakan Enkripsi dan Manajemen Kunci
	Kebijakan Pengembangan Sistem
	Kebijakan Pengujian *Software*
	Kebijakan Manajemen Proyek IT
	Kebijakan Privasi
A.15 Hubungan Pemasok	Kebijakan Akses Pihak Ketiga
	Kebijakan Penyimpanan dan Transfer Data

Aspek	Kebijakan
A.16 Manajemen Insiden Keamanan Informasi	Kebijakan Audit Layanan dari Pihak Ketiga Kebijakan Keamanan Informasi Hubungan Pemasok Kebijakan Respons Insiden Kebijakan Pengendalian Insiden Keamanan Informasi
A.17 Aspek Keamanan Informasi Dari Manajemen Keberlangsungan Bisnis	Kebijakan Manajemen Risiko Kebijakan Manajemen Keberlanjutan Bisnis Kebijakan *Backup* Dan *Restore* Data
A.18.Kesesuaian	Kebijakan Kepatuhan Terhadap Perundang-Undangan Kebijakan Hak Cipta Kebijakan Penyimpanan Data Kebijakan Pembuangan Media Kebijakan Privasi Kebijakan Enkripsi dan Manajemen Kunci Kebijakan Audit Sistem Informasi

berikut adalah daftar standar operasional prosedur yang dihasilkan sesuai hasil kebijakan keamanan informasi yang telah dihasilkan.

Tabel 5. Daftar Standar Operasional Prosedur Keamanan Informasi

Aspek	Standar Operasional Prosedur
A.5 Kebijakan Keamanan Informasi	SOP *Backup* SOP *Restore* SOP Pengujian *Backup* SOP Pengajuan Sub domain SOP Pengajuan *Server Hosting* Sop Permintaan Hak Akses SOP Penghapusan Hak Akses SOP Reset *Password* SOP Klasifikasi Data SOP Pemasangan Antivirus SOP Pelaporan Serangan *Malware* SOP Perencanaan Audit Keamanan Informasi
A.6 Organisasi Keamanan Informasi	SOP Pelatihan dan Pengembangan SDM SOP Permintaan Hak Akses Pihak Eksternal SOP Permintaan Sistem Informasi SOP Pembuatan Sistem Informasi SOP Pengendalian *Remote Access*
A.7 Keamanan Sumber Daya Manusia	SOP Perjanjian Kerja SOP Pelatihan dan Pengembangan SDM SOP Penanganan Atas Tindakan Indisipliner Pegawai SOP Penetapan Tugas dan Tanggung jawab
A.8 Manajemen Aset	SOP Inventaris Aset IT SOP Penggunaan Aset IT SOP Pemeliharaan Inventaris Aset IT SOP Penyimpanan Data SOP Klasifikasi Data SOP Inventaris Aset IT SOP Penggunaan Aset IT SOP Pengajuan Pembuangan Media

Aspek	Standar Operasional Prosedur
	SOP Inventaris Aset IT
A.9 Kendali Akses	SOP Permintaan Hak Akses
	SOP Penghapusan Hak Akses
	SOP Manajemen dan Akses Jaringan
	SOP *Log-on* Sistem Informasi
	SOP Pembuatan Email
	SOP Reset Email
	SOP Pengajuan Akses Istimewa
	SOP Pemantauan Keamanan Akses pada Sistem Informasi
	SOP Perencanaan Audit Akses Pengguna
	SOP Penghapusan Hak Akses
	SOP Pemeliharaan Keamanan Akses pada Sistem Informasi
	SOP Permintaan Hak Akses
	SOP *Log-on* Sistem dan Aplikasi
	SOP Reset *Password*
	SOP Pemantauan Sistem Utilitas
	SOP Akses Kode Sumber Program
A.10 Kriptografi	SOP Pemeliharaan Peralatan sandi (Aplikasi Enkripsi Data)
A.11 Keamanan Fisik dan	SOP Penetapan Area Kerja
Lingkungan	SOP Pengurusan Izin Masuk Area Terbatas
	SOP Pengamanan Ruang Server
	SOP Pemasangan *Fire Alarm Sistem*
	SOP Pemasangan Penangkal Petir
	SOP Pemasangan CCTV
	SOP Penggunaan Perangkat IT
	SOP Pinjam Pakai Ruangan *Commond Center*
	SOP Pemeliharaan Peralatan IT
	SOP Pelaporan Kegagalan Perangkat IT
	SOP Perawatan Kabel Jaringan Telekomunikasi
	SOP Pengelolaan dan Pemeliharaan Peralatan IT
	SOP Perizinan Peminjaman Perangkat IT
	SOP Pelaporan Pembuangan Peralatan IT
	SOP Pelaporan Penggunaan IT
	SOP Pelaksanaan Sterilisasi Ruangan
A.12 Keamanan Operasi	SOP Registrasi Pengguna
	SOP Integrasi Sistem Informasi
	SOP Sosialisasi Aplikasi Informatika
	SOP Perbaikan Sistem Informasi
	SOP Pengadaan Perangkat IT
	SOP Pengembangan Sistem Informasi
	SOP Penanganan Insiden *Malware* dan *Cybercrime*
	SOP Pelaporan Insiden *Malware* dan *Cybercrime*
	SOP *Backup*
	SOP *Restore*
	SOP Pengujian *Backup*
	SOP Pencatatan Aktivitas Log
	SOP Pemeliharaan Keamanan Akses pada Sistem Informasi
	SOP Audit Aktivitas Log
	SOP Pengelolaan Sistem
	SOP Perizinan Penambahan Perangkat Lunak pada Sistem
	SOP Pelaporan Kegagalan Perangkat IT
	SOP Perizinan Penambahan Perangkat Lunak pada Sistem

Aspek	Standar Operasional Prosedur
	SOP Keamanan Informasi
A.13 Keamanan Komunikasi	SOP Pengacakan Sinyal
	SOP Perubahan *Bandwith*
	SOP Pemasangan Jaringan Nirkabel
	SOP Pengelolaan Jaringan Internet
	SOP Penerimaan dan Pengiriman Data dan Informasi
	SOP Penggunaan Email
	SOP Pembuatan Surat Perjanjian Penerimaan dan Pengiriman Data dan Informasi
A.14 Akuisisi, Pengembangan dan Perawatan Sistem	SOP Perizinan Pengembangan Sistem Informasi
	SOP Pengajuan Pembangunan *Firewall*
	SOP Pemeliharaan Peralatan Sandi (Aplikasi Enkripsi Data)
	SOP Pengembangan Sistem Informasi
	SOP Perubahan Sistem Informasi
	SOP Pengujian Sistem Informasi
	SOP Pelaporan Pengembangan Sistem Informasi
	SOP Perizinan Pengembangan Sistem Informasi oleh Pihak Ketiga
	SOP Pelaporan Pengujian Sistem Informasi
	SOP Penggunaan Data Uji
A.15 Hubungan Pemasok perubahan layanan pemasok	SOP Pembuatan Perjanjian Hak Akses dengan Pihak Ketiga
	SOP Pelaporan Insiden Kepada Pihak Ketiga
	SOP Pengukuran Kinerja Pihak Ketiga
	SOP Pengelolaan Perubahan Layanan Pemasok
A.16 Manajemen Insiden Keamanan Informasi	SOP Penanganan Insiden Keamanan Informasi
	SOP Pelaporan Kejadian Keamanan Informasi
	SOP Penilaian Insiden Keamanan Informasi
	SOP Manajemen *Disaster Recovery Plan*
	SOP Penyusunan Manajemen Risiko IT
A.17 Aspek Keamanan Informasi dari Manajemen Keberlangsungan Bisnis	SOP Perencanaan Penyusunan Keamanan Informasi
	SOP Pelaksanaan Manajemen Keamanan Informasi
	SOP Pengukuran Perencanaan Keamanan Informasi
	SOP *Backup*
	SOP *Restore*
	SOP Pengujian *Backup*
A.18 Kesesuaian	SOP Perencanaan Audit Keamanan Informasi
	SOP Pengajuan Hak Kekayaan Intelektual
	SOP Pengendalian Rekaman
	SOP Pengendalian Kerahasiaan Informasi Pribadi
	SOP Pemeliharaan Peralatan Sandi (Aplikasi Enkripsi Data)
	SOP Audit Keamanan Informasi

4. KESIMPULAN

Kesimpulan yang didapatkan adalah berdasarkan dari hasil penelitian tugas akhir yang telah dilakukan maka yang dapat dihasilkan yaitu pemetaan *risk* kategori terhadap 14 klausul dan 114 kontrol keamanan yang ada pada standar ISO 27001:2013 sehingga dapat memunculkan 2 daftar dokumen SMKI yang terdiri dari 65 kebijakan keamanan informasi dan 96 standar operasional prosedur (SOP) keamanan informasi. Adapun saran yang dapat peneliti berikan terkait sistem manajemen keamanan informasi (SMKI) sesuai standar ISO 27001:2013 untuk Kominfo Kab. Malang yaitu penulis menyarankan agar usulan terhadap daftar dokumen kebijakan dan standar operasional prosedur (SOP) yang telah dihasilkan dapat

diimplementasikan oleh Kominfo Kab. Malang dan terus dikembangkan dengan menyesuaikan kondisi terkini pada instansi.

5. REFERENSI

[1] DIT. (2020). *IT System Maintenance Policy*.
[2] Dinas Komunikasi dan Informatika Kab. Malang. (2019). *Standar Operasional Prosedur KJKS*. 155.
[3] Atmojo, S. A., & Manuputty, A. D. (2020). Analisis Manajemen Risiko Teknologi Informasi Menggunakan ISO 31000 pada Aplikasi AHO Office. *JATISI (Jurnal Teknik Informatika Dan Sistem Informasi)*, *7*(3), 546–558. https://doi.org/10.35957/jatisi.v7i3.525
[4] Briggs, S. (2022). *Disposal of IT Equipment Policy*. *February*, 1–5.
[5] Driantami, H. T. I., Suprapto, & Perdanakusuma, A. R. (2018). Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 (Studi kasus : Sistem Penjualan PT Matahari Department Store Cabang Malang Town Square). *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, *2*(11), 4991–4998.
[6] Hartati, T. (2017). Perencanaan Sistem Manajemen Keamanan Informasi Bidang Akademik Menggunakan ISO 27001: 2013. *KOPERTIP : Jurnal Ilmiah Manajemen Informatika Dan Komputer*, *1*(2), 63–70. https://doi.org/10.32485/kopertip.v1i02.24
[7] Ismanto, I., Hidayah, F., & Charisma, K. (2020). Pemodelan Proses Bisnis Menggunakan Business Process Modelling Notation (BPMN) (Studi Kasus Unit Penelitian Dan Pengabdian Kepada Masyarakat (P2KM) Akademi Komunitas Negeri Putra Sang Fajar Blitar). *Briliant: Jurnal Riset Dan Konseptual*, *5*(1), 69.